НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 24.07.2009 №172

Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

НД ТЗІ 2.7-010-09

Чинний від 2009-07-24

ЗМІСТ

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) у частині оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки (ФПБ).

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 в сфері технічного захисту інформації. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. 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.

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації 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.

Верифікація - одинична дія в процесі проведення оцінювання рівня гарантій коректності реалізації ФПБ, яка передбачає виконання докладного дослідження змісту матеріалів з метою прийняття рішення про достатність наведених у них аргументів на користь коректності доказів.

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

Дослідження – одинична дія в процесі проведення оцінювання рівня гарантій коректності реалізації ФПБ, яка передбачає виконання поглибленого аналізу змісту матеріалів на предмет відповідності висунутим вимогам, з використанням спеціальних знань та досвіду експерта.

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 оброблюваної в ІТС інформації.

Захищений від НСД компонент обчислювальної системи – програмний, апаратний або

програмно-апаратний засіб, в якому додатково до основного призначення передбачено функції захисту інформації від загроз НСД.

Інформаційна модель процесу – модель процесу, надана у вигляді опису суттєвих для розгляду вхідних, вихідних та внутрішніх параметрів процесу та зв'язків між ними, яка дозволяє моделювати зміну вихідних параметрів процесу залежно від зміни певних його вхідних та внутрішніх параметрів.

Інформаційний ресурс – дані в електронному вигляді, які можуть бути багаторазово використані (оброблені) в певній інформаційно-телекомунікаційній системі.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які в процесі оброблення інформації діють як єдине ціле. У контексті цього документа поняття інформаційно-телекомунікаційної системи розглядається як синонім поняття автоматизованої системи згідно з НД ТЗІ 1.1-003-99.

Методика перевірки дотримання вимог до рівня гарантій – визначені (встановлені) способи проведення перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ.

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 рівня гарантій коректності реалізації ФПБ. 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 дія в процесі проведення оцінювання рівня гарантій коректності реалізації ФПБ, яка передбачає виконання простого порівняння змісту матеріалів з висунутими вимогами, без залучення спеціальних знань та досвіду експерта.

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

Програма перевірки рівня гарантій – документована сукупність вимог, що підлягає перевірці в процесі експертизи оцінюваного об'єкта експертизи на відповідність вимогам до рівня гарантій коректності реалізації ФПБ.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

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

Тестове покриття – показник, що характеризує здатність тестових процедур випробовувати вимоги до оцінюваного об'єкта експертизи.

Тестові дані – дані, що використовуються як вхідні в процесі проведення випробувань.

4 Позначення та скорочення

У цьому НД ТЗІ використано такі позначення та скорочення:

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;
ПЗ – програмне забезпечення;
ПЗП – постійний запам'ятовуючий пристрій;
ТЗІ – технічний захист інформації;
ФПБ – функціональна послуга безпеки.

5 Загальний опис методології оцінювання рівня гарантій коректності реалізації 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 від НСД інформації, оброблюваної в ІТС, можна виділити два напрями:

- забезпечення захищеності інформації у функціонуючих та/або створюваних ІТС;

- створення засобів технічного захисту інформації (ЗТЗІ) від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

При цьому, як у 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 (наприклад, інформації яка становить державну таємницю або вимоги до захисту якої встановлено законодавством), обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам. Результатами 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 і реалізованих засобів.

5.1.2 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 рівня гарантій коректності їх реалізації;
- система оцінювання, під якою слід розуміти адміністративно-правову структуру, у рамках якої організації, що проводять оцінювання, застосовують критерії оцінки;
- методологія оцінювання, яка визначає послідовність (алгоритм) дій, що виконуються експертами при оцінюванні ефективності функцій захисту інформації та рівня гарантій коректності їх реалізації, а також форму подання результатів оцінювання.

5.1.3 В Україні як критерії оцінки використовуються критерії, встановлені НД ТЗІ 2.5-004-99, а також вимоги інших 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 рівня гарантій 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, ФПБ) та рівень гарантій коректності їх реалізації (рівень гарантій).

5.1.4 Критерії гарантій, встановлені НД ТЗІ 2.5-004-99, містять вимоги до архітектури комплексу засобів захисту (КЗЗ), середовища розробки, послідовності розробки, середовища функціонування, експлуатаційної документації та випробувань КЗЗ. У них вводиться сім рівнів гарантій (Г-1 ... Г-7), які є ієрархічними. Ієрархія рівнів гарантій відображає поступово зростаючу впевненість у тому, що реалізовані в ОЕ ФПБ дозволяють протистояти певним загрозам, а також, що механізми, які їх реалізують, у свою чергу коректно реалізовані та можуть забезпечити очікуваний споживачем рівень захищеності інформації під час її оброблення в ОЕ.

5.1.5 Згідно з положеннями НД ТЗІ 1.1-002-99, гарантії коректності реалізації ФПБ (далі – гарантії) забезпечуються як у процесі розроблення, так і в процесі оцінювання. У процесі розроблення гарантії забезпечуються діями розробника щодо забезпечення правильності (коректності) розробки. У процесі оцінювання гарантії забезпечуються шляхом перевірки додержання розробником вимог критеріїв, аналізу документації, процедур розроблення та постачання ОЕ, а також іншими діями експертів, які проводять оцінювання.

5.1.6 Система оцінювання в Україні функціонує на основі Положення про державну експертизу в 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; вповноважений державний орган, а також підприємства, установи та організації, які проводять експертизу за його дорученням (організатори експертизи); фізичні особи – виконавці експертних робіт з ТЗІ (експерти). Об'єктами експертизи (ОЕ) у частині, що стосується оцінювання рівня гарантій, можуть бути КЗЗ КСЗІ, ЗТЗІ від НСД, а також захищені від НСД компоненти обчислювальної системи.

5.1.7 Методологія оцінювання рівня гарантій коректності реалізації ФПБ передбачає виконання таких етапів робіт:

- ознайомлення з оцінюваним ОЕ, збирання та аналіз матеріалів (документів), що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ;

- розроблення програми перевірки дотримання вимог до рівня гарантій у процесі розроблення, виробництва та постачання замовнику оцінюваного ОЕ;
- розроблення методики перевірки дотримання вимог до рівня гарантій у процесі розроблення, виробництва та постачання замовнику оцінюваного ОЕ;
- виконання оцінювання рівня гарантій згідно з розробленими програмою та методикою;
- аналіз та документування результатів оцінювання рівня гарантій.

5.2 Ознайомлення з оцінюваним об'єктом експертизи, збирання та аналіз матеріалів, що характеризують організацію процесу його розроблення, виробництва та постачання Замовнику

5.2.1 Головною метою цього етапу є прийняття рішення щодо можливості проведення робіт з оцінювання рівня гарантій коректності реалізації ФПБ в наданому на експертизу ОЕ, визначення обсягів та плану подальших 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 або його представником (заявником) разом з проектною, експлуатаційною та супровідною документацією, при цьому в проектній документації розробником ОЕ визначено функціональні специфікації ОЕ (перелік реалізованих в ОЕ ФПБ згідно з НД ТЗІ 2.5-004-99 або іншим чином визначений перелік функцій захисту з описом їх політики згідно з вимогами міжнародних стандартів);
- ОЕ у вигляді засобу ТЗІ або захищеного компонента обчислювальної системи подано на експертизу розробником або його представником (заявником) разом із супровідною та експлуатаційною документацією, в якій розробником ОЕ не визначено функціональні специфікації ОЕ.

5.2.2 Для досягнення поставленої мети етап ознайомлення з ОЕ, збирання та аналізу матеріалів передбачає виконання таких дій:

- ознайомлення з оцінюваним ОЕ з метою перевірки його готовності до виконання робіт з експертизи (може бути виконано в процесі проведення робіт з оцінювання ФПБ);
- попередній аналіз наданих матеріалів з метою попереднього визначення рівня гарантій, який може бути призначено ОЕ за результатами експертизи, та, відповідно, визначення наявності необхідних для виконання оцінювання матеріалів (документів), перелік та зміст яких визначається вимогами до цього рівня гарантій;
- доопрацювання, за необхідності, одержаних матеріалів (або одержання та аналіз додатково запитаних експертом матеріалів) з метою задоволення вимог відповідного рівня гарантій, встановленого НД ТЗІ 2.5-004-99;
- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів робіт.

У процесі ознайомлення з оцінюваним ОЕ експертом має бути складене чітке уявлення про:

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

При цьому необхідна інформація може отримуватися шляхом ознайомлення з наданою документацією, опитування (анкетування) розробників оцінюваного ОЕ та безпосереднього дослідження експертами оцінюваного ОЕ (ці дії доцільно виконувати в процесі проведення робіт щодо оцінювання ФПБ згідно з відповідними методичними вказівками).

На основі результатів ознайомлення з оцінюваним ОЕ, у випадку, якщо отримані результати підтверджують його готовність до проведення подальших робіт (слід розуміти, як мінімум, підтвердження працездатності ОЕ в заявлених умовах та функціонування згідно з характеристиками, наведеними в експлуатаційній документації), має бути проведено аналіз наданих матеріалів з метою попереднього визначення рівня гарантій, який може бути призначено ОЕ за результатами експертизи, після чого визначено наявність всіх необхідних для виконання оцінювання матеріалів (документів), перелік та зміст яких визначається вимогами до відповідного рівня гарантій (з уточненням, за необхідності та з урахуванням вимог цього рівня гарантій, їх складу та змісту). При цьому, у випадку наявності в проектній або експлуатаційній документації чітко визначених функціональних специфікацій ОЕ, жодних обмежень на попередньо визначений рівень гарантій не

накладається, цей рівень визначається лише вмістом наданих документів. За відсутності в наданих матеріалах чітко визначених функціональних специфікацій ОЕ такі специфікації та опис порядку їх реалізації (на рівні деталізації, який задовольняє, як мінімум, вимоги рівня Г-1 критеріїв гарантій щодо послідовності розробки), за згодою розробника (заявника), можуть бути розроблені експертом. При цьому, оскільки розроблення функціональних специфікацій ОЕ та опису порядку їх реалізації експертом не надають можливості впевнитися в дотриманні розробником у процесі проектування та реалізації ОЕ вимог забезпечення відповідності специфікацій КЗЗ ОЕ різного рівня деталізації (функціональні специфікації, проект архітектури, детальний проект, реалізація), максимальний рівень гарантій, який може бути призначений такому ОЕ за результатами експертизи, становить Г-1.

Методичні рекомендації зі збирання та аналізу матеріалів (документів), що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ, викладено в розділі 6.

5.2.3 Результатом ознайомлення з ОЕ, збирання та аналізу матеріалів має бути звіт, в якому експерти, що здійснювали аналіз, повинні викласти свою думку з приводу повноти та змісту наданих матеріалів, обґрунтувати рішення щодо можливості та доцільності проведення подальших робіт з експертизи, а у випадку позитивного рішення – попередньо визначити рівень гарантій, який може бути призначено ОЕ за результатами експертизи, та надати пропозиції щодо плану та послідовності проведення подальших робіт. Крім цього, у випадку позитивного рішення щодо проведення подальших робіт, для ОЕ, який надано на експертизу без чітко визначених функціональних специфікацій, результатом цього етапу має також бути узгоджений з розробником або заявником документ, який містить опис переліку та політики ФПБ, які реалізуються КЗЗ ОЕ, наприклад, у вигляді технічних вимог до оцінюваного ОЕ в частині реалізації ФПБ та опису порядку реалізації цих вимог (може бути використаний документ відповідного змісту, розроблений у процесі проведення робіт з оцінювання ФПБ).

5.2.4 У випадку подання на експертизу розробником (заявником) ОЕ разом з проектною, супровідною та експлуатаційною документацією та з визначеними в проектній документації функціональними специфікаціями ОЕ експерт на цьому етапі має використовувати:

- оцінюваний ОЕ в працездатному стані;
- 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 в ОЕ ФПБ згідно з НД ТЗІ 2.5-004-99 або іншим чином визначеного переліку функцій захисту з описом їх політики, а також специфікації КЗЗ ОЕ різного рівня деталізації та ступеня формалізації, які визначають порядок реалізації ФПБ (функцій захисту) засобами КЗЗ ОЕ;
- супровідну документацію на оцінюваний ОЕ (матеріали, які характеризують процес проектування, розроблення, виробництва та постачання ОЕ; матеріали, що стосуються проведених розробником випробувань ОЕ; тощо);
- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратору; настанову користувачу; тощо).

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 1):

- перевірка факту надання експлуатаційної документації на ОЕ 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 одержаної експлуатаційної документації) та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності ОЕ подальші роботи мають припинятися;
- аналіз, згідно з методичними рекомендаціями, викладеними в розділі 6, наданих розробником (заявником) матеріалів з метою попереднього визначення відповідності їх складу та змісту вимогам до рівня гарантій, визначеного розробником ОЕ або заявником (заявленого рівня гарантій), та надання рекомендацій та/або пропозицій щодо їх доопрацювання та/або надання додаткових матеріалів у випадку виявлення певних невідповідностей;
- повторний аналіз складу та змісту доопрацьованих (додатково наданих) розробником (заявником) матеріалів з метою визначення їх достатності для проведення подальших перевірок на відповідність вимогам до заявленого рівня гарантій або необхідності зниження заявленого рівня гарантій до такого, який випливає зі складу та змісту наданих матеріалів;
- прийняття (після консультацій з розробником або заявником) рішення про

прийнятність уточненого рівня гарантій, відповідність вимогам до якого має бути підтверджено в процесі експертизи, та про продовження робіт;

- документування отриманих результатів у погодженому з розробником (заявником) проміжному звіті з обов'язковою фіксацією уточненого рівня гарантій як такого, відповідність вимогам до якого має бути підтверджено в процесі експертизи.

5.2.5 У випадку подання на експертизу розробником (заявником) ОЕ разом із супровідною та експлуатаційною документацією, але без визначених функціональних специфікацій, експерт на цьому етапі має використовувати:

- оцінюваний ОЕ в працездатному стані;
- супровідну документацію на оцінюваний ОЕ (матеріали, які характеризують процес проектування, розроблення, виробництва та постачання; матеріали, що стосуються проведених розробником випробувань ОЕ; тощо);
- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратору; настанову користувачу; тощо).

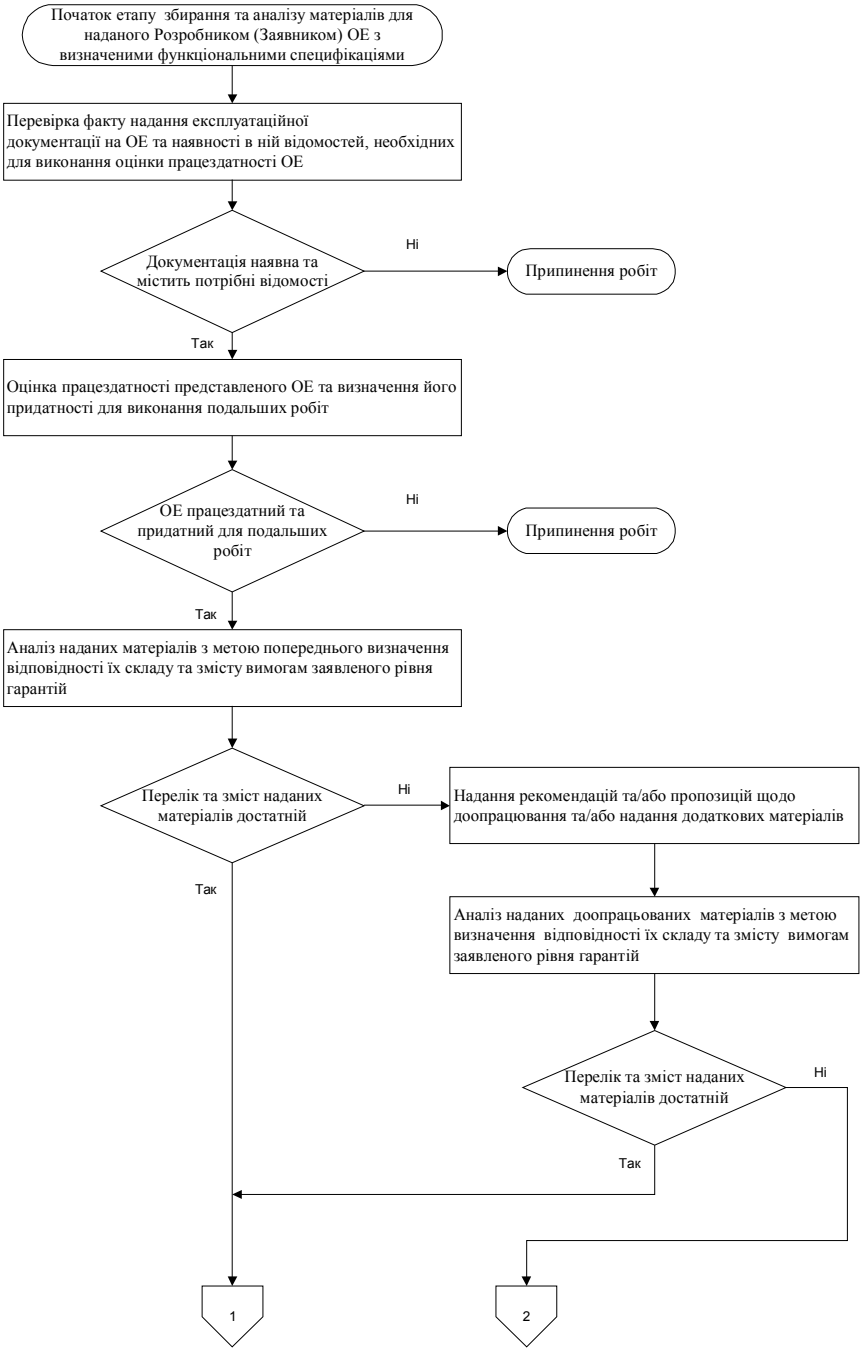


Рисунок 1 (частина 1)

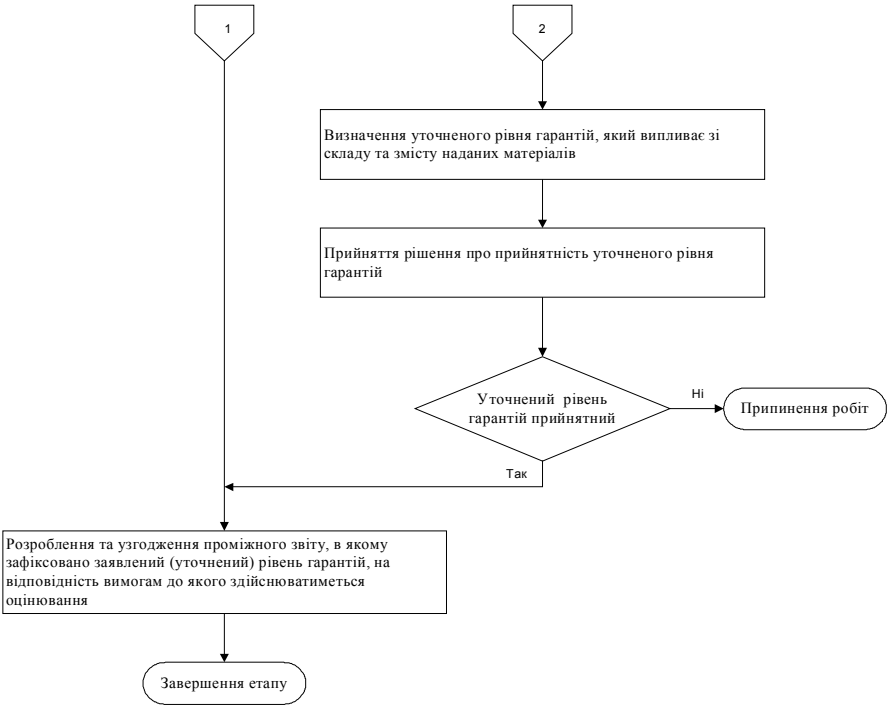
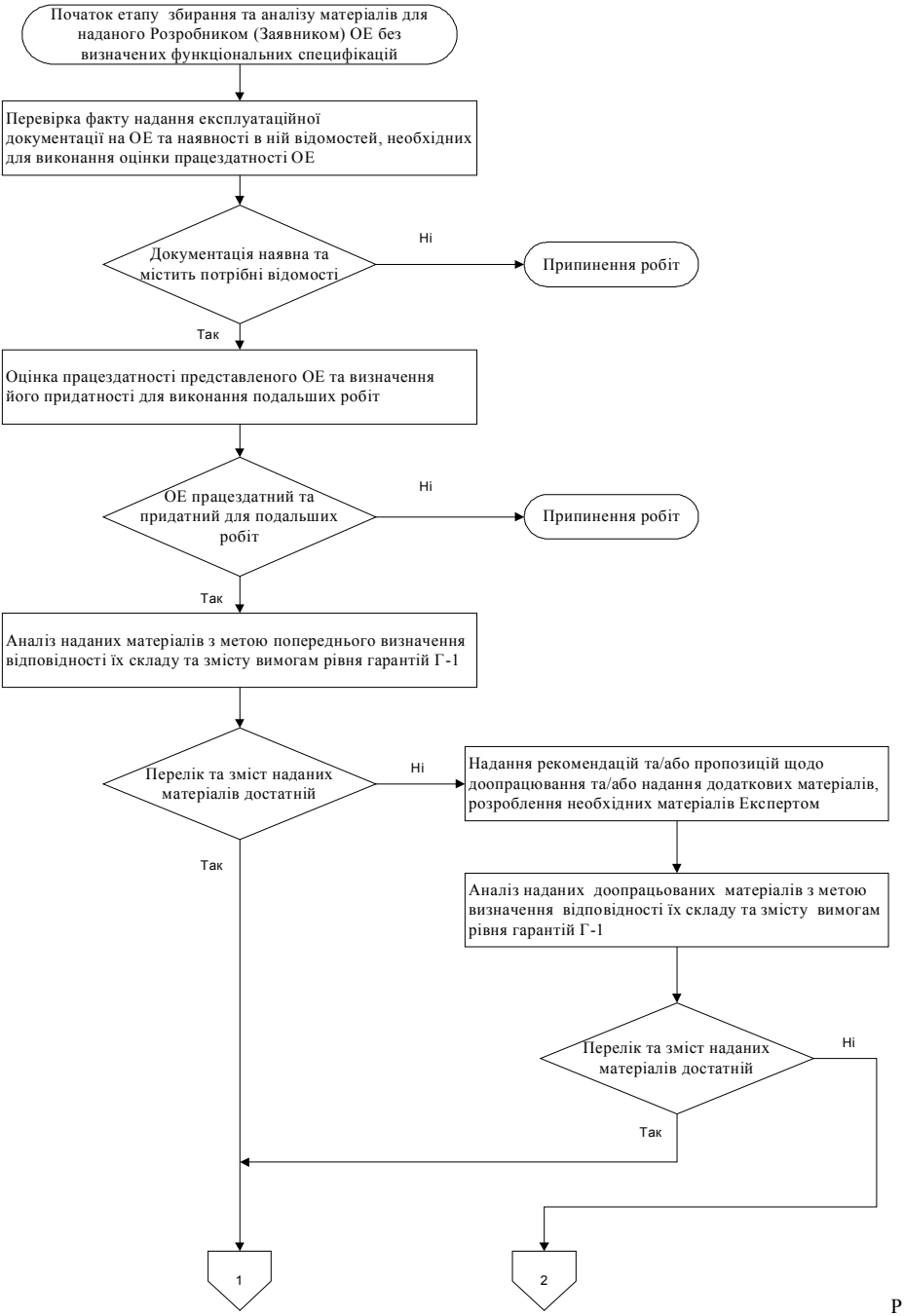


Рисунок 1 (частина 2)

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 2):

- перевірка факту надання експлуатаційної документації на ОЕ 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 одержаної експлуатаційної документації) та визначення його придатності для виконання подальших робіт. У випадку виявлення непрацездатності ОЕ подальші роботи мають припинятися;
- аналіз, згідно з методичними рекомендаціями, викладеними в розділі 6, наданих розробником (заявником) матеріалів з метою попереднього визначення відповідності їх складу та змісту вимогам рівня гарантій Г-1 та надання рекомендацій та/або пропозицій щодо їх доопрацювання та/або надання додаткових матеріалів у випадку виявлення певних невідповідностей;
- за відсутності в наданих матеріалах чітко визначених функціональних специфікацій ОЕ та опису порядку їх реалізації розроблення, за згодою розробника (заявника), таких матеріалів експертом (може бути виконано в процесі проведення робіт з оцінювання ФПБ згідно з відповідними методичними вказівками);
- повторний аналіз складу та змісту доопрацьованих (додатково наданих) розробником (заявником), а також розроблених експертом матеріалів з метою визначення їх достатності для проведення подальших перевірок на відповідність вимогам до рівня гарантій Г-1;



Р

Рисунок 2 (частина 1)

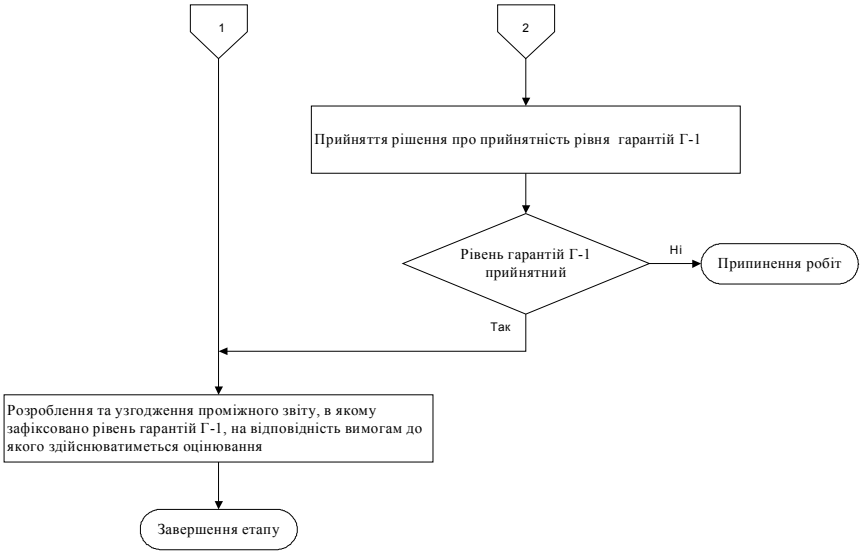


Рисунок 2 (частина 2)

- прийняття (після консультацій з розробником або заявником) рішення про прийнятність рівня гарантій Г-1, відповідність вимогам до якого має бути підтверджено в процесі експертизи, та про продовження робіт;
- документування отриманих результатів у відповідному проміжному звіті з обов'язковою фіксацією в ньому рівня гарантій Г-1 як такого, відповідність вимогам до якого має бути підтверджено в процесі експертизи.

5.3 Розроблення програми перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки

5.3.1 Головною метою цього етапу є розроблення та погодження у встановленому порядку програми перевірки дотримання вимог до заявленого розробником (заявником) та уточненого експертом на попередньому етапі рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ. Як вхідні дані на цьому етапі експертом мають використовуватися всі матеріали, які були зібрані, проаналізовані та уточнені (або розроблені експертом) на попередньому етапі.

5.3.2 Основний зміст програми перевірки дотримання вимог до рівня гарантій, яка розробляється на цьому етапі, становить опис того, що саме, тобто, відповідність яким саме вимогам критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, а також яким саме вимогам інших НД ТЗІ має бути перевірено з метою підтвердження або спростування їх дотримання в процесі розроблення, виробництва та постачання ОЕ.

5.3.3 Методичні вказівки з розроблення та документування програми перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ викладено в розділі 7.

Результатом етапу має бути розроблена та, згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації, погоджена із замовником експертизи та уповноваженим державним органом програма перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ.

5.4 Розроблення методики перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки

5.4.1 Головною метою цього етапу є розроблення та погодження у встановленому порядку методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ. У процесі розроблення методики перевірки має також бути визначена необхідність відвідування експертом підприємства – розробника ОЕ календарний план проведення таких відвідувань та обсяг виконуваних під час відвідувань перевірок. Як вхідні дані на цьому етапі експертом мають

використовуватися:

- матеріали, що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ, які були зібрані, проаналізовані та уточнені (або розроблені експертом) на етапі збирання та аналізу матеріалів;
- розроблена на попередньому етапі програма перевірки дотримання вимог до рівня гарантій.

5.4.2 Основним змістом методики перевірки дотримання вимог до рівня гарантій, яка розробляється на цьому етапі, є опис того, які саме перевірки, з використанням яких документів (матеріалів) та в якій послідовності мають бути виконані з метою підтвердження або спростування дотримання в процесі розроблення, виробництва та постачання ОЕ вимог критеріїв гарантій певного рівня, встановлених НД ТЗІ 2.5-004-99, а також вимог інших НД ТЗІ.

5.4.3 Методичні вказівки з розроблення та документування методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ викладено в розділі 8.

Результатом етапу має бути розроблена та, згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації, погоджена з уповноваженим державним органом методика перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ, а також підготовлений та узгоджений з розробником календарний план проведення відвідувань підприємства – розробника ОЕ з метою перевірки умов розроблення, виробництва та постачання ОЕ.

5.5 Виконання оцінювання

5.5.1 Головною метою цього етапу є здійснення, згідно із затвердженою методикою, певних дій з оцінювання (перевірки, аналізу та/або верифікації зібраних матеріалів, у тому числі під час відвідування підприємства – розробника ОЕ) з фіксацією (у відповідному журналі результатів проведення перевірок рівня гарантій) висновків експерта щодо результатів виконання певних пунктів методики.

5.5.2 Методичні вказівки з виконання оцінювання рівня гарантій коректності реалізації ФПБ викладено в розділі 9.

Результатом цього етапу мають бути відомості, зафіксовані в журналі результатів проведення перевірок рівня гарантій, в яких, з посиланням на відповідні пункти методики перевірки рівня гарантій та використані при цьому матеріали, зафіксовано висновки експерта щодо результатів виконання певних дій з оцінювання.

5.6 Аналіз та документування результатів оцінювання рівня гарантій

На цьому етапі має бути проведено аналіз отриманих у процесі проведення оцінювання та зафіксованих у відповідному журналі результатів. На підставі результатів проведеного аналізу має бути складено протокол, в якому повинно бути узагальнено результати, отримані під час проведення перевірок за кожним пунктом методики перевірки рівня гарантій, та зроблено висновок щодо дотримання/недотримання в процесі розроблення, виробництва та постачання ОЕ вимог критеріїв гарантій певного рівня, встановлених НД ТЗІ 2.5-004-99.

Методичні вказівки з виконання аналізу та документування результатів оцінювання рівня гарантій коректності реалізації ФПБ викладено в розділі 10.

Затверджений організатором експертизи протокол є підставою для підготовки та надання на реєстрацію до уповноваженого державного органу експертного висновку щодо відповідності або невідповідності оцінюваного ОЕ вимогам НД ТЗІ в Україні.

6 Методичні рекомендації зі збирання та аналізу матеріалів, що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного об'єкта експертизи

6.1 Основні зусилля в процесі виконання цих робіт повинні бути спрямовані, у першу чергу, на забезпечення експерта повним (з точки зору відповідності складу вимогам заявленого рівня гарантій) та коректним (з точки зору відповідності змісту вимогам заявленого рівня гарантій) набором документів (матеріалів), які характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ та можуть бути використані на подальших етапах оцінювання. Крім цього, якщо склад та зміст наданих матеріалів не відповідають вимогам заявленого розробником (заявником) рівня гарантій, а доопрацювання наданих та/або одержання додаткових матеріалів не є можливим, відповідні зусилля мають бути спрямовані на коректне визначення

(уточнення) та узгодження з розробником (заявником) більш низького рівня гарантій, вимоги щодо якого наданими та доопрацьованими матеріалами задовольняються.

6.2 У процесі збирання та аналізу матеріалів (документів), що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ, наданого на експертизу розробником (заявником) разом з проектною, супровідною та експлуатаційною документацією з визначеними в проектній документації функціональними специфікаціями ОЕ, експерт на цьому етапі 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 у вигляді переліку реалізованих в ОЕ ФПБ згідно з НД ТЗІ 2.5-004-99 або іншим чином визначеного переліку функцій захисту з описом їх політики, а також специфікації КЗЗ ОЕ різного рівня деталізації та ступеня формалізації, які визначають порядок реалізації ФПБ (функцій захисту) засобами КЗЗ ОЕ;
- супровідну документацію на оцінюваний ОЕ (матеріали, що характеризують процес проектування, розроблення, виробництва та постачання ОЕ; матеріали, що стосуються проведених розробником випробувань ОЕ, тощо);
- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратору; настанову користувачу тощо);
- результати дослідження експертами оцінюваного ОЕ під час попереднього ознайомлення з ним або в процесі проведення робіт з оцінювання ФПБ.

При цьому послідовність (алгоритм) дій експерта має бути такою (рисунок 3):

- перевірка, з використанням рекомендацій, наведених у розділі А.1 Додатка А, відповідності складу наданих розробником (заявником) матеріалів вимогам до заявленого рівня гарантій, з наданням рекомендацій та/або пропозицій щодо складу матеріалів, які мають бути надані експерту додатково з метою забезпечення можливості проведення подальших робіт з оцінювання на відповідність заявленому рівню гарантій;
- перевірка, з використанням рекомендацій, наведених у розділі А.1 Додатка А, складу додатково наданих розробником (заявником) матеріалів з метою визначення їх достатності для проведення подальших перевірок на відповідність вимогам до заявленого рівня гарантій або необхідності зниження заявленого рівня гарантій до такого, який випливає зі складу наданих матеріалів;
- прийняття (після консультацій з розробником або заявником) рішення про прийнятність уточненого за результатами перевірки складу наданих матеріалів рівня гарантій та про продовження робіт;
- аналіз, з використанням рекомендацій, наведених у розділі А.2 Додатка А, змісту наданих розробником (заявником) матеріалів (документів) з метою визначення відповідності змісту та повноти кожного з документів вимогам до заявленого (уточненого) рівня гарантій, з наданням рекомендацій та/або пропозицій щодо їх доопрацювання з метою забезпечення можливості проведення подальших робіт з оцінювання на відповідність заявленому (уточненому) рівню гарантій;

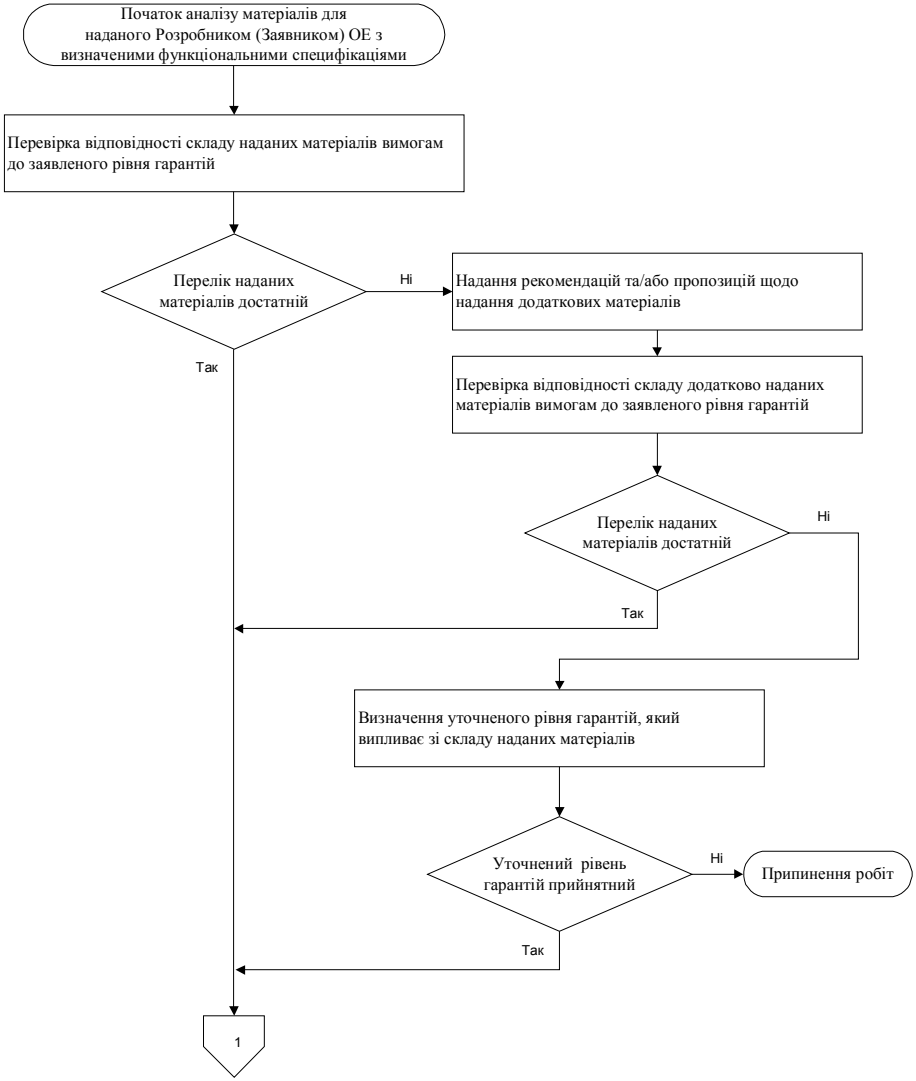


Рисунок 3 (частина 1)

- аналіз, з використанням рекомендацій, наведених у розділі А.2 Додатка А, змісту доопрацьованих розробником (заявником) матеріалів (документів) з метою визначення відповідності змісту та повноти кожного з документів вимогам до заявленого (уточненого) рівня гарантій або необхідності зниження заявленого (уточненого) рівня гарантій до такого, який випливає зі складу та змісту наданих матеріалів;
- прийняття (після консультацій з розробником або заявником) рішення про прийнятність уточненого за результатами аналізу змісту наданих матеріалів рівня гарантій, відповідність вимогам до якого має бути підтверджено в процесі експертизи, та про продовження робіт.

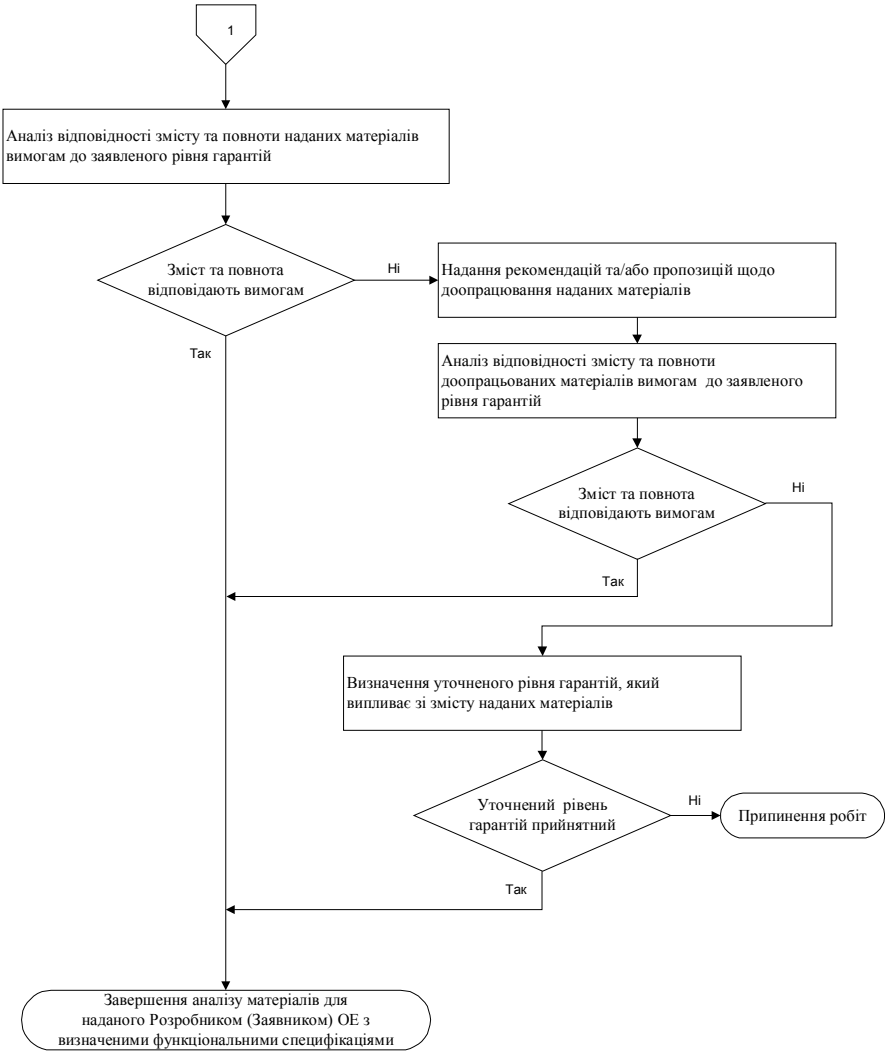


Рисунок 3 (частина 2)

Якщо за результатами перевірки складу наданих розробником (заявником) матеріалів визначено необхідність надання додаткових матеріалів, але в експерта немає сумнівів стосовно одержання (у погоджені терміни) відповідних матеріалів, рішення про достатність переліку наданих матеріалів (та, відповідно, про початок аналізу змісту та повноти наданих матеріалів) може прийматися з урахуванням як вже одержаних матеріалів, так і тих, що мають бути одержані пізніше. При цьому слід враховувати, що прийняття рішення щодо відповідності змісту та повноти певного документа вимогам до певного рівня гарантій можливе лише після завершення відповідного аналізу цього документа.

6.3 У процесі збирання та аналізу матеріалів (документів), що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ, наданого на експертизу розробником (заявником) ОЕ разом із супровідною та експлуатаційною документацією без визначених функціональних специфікацій, експерт на цьому етапі має використовувати:

- супровідну документацію на оцінюваний ОЕ (матеріали, що характеризують процес

проектування, розроблення, виробництва та постачання ОЕ; матеріали, що стосуються проведених розробником випробувань ОЕ, тощо);

- експлуатаційну документацію на оцінюваний ОЕ (опис засобу або системи; опис процедур інсталяції, генерації та запуску; настанову адміністратору; настанову користувачу тощо);
- результати дослідження експертами оцінюваного ОЕ під час попереднього ознайомлення з ним або в процесі проведення робіт з оцінювання ФПБ.

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

- перевірка, з використанням рекомендацій, наведених у розділі А.1 Додатка А, відповідності складу наданих розробником (заявником) матеріалів вимогам до рівня гарантій Г-1, з наданням рекомендацій та/або пропозицій щодо складу матеріалів, які мають бути надані експерту додатково з метою забезпечення можливості проведення подальших робіт з оцінювання на відповідність рівню гарантій Г-1;
- перевірка, з використанням рекомендацій, наведених у розділі А.1 Додатка А, складу додатково наданих розробником (заявником) матеріалів з метою визначення їх достатності для проведення подальших перевірок на відповідність вимогам до рівня гарантій Г-1;
- за відсутності в наданих матеріалах чітко визначених функціональних специфікацій ОЕ та опису порядку їх реалізації розроблення таких матеріалів, за згодою розробника (заявника), експертом;
- аналіз, з використанням рекомендацій, наведених у розділі А.2 Додатка А, змісту наданих розробником (заявником) матеріалів (документів) з метою визначення відповідності змісту та повноти кожного з документів вимогам до рівня гарантій Г-1, з наданням рекомендацій та/або пропозицій щодо їх доопрацювання з метою забезпечення можливості проведення подальших робіт з оцінювання на відповідність вимогам до рівня гарантій Г-1;
- аналіз, з використанням рекомендацій, наведених у розділі А.2 Додатка А, змісту доопрацьованих розробником (заявником) матеріалів (документів) з метою визначення відповідності змісту та повноти кожного з документів вимогам до рівня гарантій Г-1;
- прийняття (після консультацій з розробником або заявником) рішення про прийнятність рівня гарантій Г-1, відповідність вимогам до якого має бути підтверджено в процесі експертизи, та про продовження робіт.

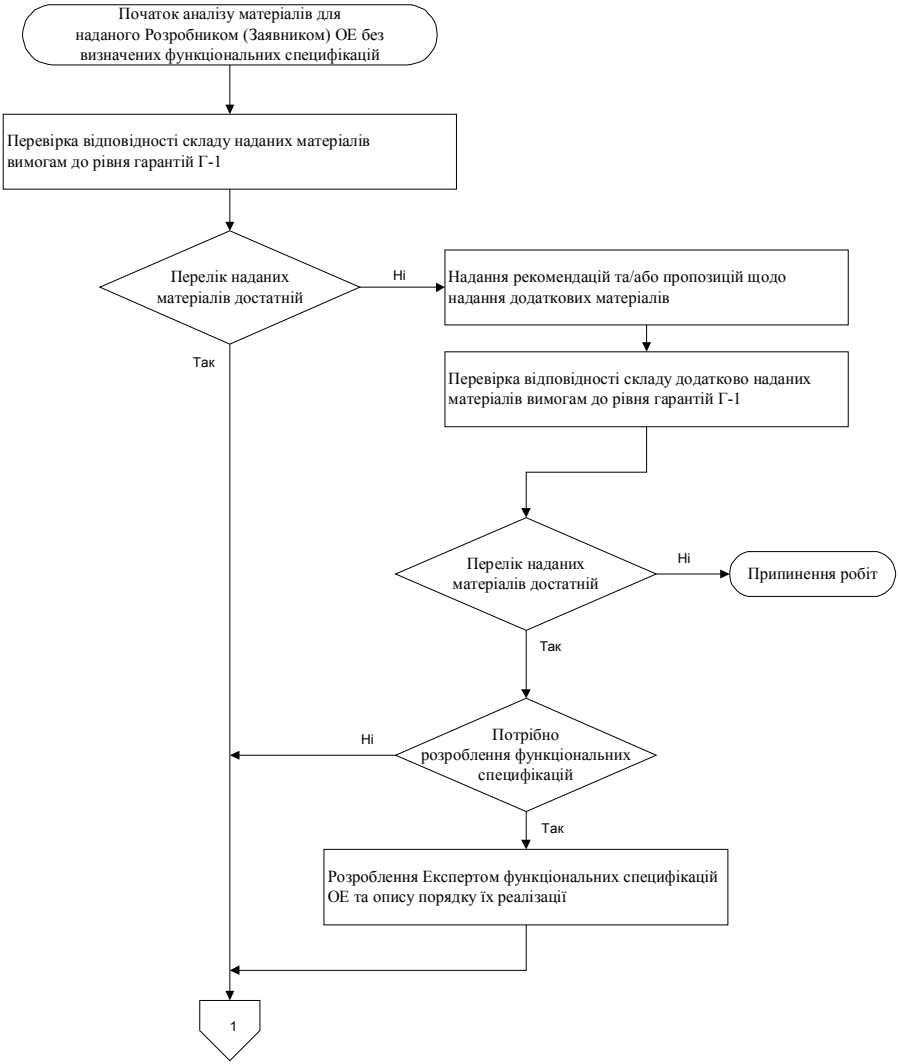


Рисунок 4 (частина 1)

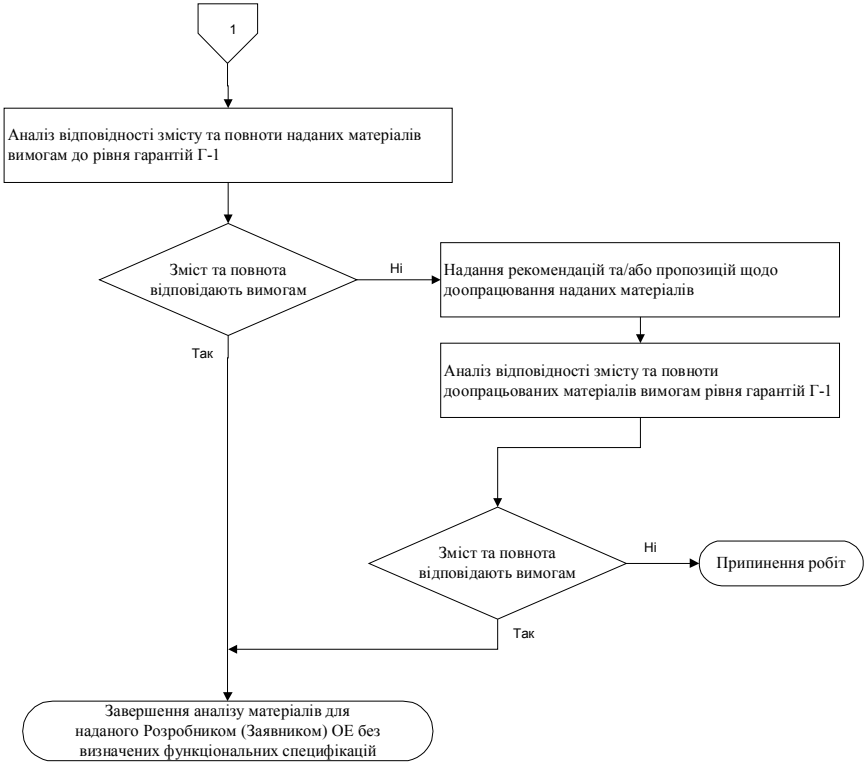


Рисунок 4 (частина 2)

6.4 Наведені в розділі А.1 Додатка А рекомендації щодо складу матеріалів (документів), які надаються для оцінювання рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ, викладено з урахуванням вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, до різних рівнів гарантій. При виконанні, з використанням зазначених рекомендацій, перевірки відповідності складу наданих розробником (заявником) матеріалів вимогам до заявленого рівня гарантій основні зусилля слід спрямувати на те, щоб чітко встановити відповідність між назвами окремих матеріалів (документів), наданими експерту, та типами документів, зазначеними в таблиці А.1. Для цього може бути доцільним проаналізувати зміст окремого документа та, з урахуванням рекомендацій щодо змісту документів певного типу, викладених у підрозділах розділу А.2, певним чином "класифікувати" проаналізований документ.

6.5 Наведені в розділі А.2 Додатка А рекомендації щодо змісту матеріалів (документів), які надаються для оцінювання рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ, викладено з урахуванням вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, до різних рівнів гарантій. При виконанні, з використанням зазначених рекомендацій, аналізу відповідності змісту наданих розробником (заявником) матеріалів вимогам до заявленого рівня гарантій основні зусилля слід спрямувати на те, щоб попередньо встановити, чи відповідають зміст та повнота викладення матеріалів у кожному окремому документі рекомендаціям, викладеним у підрозділах розділу А.2 для документів відповідного типу. При цьому особливу увагу слід приділяти:

- рівню деталізації певних відомостей щодо ОЕ в документі, який аналізується (наприклад, викладений опис порядку реалізації ФПБ на рівні підсистем або окремих модулів);
- ступеню формалізації наведених вимог або описів порядку функціонування компонентів КЗЗ ОЕ (неформалізований, частково формалізований або формалізований);
- використаному способу підтвердження відповідності специфікацій КЗЗ ОЕ різного

рівня деталізації та ступеня формалізації (показ, демонстрація, доказ).

6.6. При виконанні аналізу відповідності змісту наданих матеріалів вимогам до заявленого рівня гарантій доцільно з метою зменшення обсягу робіт там, де йдеться про проведення аналізу досить великої сукупності однорідних вхідних даних на відповідність однаковим вимогам (наприклад, при аналізі використовуваного стилю опису моделей політик різних ФПБ, вигляду представлення інтерфейсів різних компонентів КЗЗ ОЕ, стилю опису порядку захищеного функціонування різних компонентів КЗЗ ОЕ тощо), використовувати вибірку із зазначеної сукупності даних. Використання вибірки дозволить експерту пересвідчитися у задоволенні певних вимог без виконання аналізу всієї сукупності вхідних даних. При використанні вибірки слід дотримуватися таких рекомендацій:

- мінімальний обсяг вибірки має складати не менше 20% обсягу аналізованої сукупності даних;
- вибірка має бути репрезентативною по всіх аспектах, що стосуються сфери її застосування. Так, наприклад, при виконанні аналізу моделей політик ФПБ необхідно, щоб вибірка охоплювала ФПБ всіх типів (конфіденційності, цілісності, доступності та спостережності);
- відбір до вибірки має бути, по можливості, неупередженим, наприклад, не слід завжди обирати лише перший або останній елемент у переліку.

У випадку, якщо аналіз коректно зробленої вибірки дає позитивний результат, можна дійти висновку, що вся сукупність вхідних даних відповідає висунутим вимогам. У випадку негативного результату слід виконати аналіз кожного елемента сукупності та надавати рекомендації або робити висновки згідно з його результатами.

6.7 При документуванні отриманих результатів у проміжному звіті слід, крім фіксації уточненого рівня гарантій як такого, відповідність вимогам до якого має бути підтверджено в процесі експертизи:

- зазначити в ньому всі рекомендації та/або пропозиції щодо складу та змісту матеріалів, які було надано розробнику (заявнику);
- зазначити, відсутність та/або невідповідність встановленим вимогам яких саме документів (матеріалів) стало підставою для уточнення (зниження) рівня гарантій.

7 Методичні вказівки з розроблення та документування програми перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки

7.1 Оскільки основний зміст програми перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ має складати опис того відповідність яким саме вимогам критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, а також вимогам діючих НД ТЗІ має бути перевірено з метою підтвердження або спростування їх дотримання в процесі розроблення, виробництва та постачання ОЕ, основні зусилля повинні бути спрямовані на те, щоб максимально повно відобразити в ній перелік тих вимог (без наведення конкретних методів виконання їх перевірки), успішне виконання перевірки яких дозволить дійти обґрунтованого висновку про факт дотримання або недотримання вимог до заявленого рівня гарантій. Для цього розроблювана програма має передбачати перевірку:

- усіх вимог НД ТЗІ 2.5-004-99 до певного рівня гарантій коректності реалізації ФПБ, які мають бути дотримані в процесі розроблення, виробництва та постачання замовнику оцінюваного ОЕ, з урахуванням складу та змісту матеріалів (документів), наданих експерту розробником (заявником);
- усіх вимог НД ТЗІ 3.6-001-2000, які стосуються порядку взаємодії розробника ОЕ з уповноваженим державним органом на різних етапах створення ОЕ.

7.2 При розробленні програми перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ, залежно від заявленого (уточненого) рівня гарантій та варіанта подання ОЕ на експертизу, експерт має використовувати:

- проектну документацію на оцінюваний ОЕ, зазначену в пп. А.2.1-А.2.4 або аналогічну за змістом;
- супровідну документацію на оцінюваний ОЕ , зазначену в пп. А.2.5-А.2.12, А.2.14, А.2.18-А.2.20 або аналогічну за змістом;
- експлуатаційну документацію на оцінюваний ОЕ, зазначену в пп. А.2.13, А.2.15-А.2.17 або аналогічну за змістом;
- функціональні специфікації ОЕ та опис порядку їх реалізації, розроблені на етапі збирання та аналізу матеріалів або в процесі проведення робіт з оцінювання ФПБ.

Крім цього, при формулюванні вимог програми перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ рекомендується користуватися Додатком Б, в якому викладено вимоги щодо змісту програм перевірки дотримання вимог до різних рівнів гарантій. Викладені вимоги сформульовані з урахуванням вимог НД ТЗІ 2.5-004-99, НД ТЗІ 3.6-001-2000, а також результатів виконаного з використанням рекомендацій, наведених у розділі 6, аналізу матеріалів (документів), наданих експерту розробником (заявником).

7.3 При документуванні програми перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ, розробленої з урахуванням наведених вище та викладених у Додатку Б вимог, необхідно керуватися також вимогами Положення про державну експертизу в 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 підготовки та проведення випробувань.

8 Методичні вказівки з розроблення та документування методики перевірки дотримання вимог до рівня гарантій коректності реалізації функціональних послуг безпеки

8.1 Основний зміст методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ має складати виконаний з урахуванням вимог програми перевірки опис послідовності, порядку та методів виконання певних дій, метою яких є підтвердження або спростування факту дотримання вимог певного рівня гарантій у процесі розроблення, виробництва та постачання ОЕ. При цьому основні зусилля повинні бути спрямовані на те, щоб максимально повно відобразити в ній суть дій, виконуваних при перевірці окремих вимог, успішне виконання яких дозволить дійти обґрунтованого висновку про факт дотримання або недотримання вимог до заявленого рівня гарантій.

8.2 При розробленні методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ, залежно від заявленого (уточненого) рівня гарантій та варіанта подання ОЕ на експертизу, експерт має використовувати:

- проектну документацію на оцінюваний ОЕ, зазначену в пп. А.2.1-А.2.4 або аналогічну за змістом;
- супровідну документацію на оцінюваний ОЕ , зазначену в пп. А.2.5-А.2.12, А.2.14, А.2.18-А.2.20 або аналогічну за змістом;
- експлуатаційну документацію на оцінюваний ОЕ, зазначену в пп. А.2.13, А.2.15-А.2.17 або аналогічну за змістом;
- функціональні специфікації ОЕ та опис порядку їх реалізації, розроблені на етапі збирання та аналізу матеріалів або в процесі робіт з оцінювання ФПБ;
- розроблену програму перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ.

Крім цього, при розробленні методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ рекомендується користуватися Додатком В, в якому викладено вимоги до змісту методик перевірки дотримання вимог до різних рівнів гарантій. Викладені вимоги сформульовані з урахуванням вимог НД ТЗІ 2.5-004-99, НД ТЗІ 3.6-001-2000, результатів виконаного з використанням рекомендацій, наведених у розділі 6, аналізу матеріалів (документів), наданих експерту розробником (заявником), а також вимог щодо змісту програм перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ, викладених у Додатку Б. Вимоги викладено з урахуванням необхідності забезпечення максимальної незалежності процедур перевірки окремих вимог критеріїв гарантій щодо архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань ОЕ.

8.3 При документуванні методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ, розробленої з урахуванням наведених вище та викладених у Додатку В вимог, необхідно керуватися також вимогами Положення про державну експертизу в 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 підготовки та проведення випробувань.

9 Методичні вказівки з виконання оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки

9.1 Безпосередньо процес оцінювання ОЕ на відповідність вимогам до рівня гарантій

коректності реалізації ФПБ являє собою послідовне виконання необхідних дій згідно з пунктами затвердженої методики перевірки рівня гарантій, з формулюванням та фіксацією висновків експерта, що стосуються результатів виконання певних пунктів методики. Зазначені дії, залежно від заявленого (уточненого) рівня гарантій та варіанта подання ОЕ на експертизу, виконуються з використанням:

- оцінюваного ОЕ в працездатному стані;
- проектної документації на оцінюваний ОЕ, зазначеної в пп. А.2.1-А.2.4 або аналогічної за змістом;
- супровідної документації на оцінюваний ОЕ, зазначеної в пп. А.2.5-А.2.12, А.2.14, А.2.18-А.2.20 або аналогічної за змістом;
- експлуатаційної документації на оцінюваний ОЕ, зазначеної в пп. А.2.13, А.2.15-А.2.17 або аналогічної за змістом;
- функціональних специфікацій ОЕ та опис порядку їх реалізації, розроблених на етапі збирання та аналізу матеріалів або в процесі робіт з оцінювання ФПБ;
- розробленої методики перевірки дотримання вимог до рівня гарантій коректності реалізації ФПБ.

9.2 Дії з оцінювання можуть виконуватися як в умовах випробувальної лабораторії, в якій розгорнуто оцінюваний ОЕ, так і (за необхідності) безпосередньо в умовах підприємства – розробника ОЕ. При цьому основними діями, які виконуються експертом у процесі виконання певних пунктів методики, є:

- перевірка зібраних (одержаних) матеріалів з метою формулювання висновку про їх відповідність висунутим вимогам;
- дослідження зібраних (одержаних) матеріалів з метою формулювання обґрунтованого висновку про їх відповідність висунутим вимогам;
- верифікації змісту зібраних (одержаних) матеріалів з метою формулювання висновку про коректність наведених доказів.

9.3 Перевірка матеріалів з метою формулювання висновку про їх відповідність висунутим вимогам передбачає виконання простого порівняння змісту матеріалів з висунутими вимогами, без залучення спеціальних знань та досвіду експерта. Висновки, які формулюються за результатами виконаної перевірки, повинні містити лише результати виконаної перевірки без їх обґрунтування.

9.4 Дослідження матеріалів з метою формулювання обґрунтованого висновку про відповідність висунутим вимогам передбачає виконання поглибленого аналізу змісту матеріалів на предмет відповідності висунутим вимогам, з використанням спеціальних знань та досвіду експерта. Висновки, які формулюються за результатами виконаного дослідження, повинні містити як результати проведеного аналізу, так і їх обґрунтування, яке містить аргументацію на користь зроблених висновків.

9.5 Верифікація змісту матеріалів з метою формулювання висновку про коректність наведених доказів передбачає докладне дослідження змісту матеріалів для прийняття рішення про достатність наведених у них аргументів на користь коректності доказів. Висновки, які формулюються за результатами виконаної верифікації, повинні містити висновки про коректність наведених доказів, а у випадку, якщо докази визнані некоректними – аргументи на користь таких висновків.

9.6 При виконанні окремих пунктів методики перевірки рівня гарантій, які стосуються перевірки дотримання вимог певних рівнів гарантій до реалізованих розробником заходів щодо забезпечення безпеки в процесі розроблення та виробництва ОЕ, використання системи керування конфігурацією ОЕ та процедур постачання ОЕ замовнику, експерту слід користуватися рекомендаціями, викладеними в Додатку Г. Ці рекомендації сформульовані з урахуванням відповідних вимог критеріїв гарантій, викладених у НД ТЗІ 2.5-004-99, та стосуються як організації робіт експерта при відвідуванні підприємства – розробника ОЕ, так і порядку виконання певних дій, пов'язаних з перевіркою вимог критеріїв гарантій.

9.7 При виконанні окремих пунктів методики перевірки рівня гарантій, які стосуються перевірки дотримання вимог до моделі політики безпеки, яка реалізується КЗЗ оцінюваного ОЕ, слід користуватися рекомендаціями, викладеними в Додатку Д. Ці рекомендації сформульовані з урахуванням вимог критеріїв гарантій, викладених у НД ТЗІ 2.5-004-99, щодо змісту моделей політики безпеки та стосуються основних дій, які має виконувати експерт у процесі проведення аналізу таких моделей.

9.8 При виконанні окремих пунктів методики перевірки рівня гарантій, які стосуються

перевірки відповідності специфікацій КЗЗ ОЕ різного рівня деталізації (політика безпеки, модель політики безпеки, проект архітектури, детальний проект, реалізація) та ступеня формалізації, слід користуватися рекомендаціями, викладеними в Додатку Е. Ці рекомендації сформульовані з урахуванням вимог критеріїв гарантій, викладених у НД ТЗІ 2.5-004-99, щодо підтвердження відповідності специфікацій КЗЗ ОЕ різного рівня деталізації та ступеня формалізації та стосуються основних дій, які має виконувати експерт у процесі проведення такої перевірки.

9.9 При виконанні вибіркової перевірки результатів випробувань необхідно дотримуватися таких правил:

- мають бути перевірені результати проведених випробувань всіх ФПБ, реалізація яких є обов'язковою згідно з вимогами НД ТЗІ 2.5-004-99 ("Цілісність КЗЗ", "Реєстрація", "Розподіл обов'язків", "Ідентифікація та автентифікація"), а також тих ФПБ, реалізація яких є необхідною умовою для реалізації зазначених ФПБ;
- мають бути перевірені результати проведених випробувань не менше 20% ФПБ, реалізація яких не є обов'язковою згідно з вимогами НД ТЗІ 2.5-004-99;
- сукупність ФПБ, результати випробувань яких підлягають перевірці, повинна, за можливості, в однаковій мірі містити ФПБ всіх типів (конфіденційності, цілісності, доступності та спостережності).

9.10 Сформульовані експертом висновки, що стосуються результатів виконання перевірок згідно з різними пунктами методики, повинні фіксуватися в журналі проведення перевірок, форма ведення якого може бути аналогічною формі журналу випробувань, встановленій ДСТУ 2851-94. У цьому журналі повинні фіксуватися як висновки експерта, так і (безпосередньо або шляхом посилання на зібрані матеріали) аргументи, на підставі яких були зроблені відповідні висновки.

10 Методичні вказівки з виконання аналізу та документування результатів оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки

10.1 Оскільки головною метою цього етапу є підготовка обґрунтування для прийняття рішення щодо відповідності або невідповідності оцінюваного ОЕ вимогам щодо заявленого рівня гарантій, у першу чергу в процесі виконання аналізу отриманих та зафіксованих у журналі проведення перевірок результатів необхідно врахувати такі вимоги:

- умовою прийняття позитивного висновку про відповідність вимогам критеріїв до певного рівня гарантій стосовно вимог до архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань є наявність висновків про успішне виконання всіх дії з оцінювання, які передбачені методикою перевірки дотримання відповідних вимог;
- умовою прийняття позитивного висновку про відповідність оцінюваного ОЕ вимогам критеріїв до певного рівня гарантій у цілому є наявність висновків про відповідність вимогам цього або більш високого рівня гарантій стосовно вимог до архітектури, середовища розробки, послідовності розробки, середовища функціонування, документації та випробувань;
- якщо результати проведених перевірок не дають підстав дійти висновку про дотримання вимог певного рівня гарантій, але підтверджують дотримання вимог більш низького рівня гарантій, то саме цей більш низький рівень гарантій має призначатися оцінюваному ОЕ за результатами експертизи.

10.2 При документуванні результатів перевірки рівня гарантій у відповідних протоколах мають бути викладені, з посиланням на відповідні пункти затвердженої методики та зібрані матеріали:

- результати виконання відповідних дій з оцінювання згідно з пунктами методики;
- підстави, які дають або не дають можливості дійти висновку щодо успішності або неуспішності здійснення певних дій з оцінювання;
- висновки щодо підтвердження або не підтвердження фактів дотримання при розробленні, виробництві та постачанні замовнику вимог заявленого (уточненого) рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ.

10.3 При оформленні 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, які стосуються документування результатів випробувань.

Додаток А
Рекомендації щодо складу та змісту матеріалів (документів), які надаються для оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки (рекомендований)

У Додатку А викладені рекомендації щодо складу та змісту матеріалів (документів), які надаються експерту для використання в процесі оцінювання рівня гарантій коректності реалізації ФПБ в ОЕ. Рекомендації викладені з урахуванням вимог критеріїв гарантій, наведених у НД ТЗІ 2.5-004-99, а також з урахуванням методичних рекомендацій зі збирання та аналізу матеріалів, що характеризують організацію процесу розроблення, виробництва та постачання замовнику оцінюваного ОЕ, наведених у розділі 6. У п. А.1 наведено рекомендований склад матеріалів (документів), які, відповідно до заявленого рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ, повинні бути підготовлені та надані експерту заявником експертизи (розробником ОЕ). У п. А.2 наведені рекомендації щодо змісту окремих документів, відповідно до заявленого рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ.

А.1 Рекомендований склад матеріалів (документів), які надаються експерту

Рекомендований склад матеріалів (документів), які повинні бути підготовлені та надані експерту заявником експертизи (розробником ОЕ), наведено в таблиці А.1.

Таблиця А.1

№ з/п	Тип документа	Заявлений рівень гарантій коректності реалізації ФПБ						
		Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
1	Технічне завдання (що містить функціональні специфікації КЗЗ ОЕ)	+	+	+	+	=	=	=
2	Ескізний проект (що містить проект архітектури)	+	=	+	=	+	+	=
3	Технічний проект (що містить детальний проект)	+	+	=	+	=	=	+
4	Робочий проект (реалізація)			+	=	+	=	+
5	Опис результатів аналізу відповідності між політикою безпеки та моделлю політики безпеки КЗЗ ОЕ		+	=	+	=	=	=
6	Опис результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури		+	=	=	+	+	=
7	Опис результатів аналізу відповідності між проектом архітектури та детальним проектом		+	=	=	=	+	+
8	Опис результатів аналізу відповідності між детальним проектом та реалізацією			+	=	=	=	+
9	Опис методик діяльності розробника протягом життєвого циклу ОЕ	+	=	=	=	=	=	=
10	Документація використовуваних при розробленні інструментальних засобів			+	=	=	=	=
11	Опис методик забезпечення безпеки в процесі розроблення та виробництва ОЕ				+	=	+	=
12	Документація з керування конфігурацією ОЕ	+	=	=	+	=	=	=
13	Опис процедур безпечної інсталяції, генерації та запуску ОЕ	+	=	=	=	=	=	=
14	Опис процедур постачання ОЕ замовнику			+	=	=	+	=
15	Опис послуг безпеки, що реалізуються КЗЗ оцінюваного ОЕ	+	=	=	=	=	=	=
16	Настанови адміністратору з послуг безпеки	+	=	=	=	=	=	=
17	Настанови користувачу з послуг безпеки	+	=	=	=	=	=	=
18	Програма та методика випробувань функціональних послуг безпеки	+	=	=	=	=	=	=
19	Протоколи випробувань функціональних послуг безпеки	+	+	=	=	=	=	=

№ з/п	Тип документа	Заявлений рівень гарантій коректності реалізації ФПБ						
		Г-1	Г-2	Г-3	Г-4	Г-5	Г-6	Г-7
20	Опис результатів аналізу стійкості КЗЗ до атак з боку розробника				+	=	+	=

Примітка. У таблиці використовуються такі позначення: "+" – вимога до змісту документа з'являється або підвищується; "=" – вимога до змісту документа зберігається.

Вимоги до складу наданих матеріалів (документів) ранжовані залежно від заявленого рівня гарантій коректності реалізації ФПБ в оцінюваному ОЕ. Зазначені в таблиці найменування документів не є обов'язковими, допускається об'єднання схожих за змістом документів в один (наприклад, в один документ можуть бути об'єднані всі описи результатів аналізу відповідності специфікацій КЗЗ ОЕ різного рівня деталізації та ступеня формалізації).

А.2 Рекомендації щодо змісту матеріалів (документів), які надаються експерту

А.2.1 Технічне завдання (що містить функціональні специфікації КЗЗ ОЕ)

А.2.1.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, чи розробником виконано адекватний опис функціональних специфікацій КЗЗ оцінюваного ОЕ. Функціональні специфікації повинні описувати, які ФПБ реалізує КЗЗ оцінюваного ОЕ при мінімумі або повній відсутності інформації про те, як саме вони реалізуються. Функціональні специфікації подаються у вигляді неформалізованого опису реалізованої політики безпеки, а також (для заявлених рівнів гарантій Г-2 та вище) опису моделі політики безпеки різного ступеня формалізації.

А.2.1.2 Для заявлених рівнів гарантій Г-1 ... Г-7 наданий неформалізований опис реалізованої політики безпеки має описувати КЗЗ ОЕ як набір вимог до реалізованих ним ФПБ. Вимоги до кожної ФПБ мають бути викладені відповідно до вимог НД ТЗІ 2.5-004-99 для визначеного рівня цієї ФПБ та з урахуванням необхідних умов. Вимоги мають бути викладені неформалізованим чином, у вигляді тексту оригінальною мовою спілкування. При цьому не повинні використовуватися жодні нотаційні або спеціальні обмеження, відмінні від загальноприйнятих правил використовуваної мови. Використовувана термінологія повинна відповідати вимогам НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99.

А.2.1.3 Опис моделі політики безпеки, реалізованої КЗЗ оцінюваного ОЕ, має містити чіткі та несуперечливі описи правил та характеристик політик реалізованих ФПБ різного ступеня формалізації, а також відображати характеристики модельованого режиму захищеного функціонування КЗЗ ОЕ.

Наприклад:

- *для ФПБ, реалізованих з використанням механізмів керування доступом (довірча/адміністративна конфіденційність або цілісність), у моделі мають бути описані інформаційні ресурси, які підлягають захисту (у вигляді об'єктів КЗЗ певного типу), умови та правила, при дотриманні яких користувачу має надаватися доступ до цих ресурсів (об'єктів);*
- *для ФПБ "Реєстрація" мають бути описані події, які потенційно підлягають аудиту, а також правила реєстрації відповідних подій у журналах реєстрації КЗЗ;*
- *для ФПБ "Ідентифікація та автентифікація" мають бути описані атрибути, з використанням яких виконуються ідентифікація та автентифікація користувачів, а також правила (порядок) виконання автентифікації.*

А.2.1.4 Для заявленого рівня гарантій Г-2 наданий опис моделі політики безпеки, реалізованої КЗЗ оцінюваного ОЕ, має бути неформалізованим, тобто викладеним у вигляді тексту оригінальною мовою спілкування. Для термінів, використання яких у контексті наданої моделі відрізняється від загальноприйнятого (у тому числі наведеного в НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99), повинно наводитися визначення відповідних термінів.

А.2.1.5 Для заявленого рівня гарантій Г-3 наданий опис моделі політики безпеки, реалізованої КЗЗ оцінюваного ОЕ, має бути частково формалізованим, тобто викладеним у вигляді тексту мовою з обмеженим синтаксисом, що супроводжується допоміжними поясненнями, поданими в неформалізованому вигляді. При цьому, як таку мову з обмеженим синтаксисом доцільно використовувати природну мову з обмеженою структурою речень та ключових слів зі спеціальними

значеннями. Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей, які дозволяють визначити обмеження, що накладаються на синтаксис використовуваної мови.

А.2.1.6 Для заявлених рівнів гарантій Г-4 … Г-7 наданий опис моделі політики безпеки, реалізованої КЗЗ оцінюваного ОЕ, має бути формалізованим, тобто викладеним з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях та супроводжуваної допоміжними поясненнями, поданими в неформалізованому вигляді. Використовувані математичні поняття мають забезпечувати визначення синтаксису та семантики представлення об'єктів КЗЗ, їх критичних для безпеки властивостей та виконуваних над ними операцій. Формалізована модель ФПБ повинна описувати як результат виконання певної ФПБ, так і всі пов'язані з нею виняткові або помилкові умови. Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей (правил), що визначають використовувану нотацію, а також правила доказу, які підтримують логічну аргументацію.

А.2.1.7 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-3 … Г-7, надане експерту технічне завдання, що містить функціональні специфікації КЗЗ ОЕ, має бути погоджене з уповноваженим державним органом.

А.2.2 Ескізний проект (що містить проект архітектури)

А.2.2.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, чи виконано розробником на стадії розробки ескізного проекту ОЕ розроблення проекту архітектури КЗЗ ОЕ, який містить всі необхідні для виконання експертизи відомості, а також чи забезпечує КЗЗ ОЕ задоволення вимог функціональних специфікацій та чи структурований він відповідним чином.

А.2.2.2 Проект архітектури КЗЗ ОЕ має містити опис КЗЗ у термінах основних функціональних компонентів (підсистем) та зв'язувати ці компоненти (підсистеми) з тими ФПБ, які вони реалізують. Проект архітектури КЗЗ ОЕ має показувати, що ОЕ та його КЗЗ мають архітектуру, яка дозволяє реалізувати заявлені функціональні специфікації КЗЗ оцінюваного ОЕ. Для кожного функціонального компонента (підсистеми) проект архітектури має описувати його призначення та функціональні можливості в частині, що стосується реалізації ФПБ.

Примітка. Стосовно проекту архітектури КЗЗ ОЕ, термін "підсистема" належить до великих зв'язаних функціональних компонентів (наприклад, засоби керування пам'яттю, керування файлами, керування процесами). Розподіл проекту на базові функціональні компоненти сприяє його розумінню. Функціональні компоненти, які використовуються в описі проекту архітектури, не обов'язково мають називатися "підсистемами", але вони мають представляти подібний рівень декомпозиції. Наприклад, при декомпозиції проекту можуть використовуватися поняття "шари" або "менеджери".

А.2.2.3 Проект архітектури має визначати всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ, з описом функцій, які підтримуються механізмами захисту, реалізованими цими засобами. У проекті архітектури також мають бути визначені взаємозв'язки між всіма функціональними компонентами (підсистемами). Ці взаємозв'язки мають бути представлені на рівні зовнішніх інтерфейсів підсистем, потоків даних, керування тощо. Мають бути чітко зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ, які є видимими ззовні КЗЗ. Представлення інтерфейсів функціональних компонентів (підсистем) КЗЗ має містити опис призначення, методів використання інтерфейсів, повідомлень про помилки та кодів повернення, забезпечуючи, де це необхідно, деталізацію результатів та можливих позаштатних ситуацій (винятків). Проект архітектури має містити опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ – опис того, що саме робить компонент (підсистема) КЗЗ при функціонуванні в складі КЗЗ. Цей опис має містити опис будь-яких операцій, виконання яких може бути доручено функціональному компоненту (підсистемі) КЗЗ, з точки зору його функцій та впливу, який може здійснити цей компонент (підсистема) КЗЗ на захищений стан ОЕ (наприклад, зміна атрибутів об'єктів-користувачів, об'єктів-процесів або пасивних об'єктів). Опис порядку захищеного функціонування компонента (підсистеми) КЗЗ має викладатися в термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс. Аналогічно мають бути описані всі використовувані зовнішні послуги безпеки (послуги, реалізовані функціональними компонентами, що не входять до складу КЗЗ ОЕ).

А.2.2.4 Для заявлених рівнів гарантій Г-1 … Г-2 проект архітектури має бути викладений у

неформалізованому вигляді, тобто, опис порядку захищеного функціонування компонентів (підсистем) КЗЗ має бути викладений у вигляді тексту оригінальною мовою спілкування.

А.2.2.5 Для заявлених рівнів гарантій Г-3 … Г-5 проект архітектури має бути викладений у частково формалізованому вигляді, тобто, опис порядку захищеного функціонування компонентів (підсистем) КЗЗ має бути викладений мовою з обмеженим синтаксисом у вигляді тексту, супроводжуваного допоміжними поясненнями, наданими у неформалізованому вигляді. Як така мова може бути використана оригінальна мова з обмеженою структурою речень та ключових слів зі спеціальними значеннями, а також мова діаграм (наприклад, діаграм потоків команд, потоків даних або станів переходу). Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей, які дозволяють визначити обмеження, що накладаються на синтаксис використовуваної мови.

А.2.2.6 Для заявлених рівнів гарантій Г-6 … Г-7 проект архітектури має бути викладений у формалізованому вигляді, тобто, опис порядку захищеного функціонування компонентів (підсистем) КЗЗ має бути викладений з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях та супроводжуваної допоміжними поясненнями, наданими в неформалізованому вигляді. Використовувані математичні поняття мають забезпечувати визначення синтаксису та семантики представлення об'єктів КЗЗ, їх критичних для безпеки властивостей та виконуваних над ними операцій. У формалізованому описі мають бути відображені як послідовність, так і результати виконання різних операцій у функціональних компонентах (підсистемах) КЗЗ та всі пов'язані з їх виконанням виняткові або помилкові умови. Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей (правил), що визначають використовувану нотацію.

А.2.2.7 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-5 … Г-7 надані експерту матеріали ескізного проекту, що містять проект архітектури КЗЗ ОЕ, мають бути погоджені з уповноваженим державним органом.

А.2.3 Технічний проект (що містить детальний проект)

А.2.3.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, чи виконано розробником на стадії розробки технічного проекту ОЕ розроблення детального проекту КЗЗ ОЕ, який містить усі необхідні для виконання експертизи відомості, чи забезпечує КЗЗ задоволення вимог функціональних специфікацій та чи є він коректним та ефективним уточненням проекту архітектури.

А.2.3.2 Детальний проект КЗЗ ОЕ має містити деталізовану проектну специфікацію, яка уточнює проект архітектури до такого рівня деталізації, що може бути використана як основа для програмування та/або проектування апаратури. Детальний проект КЗЗ має містити опис КЗЗ у термінах структурних компонентів (модулів), їх взаємозв'язків та залежностей. Для кожного структурного компонента (модуля) КЗЗ детальний проект має описувати його призначення, функції, інтерфейси, залежності від інших модулів та порядок реалізації всіх ФПБ, до яких має відношення цей компонент (у тому числі алгоритми реалізації механізмів захисту, необхідні для розуміння порядку їх реалізації внутрішні структури даних та інтерфейси), а також порядок взаємодії з іншими модулями.

Примітка. Стосовно детального проекту КЗЗ ОЕ, термін "модуль" використовується для позначення менш абстрактної сутності, ніж підсистема, яка максимально наближена до кінцевої реалізації. Це означає, що детальний проект містить більше подробиць стосовно не лише цілей функціонування кожного модуля, а також і щодо способу досягнення цим модулем відповідних цілей. В ідеалі, в детальному проекті має бути наведена вся інформація, необхідна для реалізації описаних у ньому модулів. Структурні компоненти (модулі) КЗЗ не обов'язково однозначно ототожнюються з конкретними ФПБ, реалізованими КЗЗ. Кожен конкретний модуль може цілком реалізовувати як одну, так і декілька ФПБ. Можливим є також випадок, коли кілька модулів спільно реалізують одну ФПБ.

А.2.3.3 Детальний проект, за необхідності, може уточнювати базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ. Детальний проект має містити опис призначення кожного структурного компонента (модуля) КЗЗ ОЕ. Цей опис має бути настільки чітким, щоб відобразити, виконання яких функцій передбачається відповідним модулем. У детальному проекті мають бути однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), які входять до складу КЗЗ. Ці взаємозв'язки мають бути представлені на

рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо. Мають бути визначені всі інтерфейси структурних компонентів (модулів) КЗЗ, а також зазначені ті інтерфейси, які є видимими ззовні КЗЗ. Представлення інтерфейсів структурних компонентів (модулів) КЗЗ має містити імена точок входу, опис призначення, методів використання та параметрів інтерфейсів, результатів, повідомлень про помилки та кодів повернення. Детальний проект має містити опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ, а для заявленого рівня гарантій Г-1 – лише тих модулів, що мають безпосереднє відношення до реалізації ФПБ та інтерфейси яких є видимими ззовні КЗЗ. Опис порядку захищеного функціонування структурного компонента (модуля) має містити опис того, що саме робить структурний компонент (модуль) КЗЗ при взаємодії з іншими компонентами (модулями), які функціонують у складі КЗЗ, при реалізації різних ФПБ. При розгляді спільного з іншими модулями функціонування доцільно розглядати два способи взаємодії модулів: надання послуг один одному та/або спільне функціонування при реалізації ФПБ. У детальному проекті має бути відображена конкретна інформація про ці взаємозв'язки (наприклад, якщо модуль виконує обчислення, які залежать від результатів обчислень, виконуваних іншими модулями, останні мають бути перелічені). Опис режиму захищеного функціонування структурного компонента (модуля) КЗЗ має викладатися в термінах послідовностей дій, які виконуються в компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс.

А.2.3.4 Для заявлених рівнів гарантій Г-1 … Г-3 детальний проект має бути представлений у неформалізованому вигляді, тобто, опис порядку захищеного функціонування компонентів (підсистем) КЗЗ має бути викладений у вигляді тексту оригінальною мовою спілкування.

А.2.3.5 Для заявлених рівнів гарантій Г-4 … Г-6 детальний проект має бути представлений у частково формалізованому вигляді, тобто, опис порядку захищеного функціонування структурних компонентів (модулів) КЗЗ має бути викладений мовою з обмеженим синтаксисом у вигляді тексту, супроводжуваного допоміжними поясненнями, представленими в неформалізованому вигляді. Як така мова може бути використана оригінальна мова з обмеженою структурою речень та ключових слів зі спеціальними значеннями, а також мова діаграм (наприклад, діаграм потоків команд, потоків даних або станів переходу). Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей, які дозволяють визначити обмеження, що накладаються на синтаксис використовуваної мови.

А.2.3.6 Для заявленого рівня гарантій Г-7 детальний проект має бути представлений у формалізованому вигляді, тобто, опис порядку захищеного функціонування структурних компонентів (модулів) КЗЗ має бути викладений з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях та супроводжуваної допоміжними поясненнями, представленими в неформалізованому вигляді. Використовувані математичні поняття мають забезпечувати визначення синтаксису та семантики представлення об'єктів КЗЗ, їх критичних для безпеки властивостей та виконуваних над ними операцій. У формалізованому описі мають бути відображені як послідовність та результати виконання різних операцій у структурних компонентах (модулях) КЗЗ, так і всі пов'язані з їх виконанням виняткові або помилкові умови. Обов'язково має бути наведений (явно або у вигляді посилання) використовуваний набір домовленостей (правил), що визначають використовувану нотацію.

А.2.3.7 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-5 … Г-7 надані експерту матеріали технічного проекту, що містять детальний проект КЗЗ ОЕ, мають бути погоджені з уповноваженим державним органом.

А.2.4 Робочий проект (реалізація)

А.2.4.1 Надані розробником матеріали робочого проекту (реалізації) повинні дозволити експерту дійти висновку про те, чи є реалізація КЗЗ ОЕ коректною реалізацією вимог детального проекту та чи забезпечується при цьому задоволення вимог функціональних специфікацій.

А.2.4.2 Робочий проект (реалізація) є завершальним представленням ОЕ, яке складається з програмного, програмно-апаратного та апаратного забезпечення. Кожен компонент робочого проекту (реалізації) має бути створений та документований відповідно до вимог процесу проектування. Якщо ОЕ являє собою програмний засіб, то представленням робочого проекту (реалізації) є вхідний код реалізації структурних компонентів (модулів) ОЕ. Якщо ОЕ являє собою програмно-апаратний або апаратний виріб, то представленням робочого проекту (реалізації) є також графічні представлення (принципові схеми, креслення друкованих плат тощо) компонентів (модулів) ОЕ. У будь-якому випадку представлення робочого проекту (реалізації) можуть вважатися

придатними для аналізу лише тоді, коли процес одержання (компонування) з них екземпляра ОЕ є цілком визначеним та не вимагає подальших проектних рішень (наприклад, потрібна лише компіляція вхідного коду або побудова апаратних засобів на основі креслень апаратних засобів).

А.2.4.3 Для заявлених рівнів гарантій Г-3 ... Г-4 у складі матеріалів робочого проекту (реалізації) має надаватися вхідний код реалізації частини структурних компонентів (модулів) КЗЗ. Обсяг переданого вхідного коду має бути достатнім для того, щоб дозволити експерту дійти обґрунтованого висновку про те, що одержані (скомпоновані) з наданого вхідного коду структурні компоненти (модулі) КЗЗ коректно, у повному обсязі та відповідно до визначеного в детальному проекті порядку їх захищеного функціонування реалізують вимоги функціональної специфікації.

А.2.4.4 Для заявлених рівнів гарантій Г-5 ... Г-6 у складі матеріалів робочого проекту (реалізації) має надаватися вхідний код реалізації всіх структурних компонентів (модулів) КЗЗ.

А.2.4.5 Для заявленого рівня гарантій Г-7 у складі матеріалів робочого проекту (реалізації) має надаватися вхідний код реалізації всіх структурних компонентів (модулів) КЗЗ, а також вхідний код усіх бібліотек часу виконання операційної системи (ядра операційної системи), що використовуються у процесі функціонування всіх структурних компонентів (модулів) КЗЗ.

А.2.4.6 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-5 … Г-7 надані експерту матеріали робочого проекту, що містять реалізацію КЗЗ ОЕ, мають бути погоджені з уповноваженим державним органом.

А.2.5 Опис результатів аналізу відповідності між політикою безпеки та моделлю політики безпеки КЗЗ ОЕ

А.2.5.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що в моделі політики безпеки, реалізованої КЗЗ ОЕ, адекватно та несуперечливо відображені вимоги політики безпеки.

А.2.5.2 Для підтвердження такої адекватності та несуперечності в описі результатів аналізу відповідності між політикою безпеки та моделлю політики безпеки КЗЗ ОЕ мають бути наведені аргументи, які підтверджують, що правила та характеристики політик реалізованих ФПБ, викладені в моделі політики безпеки відповідного ступеня формалізації, реалізованої КЗЗ ОЕ, ідентифікують ті ж самі правила та атрибути, що наведені в описі реалізованої політики безпеки (у вигляді набору вимог до ФПБ, реалізованих КЗЗ ОЕ).

А.2.5.3 Для заявлених рівнів гарантій Г-2 ... Г-3 відповідність між політикою безпеки та моделлю політики безпеки КЗЗ ОЕ має бути показана неформальним чином. При цьому необхідно показати наявність відповідності тільки між характеристиками основних елементів політики безпеки та моделі політики безпеки, а саме – переліком реалізованих ФПБ, переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу. Опис відповідності може бути викладений як в оповідній формі, так і, наприклад, у вигляді таблиці.

А.2.5.4 Для заявлених рівнів гарантій Г-4 ... Г-7 відповідність між політикою безпеки та моделлю політики безпеки КЗЗ ОЕ має бути продемонстрована, тобто, показана з використанням результатів структурованого аналізу. При цьому необхідно показати наявність відповідності між характеристиками всіх елементів політики безпеки та моделі політики безпеки, а саме – переліком реалізованих ФПБ, переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу. Опис відповідності має бути викладений з використанням, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями, які містять аргументи на користь того, що існує повна відповідність між елементами двох розглянутих специфікацій КЗЗ ОЕ. При викладенні таких пояснень варто прагнути до зменшення неоднозначності, яка може існувати при неформальному показі відповідності, наприклад, обмежуючи інтерпретацію використовуваних термінів.

А.2.6 Опис результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури

А.2.6.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що при розробленні проекту архітектури КЗЗ ОЕ розробником адекватно та несуперечливо реалізовані вимоги моделі політики безпеки.

Для підтвердження такої адекватності та несуперечності в описі результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури мають бути наведені аргументи, які підтверджують, що функціональними компонентами (підсистемами) КЗЗ ОЕ в процесі їх захищеного функціонування згідно з порядком, викладеним у проекті архітектури, забезпечується реалізація правил та характеристик політик реалізованих ФПБ, викладених у моделі політики безпеки відповідного ступеня формалізації.

А.2.6.2 Для заявлених рівнів гарантій Г-2 ... Г-4 відповідність між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури має бути показана неформальним чином. При цьому необхідно показати наявність відповідності тільки між характеристиками основних елементів моделі політики безпеки та характеристиками основних функціональних компонентів (підсистем) КЗЗ ОЕ, а саме – переліком реалізованих ФПБ, переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ та підсистем КЗЗ) атрибутами об'єктів КЗЗ різного типу. Опис відповідності може бути викладений як в оповідній формі, так і, наприклад, у вигляді таблиці.

А.2.6.3 Для заявленого рівня гарантій Г-5 відповідність між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури має бути продемонстрована, тобто, показана з використанням результатів структурованого аналізу. При цьому необхідно показати наявність відповідності між характеристиками всіх елементів моделі політики безпеки та характеристиками всіх функціональних компонентів (підсистем) КЗЗ ОЕ, а саме – переліком реалізованих ФПБ, переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу. Опис відповідності має бути викладений з використанням, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями, які містять аргументи на користь того, що існує повна відповідність між елементами двох розглянутих специфікацій КЗЗ ОЕ. При викладенні таких пояснень варто прагнути до зменшення неоднозначності, яка може існувати при неформальному показі відповідності, наприклад, обмежуючи інтерпретацію використовуваних термінів.

А.2.6.4 Для заявлених рівнів гарантій Г-6 … Г-7 відповідність між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури має бути доведена, тобто, виражена формально, з використанням відомих математичних понять для визначення синтаксису і семантики формалізованої нотації та правил доказів, які підтримують логічну аргументацію. При цьому, додатково до результатів демонстрації відповідності між характеристиками всіх елементів моделі політики безпеки та характеристиками всіх функціональних компонентів (підсистем) КЗЗ ОЕ, що наводяться для заявленого рівня гарантій Г-5, мають бути наведені формальні докази відповідності між правилами реалізації ФПБ та порядком захищеного функціонування підсистем КЗЗ, викладеними, відповідно, у моделі політики безпеки КЗЗ ОЕ і проекті архітектури.

А.2.7 Опис результатів аналізу відповідності між проектом архітектури та детальним проектом

А.2.7.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що при розробленні детального проекту КЗЗ ОЕ розробником адекватно та несуперечливо реалізовані вимоги проекту архітектури.

Для підтвердження такої адекватності та несуперечності в описі результатів аналізу відповідності між проектом архітектури та детальним проектом мають бути наведені аргументи, які підтверджують, що структурними компонентами (модулями) КЗЗ ОЕ в процесі їх захищеного функціонування згідно і порядком, викладеним у детальному проекті, забезпечується реалізація правил та порядку захищеного функціонування функціональних компонентів (підсистем) КЗЗ ОЕ, викладених у проекті архітектури відповідного ступеня формалізації.

А.2.7.2 Для заявлених рівнів гарантій Г-2 ... Г-5 відповідність між проектом архітектури та детальним проектом має бути показана неформальним чином. При цьому необхідно показати наявність відповідності між характеристиками всіх функціональних компонентів (підсистем) КЗЗ ОЕ та характеристиками основних структурних компонентів (модулів) КЗЗ ОЕ, які функціонують у складі цих підсистем, а саме – переліком реалізованих підсистемою/модулем ФПБ, переліком об'єктів КЗЗ, на які поширюється політика реалізованих ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до

розглянутих підсистем та модулів КЗЗ) атрибутами об'єктів КЗЗ різного типу. Опис відповідності може бути викладений як в оповідній формі, так і, наприклад, у вигляді таблиці.

А.2.7.3 Для заявленого рівня гарантій Г-6 відповідність між проектом архітектури та детальним проектом має бути продемонстрована, тобто показана з використанням результатів структурованого аналізу. При цьому необхідно показати наявність відповідності між характеристиками всіх функціональних компонентів (підсистем) КЗЗ ОЕ та характеристиками всіх структурних компонентів (модулів) КЗЗ ОЕ, які функціонують у складі цих підсистем, а саме – переліком реалізованих підсистемою/модулем ФПБ, переліком об'єктів КЗЗ, на які поширюється політика реалізованих ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу. Опис відповідності має бути викладений з використанням, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями, які містять аргументи на користь того, що існує повна відповідність між елементами двох розглянутих специфікацій КЗЗ ОЕ. При викладенні таких пояснень варто прагнути до зменшення неоднозначності, яка може існувати при неформальному показі відповідності, наприклад, обмежуючи інтерпретацію використовуваних термінів.

А.2.7.4 Для заявленого рівня Г-7 відповідність між проектом архітектури та детальним проектом має бути доведена, тобто, виражена формально з використанням відомих математичних понять для визначення синтаксису і семантики формалізованої нотації та правил доказів, які підтримують логічну аргументацію. При цьому додатково до результатів демонстрації відповідності між характеристиками всіх функціональних компонентів (підсистем) КЗЗ ОЕ та характеристиками всіх структурних компонентів (модулів) КЗЗ ОЕ, що функціонують у складі цих підсистем, які наводяться для заявленого рівня гарантій Г-6, мають бути наведені формальні докази відповідності між порядком захищеного функціонування підсистем КЗЗ та порядком захищеного функціонування модулів КЗЗ, викладеними, відповідно, у проекті архітектури та детальному проекті.

А.2.8 Опис результатів аналізу відповідності між детальним проектом та реалізацією

А.2.8.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що при реалізації структурних компонентів (модулів) КЗЗ розробником адекватно та несуперечливо реалізовані вимоги детального проекту.

Для підтвердження такої адекватності та несуперечності в описі результатів аналізу відповідності між детальним проектом та реалізацією мають бути наведені аргументи, які підтверджують, що наданим вхідним кодом реалізації структурних компонентів (модулів) КЗЗ ОЕ забезпечується реалізація правил та порядку захищеного функціонування цих модулів, викладених у детальному проекті відповідного ступеня формалізації.

А.2.8.2 Для заявлених рівнів гарантій Г-3 ... Г-6 відповідність між детальним проектом та реалізацією має бути показана неформальним чином. При цьому необхідно показати наявність відповідності між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів. Опис відповідності може бути викладений як в оповідній формі, так і, наприклад, у вигляді таблиці.

А.2.8.3 Для заявленого рівня гарантій Г-7 відповідність між детальним проектом та реалізацією має бути продемонстрована, тобто, показана з використанням результатів структурованого аналізу. При цьому необхідно показати наявність відповідності:

- між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) усіх структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів;

- між наведеними в детальному проекті характеристиками (реалізованими функціями, параметрами інтерфейсів) процедур, які містяться в бібліотеках часу виконання операційної системи (ядрі операційної системи) та використовуються в процесі функціонування всіх структурних компонентів (модулів) КЗЗ, та наданим розробником вхідним кодом реалізації цих процедур.

Опис відповідності має бути викладений з використанням, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями, які містять аргументи на користь того, що існує повна відповідність між елементами двох розглянутих специфікацій КЗЗ ОЕ.

При викладенні таких пояснень варто прагнути до зменшення неоднозначності, яка може існувати при неформальному показі відповідності, наприклад, обмежуючи інтерпретацію використовуваних термінів.

А.2.9 Опис методик діяльності розробника протягом життєвого циклу ОЕ

А.2.9.1 У цьому документі розробником мають бути визначені всі стадії життєвого циклу ОЕ, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги (вимоги, що мають бути виконані перш, ніж розпочинати наступний етап), а також викладені (безпосередньо або шляхом посилання на інші документи) методики діяльності, що застосовуються на кожній стадії життєвого циклу.

Примітка. У загальному випадку в життєвому циклі будь-якого ОЕ можуть бути виділені такі стадії:

- визначення вимог;
- розроблення;
- введення в експлуатацію;
- експлуатація (супроводження);
- зняття з експлуатації.

Кожній стадії життєвого циклу відповідають певні виконувані розробником дії (розв'язувані задачі) та, відповідно, методики діяльності в процесі вирішення цих задач.

На стадії визначення вимог до ОЕ аналізуються потреби споживача в захисті інформаційних ресурсів, визначаються потенційні загрози цим інформаційним ресурсам, робляться припущення про шляхи та способи реалізації цих загроз, формулюється реалізована політика безпеки та вхідні вимоги щодо забезпечення захищеності інформації, які мають бути реалізовані КЗЗ ОЕ.

На стадії розроблення ОЕ здійснюється уточнення переліку реалізованих ФПБ та вибір механізмів їх реалізації в КЗЗ ОЕ, проводиться проектування та реалізація функціональних і структурних компонентів КЗЗ ОЕ, тестування (випробування) засобів реалізації ФПБ та розроблення документації. На цьому ж етапі проводиться підготовка всіх необхідних матеріалів для проведення експертизи ОЕ, у тому числі оцінювання ФПБ та оцінювання рівня гарантій коректності реалізації ФПБ.

На стадії введення ОЕ в експлуатацію на конкретному об'єкті інформаційної діяльності здійснюється передача ОЕ (при початковому постачанні та наступних модифікаціях) замовнику. Вона передбачає спеціальні процедури або дії, необхідні для підтвердження справжності поставленого ОЕ, встановлення, генерації та запуску ОЕ безпечним чином.

На стадії експлуатації (супроводження) ОЕ здійснюються планування та організація експлуатації ОЕ відповідно до вимог нормативних документів та експлуатаційної документації; виконується підтримка користувачів ОЕ, забезпечення їх консультаціями та методичними матеріалами; оцінюється ефективність забезпечення захищеності інформації з використанням ОЕ, виконується аналіз проблем, що виникають, та виявлених недоліків; оцінюється потреба в доопрацюванні (модернізації) та виконується доопрацювання (модернізація) ОЕ.

На стадії зняття з експлуатації виконується планування і реалізація заходів щодо вилучення інформаційних ресурсів та очищення (знищення) носіїв інформації, що використовувалися в процесі експлуатації ОЕ.

А.2.9.2 Опис методик діяльності розробника протягом життєвого циклу ОЕ має стосуватися методик, використовуваних при визначенні вимог, розробленні, введенні в експлуатацію та експлуатації (супроводженні) ОЕ. В опис має вноситися інформація про процедури, інструментальні засоби та методи, використовувані розробником (наприклад, при проектуванні, реалізації, тестуванні, виправленні помилок). У ньому має бути наведена загальна структура керування застосуванням певних процедур (наприклад, ідентифікація та опис персональної відповідальності за реалізацію кожної з процедур, виконуваних на відповідних стадіях життєвого циклу ОЕ). З урахуванням специфіки конкретного ОЕ, в описі мають бути окремо відображені та охарактеризовані аспекти забезпечення достатнього рівня захищеності ОЕ, а також безпеки середовища його розробки та експлуатації.

А.2.9.3 Рівень деталізації описів використовуваних розробником на всіх зазначених стадіях методик діяльності (у т.ч. процедур, інструментальних засобів та методів) має дозволити експерту дійти обґрунтованого висновку про те, що їх використання дає можливість мінімізувати імовірність виникнення недоліків, які мають відношення до захищеності оброблюваної інформації, а у випадку виявлення таких недоліків – дозволяє усунути їх у найкоротший термін і з мінімальним

(тимчасовим) зниженням рівня захищеності оброблюваної інформації.

А.2.10 Документація використовуваних при розробленні інструментальних засобів

А.2.10.1 Інформація, яка міститься в документації використовуваних при розробленні інструментальних засобів, повинна дозволити експерту дійти висновку про те, чи використовувалися розробником для розроблення і реалізації ОЕ добре визначені мови програмування та інструментальні засоби, які дають несуперечливі та передбачувані результати, а також чи документовані всі необхідні для використання цих засобів параметри.

А.2.10.2 У наведеній документації мають бути описані всі використовувані при розробленні та реалізації програмного забезпечення ОЕ мови програмування та інструментальні засоби. Якщо при розробленні та реалізації програмного забезпечення ОЕ використовуються тільки мови програмування та інструментальні засоби, які відповідають вимогам діючих національних, міждержавних або міжнародних стандартів, мають бути зазначені відповідні стандарти. В іншому випадку варто надати повне визначення та опис використовуваних мов.

Примітка. Використовувані мови програмування та інструментальні засоби мають бути добре визначеними. Добре визначеною мовою програмування є така, для якої існує чіткий та повний опис її синтаксису та детальний опис семантики кожної з її конструкцій. Добре визначеними інструментальними засобами є такі, котрі можуть бути використані без залучення додаткових матеріалів, які пояснюють їх використання. Такими, наприклад, вважаються мови програмування та системи автоматизації проектування, які відповідають діючим міжнародним стандартам. Вимога доброї визначеності стосується всіх використовуваних інструментальних засобів, у тому числі засобів розробки проекту архітектури, детального проекту та реалізації.

А.2.10.3 У документації інструментальних засобів розробки (наприклад, у специфікаціях мови програмування та в настановах користувачу) мають бути наведені всі конструкції, використовувані у вхідному коді програмного забезпечення ОЕ, і для кожної такої конструкції має бути надане чітке та однозначне визначення її призначення та результатів її виконання. Наприклад, документація інструментальних засобів не повинна передбачати, що читач є фахівцем з використовуваної мови програмування. Якщо інструментальні засоби відрізняються від того, що визначено стандартом, то ці відмінності також мають бути описані.

А.2.10.4 Незалежно від рівня відповідності використовуваних мов програмування та інструментальних засобів вимогам діючих стандартів, додатково має бути документовано використання всіх залежних від конкретної реалізації інструментальних засобів параметрів мов програмування та/або компіляторів, які можуть уплинути на виконуваний код або відрізняються від стандарту використовуваної мови.

А.2.10.5 У документації інструментальних засобів проектування та розробки апаратних засобів має бути описано використання всіх параметрів розроблюваних засобів, які впливають на результати застосування інструментальних засобів (наприклад, детальні апаратні специфікації або самі апаратні засоби).

А.2.11 Опис методик забезпечення безпеки в процесі розроблення та виробництва ОЕ

А.2.11.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, чи документовані розробником методики забезпечення фізичної, технічної, організаційної та кадрової безпеки в процесі розроблення та реалізації ОЕ, а також чи використовуються відповідні заходи для захисту від несанкціонованої модифікації чи руйнування всіх засобів та матеріалів, використовуваних для генерації ОЕ.

А.2.11.2 Для заявлених рівнів гарантій Г-4 ... Г-7 опис відповідних методик має містити опис суті та порядку застосування заходів безпеки при розробленні та реалізації ОЕ. При цьому має бути відображена специфіка застосування різних заходів, а саме:

- заходів фізичної безпеки, заснованих, наприклад, на використанні засобів керування фізичним доступом, використовуваних для запобігання несанкціонованому доступу до засобів і матеріалів розробки ОЕ (як у робочий, так і в позаробочий час);

- заходів технічної безпеки, заснованих, наприклад, на використанні відповідних засобів захисту інструментальних засобів розробки та матеріалів розробки від несанкціонованого доступу через засоби обчислювальної техніки;

- організаційних заходів безпеки, наприклад, таких, які регламентують порядок надання/скасування прав доступу до приміщень, де виконується розроблення, або до конкретних

засобів чи матеріалів розробки; порядок передачі матеріалів розробки до зовнішніх організацій; порядок зустрічі та супроводження відвідувачів; ролі та обов'язки щодо забезпечення безупинного застосування заходів безпеки та виявлення порушень режиму безпеки;

- заходів кадрової безпеки, заснованих, наприклад, на використанні спеціальних процедур перевірки, які дозволяють установити, чи заслуговують довіри прийняті на роботу співробітники.

Зазначені заходи мають бути спрямовані на захист конфіденційності та цілісності проектних документів та вхідного коду реалізації ОЕ. Крім самих заходів безпеки, мають бути передбачені процедури їх перегляду та аудиту.

В описі мають бути зазначені конкретні робочі місця, описані види виконуваних робіт та конкретні заходи безпеки, які застосовуються на кожному з робочих місць при виконанні цих робіт. Окремо мають бути виділені заходи безпеки, які застосовуються на підприємстві в цілому.

А.2.11.3 Для заявлених рівнів гарантій Г-6 ... Г-7 додатково мають бути наведені відомості, які підтверджують факт застосування зазначених заходів безпеки для захисту від несанкціонованої модифікації чи руйнування всіх засобів та матеріалів, використовуваних для генерації ОЕ. Має бути наведено опис політики забезпечення цілісності використовуваних для генерації ОЕ матеріалів, в якому має бути відображено, які саме матеріали повинні бути захищені від несанкціонованої модифікації з метою збереження цілісності ОЕ, кому з персоналу розробника дозволено модифікувати такі матеріали, а також те, яким чином виконується перевірка цілісності відповідних матеріалів перед виконанням генерації ОЕ. Крім цього, мають бути наведені відомості, які дозволять експерту упевнитися в самому факті застосування зазначених процедур при генерації ОЕ (наприклад, записи відповідних журналів реєстрації).

А.2.12 Документація з керування конфігурацією ОЕ

А.2.12.1 Інформація, яка міститься в документації з керування конфігурацією, повинна дозволити експерту дійти висновку про те, що розробником впроваджена та на всіх етапах життєвого циклу ОЕ використовується система керування конфігурацією ОЕ, яка забезпечує керування внесенням змін до апаратного та програмного забезпечення, тестового покриття та документації, а також гарантує постійну відповідність між усією документацією та реалізацією ОЕ.

А.2.12.2 Використовувана система керування конфігурацією ОЕ повинна забезпечувати впевненість у цілісності ОЕ, починаючи від початкових етапів проектування та закінчуючи завершенням його експлуатації. З цією метою система керування конфігурацією повинна забезпечувати: можливість контролю всіх включених під її керування елементів конфігурації (усіх компонентів ОЕ, засобів та матеріалів, використовуваних у процесі розроблення) у процесі проектування, реалізації та супроводження ОЕ; запобігання несанкціонованій модифікації, додаванню або знищенню елементів конфігурації; повноту та коректність ОЕ до моменту його передачі замовнику.

А.2.12.3 Для забезпечення зазначених можливостей система керування конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації (однозначна ідентифікація всіх елементів конфігурації); регулювання конфігурації (контроль за внесенням будь-яких змін до ОЕ); облік стану (фіксація інформації щодо стану кожного елемента конфігурації, у тому числі його вхідне визначення та будь-які внесені зміни); перевірка якості конфігурації (перевірка інформації щодо стану всіх елементів конфігурації з метою досягнення впевненості в тому, що система керування конфігурацією працює належним чином).

А.2.12.4 Система керування конфігурацією може складатися як з організаційних, так і з технічних заходів та засобів. Система керування конфігурацією повинна охоплювати процеси розроблення та супроводження програмного, апаратного, програмно-апаратного забезпечення, розроблення документації, тестів тощо. Перелік елементів конфігурації, якими має керувати система керування конфігурацією, визначає область дії керування конфігурацією. Вона, як правило, містить: робочий проект (реалізацію) ОЕ; усю необхідну документацію (у тому числі проектну, тестову, експлуатаційну), документацію системи керування конфігурацією та інші документи, у тому числі повідомлення про недоліки, які виникають під час розроблення та експлуатації; параметри конфігурації, у тому числі настроювання інструментальних засобів розробки; інструментальні засоби розробки.

А.2.12.5 Для заявлених рівнів гарантій Г-1 … Г-7 документація з керування конфігурацією повинна містити: список елементів конфігурації ОЕ, план керування конфігурацією, план приймання елементів конфігурації під керування системи керування конфігурацією, опис процедур компонування елементів конфігурації до складу ОЕ та вихідні матеріали системи керування

конфігурацією.

А.2.12.5.1 До списку елементів конфігурації повинні входити всі елементи, які становлять область дії керування конфігурацією. Для кожного елемента конфігурації має бути наведений його опис.

А.2.12.5.2 План керування конфігурацією має визначати порядок застосування системи керування конфігурацією на всіх етапах життєвого циклу ОЕ. Відомості, які містяться в плані керування конфігурацією, мають містити:

- опис всіх операцій, виконуваних у процесі розроблення ОЕ, що підлягають процедурам керування конфігурацією (наприклад, створення, модифікація, видалення елемента конфігурації або повернення до більш ранньої версії);
- опис ролей та обов'язків осіб, необхідних для виконання операцій з окремими елементами конфігурації (для різних типів елементів конфігурації, наприклад, для документації та вхідного коду можуть бути ідентифіковані різні ролі);
- опис процедур, які використовуються для забезпечення того, щоб тільки уповноважені особи могли змінювати елементи конфігурації;
- опис процедур, які використовуються для синхронізації змін, внесених одночасно різними особами до одного елемента конфігурації;
- опис методу, використовуваного для унікальної ідентифікації елементів конфігурації, з обов'язковим забезпеченням того, щоб модифікація елемента конфігурації призводила до призначення нового унікального ідентифікатора;
- опис інформації, яка генерується в результаті застосування процедур керування конфігурацією та може свідчити про факт їх застосування;
- порядок контролю версій та унікального маркірування версій ОЕ (який охоплює, наприклад, випуск пакетів оновлення та подальше виявлення фактів їх використання).

А.2.12.5.3 План приймання елементів конфігурації має описувати критерії та процедури включення розробленого або зміненого елемента конфігурації до складу версії ОЕ, яка знаходиться під керуванням системи керування конфігурації. Призначення процедур включення: підтвердити, що будь-яке створення (або модифікація) елементів конфігурації було санкціоновано. При цьому мають бути визначені процедури включення, які застосовуються:

- на кожній стадії компонування ОЕ (наприклад, для окремих модулів, їх інтеграції, ОЕ в цілому);
- для програмних, програмно-апаратних та апаратних компонентів;
- для компонентів, які раніше пройшли експертизу.

Опис критеріїв включення має містити інформацію:

- про ролі окремих осіб розробника, відповідальних за приймання різних елементів конфігурації;
- про будь-які критерії приймання, які застосовуються при прийманні елементів конфігурації під контроль системи керування конфігурацією (наприклад, успішний перегляд документа або успішне виконання певних перевірок для програмного забезпечення та апаратних компонентів).

А.2.12.5.4 Опис процедур компонування має містити відомості про всі необхідні дії, які повинні бути виконані за допомогою використовуваних інструментальних засобів розробки при внесенні створеного або модифікованого елемента конфігурації до складу ОЕ.

А.2.12.5.5 Вихідні матеріали системи керування конфігурацією повинні підтверджувати те, що план керування конфігурацією застосовується, а всі елементи конфігурації підтримуються системою керування конфігурацією. Як такі вихідні матеріали можуть використовуватися, наприклад, записи журналів контролю змін або форми дозволу доступу до елементів конфігурації.

А.2.12.5.6 Для заявлених рівнів гарантій Г-4 … Г-7 система керування конфігурацією повинна базуватися на автоматизованих засобах, відповідно, описи плану керування конфігурацією, плану приймання елементів конфігурації під керування системи керування конфігурацією та процедур компонування елементів конфігурації до складу ОЕ мають відображати порядок використання таких засобів, які, як мінімум, повинні: надавати можливості для виявлення розбіжностей між поточною та попередньою версіями ОЕ для визначення всіх інших елементів конфігурації, на які впливає модифікація цього елемента конфігурації; вести журнал аудиту зроблених змін та дозволяти одержувати звіти про стан елементів конфігурації. При цьому в описі процедур компонування мають бути спеціально зазначені як використовувані при компонуванні

інструментальні засоби, так і ті елементи конфігурації (файли вхідного тексту програмного забезпечення, інструментальні засоби, файли настроювань інструментальних засобів), стан яких контролюється з використанням автоматизованих засобів керування конфігурацією. Вихідні матеріали системи керування конфігурацією мають обов'язково містити підготовлені з використанням автоматизованих засобів керування конфігурацією звіти про стан певних, обраних розробником, елементів конфігурації.

А.2.13 Опис процедур безпечної інсталяції, генерації та запуску ОЕ

А.2.13.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що розробником надані та документовані засоби та процедури інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану, а також що всі можливі параметри конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, документовані.

А.2.13.2 Засоби та процедури інсталяції, генерації та запуску повинні забезпечувати безпечний перехід ОЕ від перебування під контролем системи керування конфігурацією розробника до початкових операцій у середовищі експлуатації. Вони повинні, у тому числі забезпечувати контроль правильності формування версії ОЕ, яка постачається замовнику, а також контроль коректності настроювання всіх необхідних параметрів КЗЗ та запуску ОЕ в безпечний спосіб, так, як це визначено розробником.

А.2.13.3 Склад засобів та процедур залежить від виду та технології функціонування ОЕ. Зазвичай, має місце розподіл відповідальності щодо інсталяції, генерації та запуску ОЕ між розробником та замовником ОЕ, хоча всі дії можуть виконуватися й однією стороною. Безпека ОЕ під час його інсталяції, генерації та запуску повинна забезпечуватися розробником, який здійснює (безпосередньо на місці або шляхом передачі відповідних програмних засобів, що автоматизують процес інсталяції) виконання цих операцій, з обов'язковим здійсненням контролю за реалізацією необхідних заходів з боку замовника ОЕ.

А.2.14 Опис процедур постачання ОЕ замовнику

А.2.14.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що розробником реалізована та застосовується система технічних, організаційних та фізичних заходів безпеки, які забезпечують підтримку цілісності ОЕ та виявлення модифікації або підміни ОЕ (або забезпечення неможливості такої модифікації чи підміни) при постачанні ОЕ замовнику.

А.2.14.2 Опис процедур постачання має відображати використання відповідних заходів та процедур як при початковому постачанні ОЕ замовнику (для заявлених рівнів гарантій Г-3 … Г-7), так і при постачанні випущених розробником модифікацій (оновлень) ОЕ (для заявлених рівнів гарантій Г-6 … Г-7). Ці заходи та процедури повинні бути спрямовані на підтвердження справжності переданого ОЕ, унеможливлення навмисного та ненавмисного внесення змін до актуальної версії ОЕ або заміну її фальсифікованою версією на всьому шляху доставки ОЕ від організації розробника до об'єкта замовника. У документації має бути описано, яким чином застосовувані заходи та процедури забезпечують виявлення та запобігання модифікації або будь-якій розбіжності між еталонною копією ОЕ, яка знаходиться в розробника, та версією, одержаною в місці експлуатації. Мають бути наведені процедури ідентифікації ОЕ або його складових частин, процедури забезпечення цілісності ОЕ або його складових частин під час пересилання, а також процедури перевірки цілісності ОЕ або його складових частин при одержанні замовником.

Примітка. Використовувані процедури забезпечення і перевірки цілісності ОЕ та його складових частин можуть будуватися з використанням заходів технічного захисту (наприклад, з використанням механізмів вироблення/перевіряння електронного цифрового підпису, криптографічних контрольних сум файлів програмного забезпечення тощо), організаційних заходів (контроль конфігурації для досягнення впевненості в тому, що замовнику надано потрібну версію ОЕ), а також заходів фізичного захисту (наприклад, використання вакуумної упаковки носіїв з програмним забезпеченням та документації або інших захисних оболонок, які запобігають (або фіксують) спробам фізичного доступу). Якщо використовується декілька різних способів пересилання ОЕ замовникам (наприклад, шляхом передачі носіїв з програмним забезпеченням та передачею програмного забезпечення в електронному вигляді через Internet), відповідні процедури мають бути наведені для кожного з таких способів.

А.2.14.3 Для заявлених рівнів гарантій Г-6 … Г-7 додатково має бути наведений опис процедур та відповідних механізмів, що дозволяють виявити спробу підміни відправника, навіть у тих випадках, коли розробник нічого не відправляв Замовнику, та гарантують, що одержаний замовником ОЕ (або його оновлення) був переданий йому саме розробником.

А.2.15 Опис послуг безпеки, що реалізуються КЗЗ оцінюваного ОЕ

А.2.15.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що в наданій замовнику експлуатаційній документації розробником наведено опис основних принципів безпеки, необхідних для правильного використання ФПБ, реалізованих КЗЗ ОЕ, а також опис самих реалізованих послуг безпеки.

А.2.15.2 В описі послуг безпеки мають бути наведені, як мінімум, такі відомості:

- стислий опис вимог до апаратного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому апаратні засоби;
- стислий опис вимог до програмного середовища функціонування ОЕ та існуючих обмежень на використовувані в ньому програмні засоби;
- визначення проблем (цілей) забезпечення безпеки інформації, вирішення яких покладається на ОЕ;
- визначення завдань захисту, вирішення яких забезпечується ОЕ;
- високорівневе визначення переліку та політики ФПБ, заявлених розробником як таких, що призначені для вирішення визначених завдань захисту;
- неформалізований опис порядку реалізації кожної ФПБ на рівні деталізації, необхідному для розуміння основних принципів її реалізації.

А.2.16 Настанови адміністратору з послуг безпеки

А.2.16.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що в наданій замовнику експлуатаційній документації розробником викладені всі відомості, необхідні адміністратору (адміністраторам, якщо реалізовано декілька адміністративних ролей) для того, щоб здійснювати безпечне адміністрування ОЕ.

А.2.16.2 Настанови адміністратору з послуг безпеки повинні сприяти розумінню особливостей усіх ФПБ (функцій захисту), реалізованих КЗЗ ОЕ, у тому числі функцій, які вимагають виконання адміністратором дій, критичних з погляду безпеки, так і функцій, які надають доступ до інформації, критичної з погляду безпеки.

А.2.16.3 У настановах адміністратору з послуг безпеки мають бути наведені (для кожної адміністративної ролі), як мінімум, такі відомості:

- опис усіх засобів адміністрування ОЕ, реалізованих ними функцій адміністрування та інтерфейсів до цих функцій, доступних адміністратору, який містить інформацію про: метод (методи) виклику інтерфейсу (наприклад, з використанням командного рядка, системних викликів мови програмування, меню тощо); параметри, які встановлюються адміністратором, їх допустимі значення та значення за замовчуванням; повідомлення або коди повернення, що формуються КЗЗ ОЕ у відповідь на виклик інтерфейсу. Мають бути розглянуті як функції адміністрування, використовувані в процесі інсталяції, генерації та запуску ОЕ, так і функції, використовувані в штатному режимі функціонування ОЕ;
- опис усіх параметрів безпеки, контрольованих адміністратором, із зазначенням, за необхідності, їх безпечних значень;
- опис вимог до порядку роботи з ОЕ користувачів – не адміністраторів (або користувачів, призначених на інші адміністративні ролі), дотримання яких має контролюватися адміністратором;
- попередження щодо функцій та привілеїв, використання яких користувачами – не адміністраторами (або користувачами, призначеними на інші адміністративні ролі) слід контролювати з метою забезпечення безпечного функціонування ОЕ;
- опис усіх типів подій, що мають відношення до безпеки, які реєструються КЗЗ, у тому числі подій, пов'язаних з виконанням функцій адміністрування, наявність яких має контролюватися адміністратором, із зазначенням дій, які повинні виконуватися (якщо буде потрібно) з метою підтримки безпечного функціонування ОЕ;
- опис засобів ОЕ та реалізованих ними функцій, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ;
- опис усіх вимог безпеки до середовища функціонування ОЕ, які повинні

контролюватися адміністратором організаційними заходами.

А.2.17 Настанови користувачу з послуг безпеки

А.2.17.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про те, що в наданій замовнику експлуатаційної документації розробником викладені всі відомості, необхідні користувачу (користувачам, якщо реалізовано декілька ролей користувачів) для того, щоб здійснювати безпечне використання ОЕ.

А.2.17.2 Настанови користувачу з послуг безпеки мають містити опис ФПБ (функцій захисту), реалізованих КЗЗ ОЕ, інтерфейсів до них, доступних користувачу, а також інструкції з їх використання. Матеріали, що вносяться до настанов користувачу, мають надавати можливість користувачам сформувати правильне уявлення про можливості ФПБ (функцій захисту), реалізованих КЗЗ ОЕ, та порядок їх безпечного використання.

А.2.17.3 У настановах користувачу з послуг безпеки мають бути наведені (для кожної ролі користувачів), як мінімум, такі відомості:

- опис усіх функціональних можливостей ОЕ щодо забезпечення безпеки, реалізованих функцій захисту та інтерфейсів до цих функцій, доступних користувачу, який містить інформацію про: метод (методи) виклику інтерфейсу (наприклад, з використанням командного рядка, системних викликів мови програмування, меню тощо); параметри, які встановлюються користувачем, їх допустимі значення та значення за замовчуванням; повідомлення або коди повернення, що формуються КЗЗ ОЕ у відповідь на виклик інтерфейсу. Має бути відображено, що саме реалізують доступні користувачу функції захисту та як їх необхідно використовувати, щоб користувачі мали можливість надійно захищати свою інформацію;
- опис вимог щодо порядку роботи користувачів з ОЕ, який містить роз'яснення ролі користувачів щодо підтримки безпечного функціонування ОЕ, а також зміст обов'язків користувачів щодо забезпечення безпечного функціонування ОЕ;
- попередження щодо доступних користувачу функцій та привілеїв, які слід контролювати в безпечному середовищі експлуатації;
- рекомендації з ефективного використання функцій захисту (наприклад, опис практичних прийомів формування стійких до зламання паролів, рекомендована періодичність резервного копіювання файлів користувачів тощо).

А.2.18 Програма та методика випробувань функціональних послуг безпеки

А.2.18.1 Інформація, яка міститься в цьому документі, повинна дозволити експерту дійти висновку про повноту та ефективність проведених розробником випробувань засобів, що реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

А.2.18.2 Основний зміст документа в частині викладення програми випробувань ФПБ має складати опис того, що саме, тобто, які властивості ОЕ мають бути перевірені під час проведення випробувань з метою підтвердження або спростування реалізації кожної з ФПБ, наведених у функціональній специфікації КЗЗ ОЕ. У цьому описі необхідно максимально повно відобразити перелік тих перевірок (без наведення конкретних методів їх виконання), успішне виконання яких дозволить дійти обґрунтованого висновку про факт реалізації ФПБ певного рівня згідно з визначеною політикою. Для цього програма випробувань має передбачати:

- виконання перевірок усіх вимог НД ТЗІ 2.5-004-99 щодо політики та порядку функціонування засобів, які реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих послуг та охопленням усіх об'єктів КЗЗ і засобів (структурних компонентів) КЗЗ, на які поширюється ця політика;
- виконання перевірок усіх вимог НД ТЗІ 2.5-004-99, що стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, наведених у функціональній специфікації КЗЗ ОЕ.

А.2.18.3 Для заявлених рівнів гарантій Г-4 ... Г-7 програма випробувань також повинна передбачати виконання додаткових перевірок з метою підтвердження того, що КЗЗ ОЕ є відносно або абсолютно стійким до атак з боку розробника.

А.2.18.4 Основний зміст документа в частині викладення методики випробувань ФПБ має складати виконаний з урахуванням вимог програми випробувань опис переліку, послідовності, порядку та методів виконання перевірок ФПБ, метою яких є підтвердження фактів реалізації ФПБ засобами КЗЗ ОЕ згідно з визначеною у функціональній специфікації політикою. При цьому, з метою забезпечення максимально достовірних результатів випробувань, необхідно звернути особливу увагу

на вибір підходу до тестування засобів реалізації ФПБ, а також вибір тестових даних.

А.2.18.5 Для ОЕ із заявленим рівнем гарантій Г-2 і нижче доцільно використовувати підхід монолітного тестування, який передбачає використання в процесі проведення випробувань лише видимих ззовні КЗЗ ОЕ інтерфейсів підсистем та модулів КЗЗ, документованих у проекті архітектури та детальному проекті.

А.2.18.6 Для ОЕ із заявленим рівнем гарантій Г-3 і вище доцільно використовувати також підхід функціонально-синтетичного тестування, який передбачає використання в процесі тестування як видимих ззовні КЗЗ ОЕ інтерфейсів підсистем та модулів КЗЗ, так і невидимих ззовні (внутрішньосистемних) інтерфейсів.

А.2.18.7 При розробленні, з урахуванням зазначених рекомендацій, методики перевірки різних ФПБ необхідно 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, а також необхідних для виконання перевірок тестових даних. 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 ФПБ як в штатному, так і в позаштатному режимах функціонування, наприклад, у процесі виконання спроб НСД.

А.2.18.8 Для заявлених рівнів гарантій Г-4 ... Г-7, з метою підтвердження того, що КЗЗ ОЕ є відносно стійким до атак з боку розробника, у методиці випробувань має бути наведений опис порядку перевірки засобів реалізації ФПБ в процесі виконання спроб НСД з використанням невидимих ззовні внутрішньосистемних інтерфейсів. Для заявлених рівнів гарантій Г-6 ... Г-7, з метою підтвердження того, що КЗЗ ОЕ є абсолютно стійким до атак з боку розробника, у методиці випробувань має бути наведений опис порядку перевірки засобів реалізації ФПБ у процесі виконання спроб НСД з використанням не довірених (спеціально розроблених) структурних модулів КЗЗ, які навмисно вводяться до складу КЗЗ і реалізують додаткову функціональність, не відображену в детальному проекті КЗЗ.

А.2.18.9 Окремий розділ (підрозділ) наданої програми та методики має містити відомості, які підтверджують достатність використовуваного тестового покриття. Наведені відомості мають показувати, що:

- перевірялися засоби, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ;
- у ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ;
- у ході виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

А.2.18.10 Відповідність між виконаними перевірками, ФПБ, функціональними компонентами КЗЗ (підсистемами) та структурними компонентами КЗЗ (модулями) може бути показана як в оповідній формі, так і в інший спосіб, наприклад, у вигляді таблиці.

А.2.18.11 Програма та методика випробувань має бути оформлена з урахуванням вимог 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.

А.2.18.12 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-3 … Г-7 надана експерту програма та методика випробувань повинна бути погоджена з уповноваженим державним органом.

А.2.19 Протоколи випробувань функціональних послуг безпеки

А.2.19.1 Інформація, яка міститься цих матеріалах, повинна дозволити експерту дійти висновку про те, що наведені в програмі та методиці випробувань очікувані результати випробувань засобів, які реалізують усі ФПБ, відповідають наданим фактичним результатам проведених розробником випробувань та можуть бути перевірені шляхом повторення відповідних тестових процедур.

А.2.19.2 У наданих розробником протоколах випробувань мають бути викладені, з посиланням на відповідні пункти програми 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 КЗЗ ОЕ певних ФПБ.

А.2.19.3 Протоколи випробувань мають бути оформлені з урахуванням вимог ДСТУ 2851-94, інших стандартів та нормативних документів у галузі інформаційних технологій та захисту інформації, які стосуються документування результатів випробувань.

А.2.19.4 Відповідно до вимог НД ТЗІ 3.6-001-2000, для заявлених рівнів гарантій Г-4 ... Г-7 надані експерту протоколи випробувань повинні підтверджувати факт участі у випробуваннях представників уповноваженого державного органу.

А.2.20 Опис результатів аналізу стійкості КЗЗ до атак з боку розробника

А.2.20.1 У цьому документі розробником, з урахуванням наведених у протоколах випробувань результатів проведених перевірок засобів реалізації ФПБ у процесі виконання спроб НСД, з використанням невидимих ззовні внутрішньосистемних інтерфейсів (для заявлених рівнів гарантій Г-4 ... Г-7) та не довірених (спеціально розроблених) структурних модулів КЗЗ ОЕ, які навмисно вводяться до складу КЗЗ (для заявлених рівнів гарантій Г-6 ... Г-7), мають бути наведені аргументи, які дозволять експерту дійти висновку про те, що КЗЗ ОЕ є відносно або абсолютно стійким до атак з боку розробника.

А.2.20.2 При викладенні таких аргументів для заявлених рівнів гарантій Г-4 ... Г-5 має передбачатися, що, відповідно до класифікації рівнів можливостей порушників, наведеної в НД ТЗІ 1.1-002-99, розробник має можливості, які відповідають третьому рівню. Для заявлених рівнів гарантій Г-6 ... Г-7 має передбачатися, що, відповідно до класифікації рівнів можливостей порушників, наведеної в НД ТЗІ 1.1-002-99, розробник має можливості, які відповідають четвертому рівню. Зміст аргументів, які наводяться, має грунтуватися на результатах виконання відповідних перевірок, наведених у протоколах випробувань.

Додаток Б
Вимоги щодо змісту програми перевірки дотримання вимог різних рівнів гарантій коректності реалізації функціональних послуг безпеки
(рекомендований)

У Додатку Б викладені специфічні вимоги щодо змісту програми перевірки дотримання вимог різних рівнів гарантій коректності реалізації ФПБ. Вимоги викладені з урахуванням вимог НД ТЗІ 2.5-004-99 щодо різних рівнів гарантій коректності реалізації ФПБ, а також з урахуванням рекомендацій щодо складу та змісту матеріалів (документів), які надаються розробником експерту для оцінювання рівня гарантій коректності реалізації ФПБ, наведених у додатку А.

Б.1 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ

Б.1.1 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.1.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.1.2 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.1.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.1.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.1.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.1.2.2.1 Розробником розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Б.1.3 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.1.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.1.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Представлені функціональні

специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.1.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.1.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у неформалізованому вигляді. Поданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.1.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.1.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у неформалізованому вигляді. Наданий детальний проект містить перелік структурних компонентів (модулів) КЗЗ ОЕ, що мають безпосереднє відношення до безпеки, і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У наданому детальному проекті описані призначення і параметри інтерфейсів структурних компонентів (модулів) КЗЗ ОЕ, що мають безпосереднє відношення до безпеки.

Б.1.4 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.1.4.1 Розробником надано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.1.5 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.1.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні, необхідні для правильного використання ФПБ, принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.1.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.1.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.1.6 Вимоги до програми перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.1.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.1.6.2 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, які можуть бути перевірені шляхом повторення тестування.

Б.2 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ

Б.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.2.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.2.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.2.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.2.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.2.2.2.1 Розробником розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Б.2.3 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.2.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.2.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.2.3.1.2 Подані функціональні специфікації містять неформалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.2.3.1.3 У матеріалах, зазначених у п. А.2.5, неформалізованим чином показано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.2.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.2.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у неформалізованому вигляді. Наданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У наданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У наданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.2.3.2.2 У матеріалах, зазначених у п. А.2.6, неформалізованим чином показано відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.2.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.2.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у неформалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.2.3.3.2 У матеріалах, зазначених у п. А.2.7, неформалізованим чином показано відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.2.4 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.2.4.1 Розробником представлено описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.2.5 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.2.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.2.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.2.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо

послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.2.6 Вимоги до програми перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.2.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.2.6.2 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, які можуть бути перевірені шляхом повторення тестування.

Б.2.6.3 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених “слабких місць” та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”.

Б.3 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ

Б.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.3.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.3.1.2 Усі структурні компоненти КЗЗ ОЕ (модулі), описані в матеріалах, зазначених у п. А.2.3, є добре визначеними і максимально незалежними від інших модулів. Кожний із структурних компонентів (модулів) КЗЗ спроектовано відповідно до принципу мінімуму повноважень.

Б.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.3.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.3.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.3.2.1.2 Розробником у матеріалах, зазначених у п. А.2.10, описано стандарти кодування, яких необхідно додержуватися в процесі реалізації, та гарантовано, що всі вхідні коди компілюються відповідно до цих стандартів. Усі використовувані під час реалізації мови програмування є добре визначеними. Усі залежні від реалізації параметри мов програмування або компіляторів документовані.

Б.3.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.3.2.2.1 Розробником розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на

всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ

Б.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.3.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.3.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.3.3.1.2 Подані функціональні специфікації містять частково формалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.3.3.1.3 Матеріали технічного завдання, зазначені в п. А.2.1, погоджені з уповноваженим державним органом.

Б.3.3.1.4 У матеріалах, зазначених у п. А.2.5, неформалізованим чином показано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.3.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.3.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.3.3.2.2 У матеріалах, зазначених у п. А.2.6, неформалізованим чином показано відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.3.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.3.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у неформалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.3.3.3.2 У матеріалах, зазначених у п. А.2.7, неформалізованим чином показано відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.3.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації має передбачати перевірку таких вимог:

Б.3.3.4.1 Розробником у матеріалах, зазначених у п. А.2.4, наведено вхідний код реалізації частини КЗЗ ОЕ.

Б.3.3.4.2 У матеріалах, зазначених у п. А.2.8, неформалізованим чином показано відповідність між детальним проектом КЗЗ ОЕ та реалізацією частини КЗЗ ОЕ.

Б.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.3.4.1 Розробником надано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.3.4.2 Існує описана в матеріалах, зазначених у п. А.2.14, система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ ОЕ, яке поставляється замовнику, точно відповідає еталонній копії.

Б.3.5 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.3.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.3.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.3.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.3.6 Вимоги до програми перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.3.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.3.6.2 Програма та методика випробувань ФПБ, документована в матеріалах, зазначених у п. А.2.18, погоджена з уповноваженим державним органом.

Б.3.6.3 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, що можуть бути перевірені шляхом повторення тестування.

Б.3.6.4 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених “слабких місць” та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”.

Б.4 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ

Б.4.1 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.4.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У

матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.4.1.2 Усі структурні компоненти КЗЗ ОЕ (модулі), описані в матеріалах, зазначених у п. А.2.3, є добре визначеними і максимально незалежними від інших модулів. Кожний із структурних компонентів (модулів) КЗЗ спроектовано відповідно до принципу мінімуму повноважень.

Б.4.1.3 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що критичні для безпеки структурні компоненти КЗЗ ОЕ (модулі) захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня.

Б.4.2 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.4.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.4.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.4.2.1.2 Розробником у матеріалах, зазначених у п. А.2.10, описано стандарти кодування, яким необхідно додержуватися в процесі реалізації, та гарантовано, що всі вхідні коди компілюються відповідно до цих стандартів. Усі використовувані під час реалізації мови програмування є добре визначеними. Усі залежні від реалізації параметри мов програмування або компіляторів документовані.

Б.4.2.1.3 Розробником розроблені, запроваджені та підтримуються в робочому стані документально оформлені в матеріалах, зазначених у п. А.2.11, методики забезпечення фізичної, технічної, організаційної і кадрової безпеки.

Б.4.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, яка стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.4.2.2.1 Розробником розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією базується на автоматизованих засобах. Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Б.4.2.2.2 Запроваджена система керування конфігурацією використовується для генерації КЗЗ ОЕ з вхідного коду та обліку всіх змін з появою нових версій.

Б.4.2.2.3 Запроваджена система керування конфігурацією здатна видавати звіти про стан елементів конфігурації.

Б.4.3 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.4.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.4.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.4.3.1.2 Подані функціональні специфікації містять формалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.4.3.1.3 Матеріали технічного завдання, зазначені в п. А.2.1, погоджені з уповноваженим державним органом.

Б.4.3.1.4 У матеріалах, зазначених у п. А.2.5, з використанням результатів структурованого аналізу продемонстровано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.4.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.4.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.4.3.2.2 В матеріалах, зазначених у п. А.2.6, неформалізованим чином показано відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.4.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.4.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.4.3.3.2 У матеріалах, зазначених у п. А.2.7, неформалізованим чином показано відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.4.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації має передбачати перевірку таких вимог:

Б.4.3.4.1 Розробником у матеріалах, зазначених у п. А.2.4, наведено вхідний код реалізації частини КЗЗ ОЕ.

Б.4.3.4.2 У матеріалах, зазначених у п. А.2.8, неформалізованим чином показано відповідність між детальним проектом КЗЗ ОЕ та реалізацією частини КЗЗ ОЕ.

Б.4.4 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.4.4.1 Розробником подано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.4.4.2 Існує описана в матеріалах, зазначених у п. А.2.14, система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ ОЕ, яке поставляється замовнику, точно відповідає еталонній копії.

Б.4.5 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.4.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.4.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.4.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.4.6 Вимоги до програми перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.4.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.4.6.2 Програма та методика випробувань ФПБ, документована в матеріалах, зазначених у п. А.2.18, погоджена з уповноваженим державним органом.

Б.4.6.3 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, що можуть бути перевірені шляхом повторення тестування.

Б.4.6.4 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених “слабких місць” та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця”.

Б.4.6.5 Надані розробником матеріали, зазначені в пп. А.2.19 та А.2.20, підтверджують факт виконання розробником тестів з подолання механізмів захисту та доводять, що КЗЗ ОЕ є відносно стійкий до такого роду атак з боку розробника.

Б.4.6.6 До складу приймальної комісії з проведення випробувань залучаються представники уповноваженого державного органу.

Б.5 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ

Б.5.1 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.5.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.5.1.2 Усі структурні компоненти КЗЗ ОЕ (модулі), описані в матеріалах, зазначених у п. А.2.3, є добре визначеними і максимально незалежними від інших модулів. Кожний із структурних компонентів (модулів) КЗЗ спроектовано відповідно до принципу мінімуму повноважень.

Б.5.1.3 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що критичні для безпеки структурні компоненти КЗЗ ОЕ (модулі) захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня.

Б.5.1.4 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що розробником вжито заходів, спрямованих на виключення з КЗЗ ОЕ компонентів, що не є критичними для безпеки. У матеріалах, зазначених у п. А.2.3, наведені підстави для включення до КЗЗ ОЕ будь-якого елемента, який не має відношення до захисту.

Б.5.1.5 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що: розробка ПЗ переважно була спрямована на мінімізацію складності КЗЗ ОЕ; КЗЗ спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою, який відіграє центральну роль у реалізації внутрішньої структури КЗЗ; під час розробки КЗЗ були задіяні такі підходи, як модульність побудови і приховання (локалізація видимості) даних.

Б.5.2 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.5.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.5.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.5.2.1.2 Розробником у матеріалах, зазначених у п. А.2.10, описано стандарти кодування, яких необхідно додержуватися в процесі реалізації, та гарантовано, що всі вхідні коди компілюються відповідно до цих стандартів. Усі використовувані під час реалізації мови програмування є добре визначеними. Усі залежні від реалізації параметри мов програмування або компіляторів документовані.

Б.5.2.1.3 Розробником розроблені, запроваджені та підтримуються в робочому стані документально оформлені в матеріалах, зазначених у п. А.2.11, методики забезпечення фізичної, технічної, організаційної та кадрової безпеки.

Б.5.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.5.2.2.1 Розробником розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією базується на автоматизованих засобах. Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Б.5.2.2.2 Запроваджена система керування конфігурацією використовується для генерації КЗЗ ОЕ з вхідного коду і обліку всіх змін з появою нових версій.

Б.5.2.2.3 Запроваджена система керування конфігурацією здатна видавати звіти про стан елементів конфігурації.

Б.5.3 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.5.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.5.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.5.3.1.2 Подані функціональні специфікації містять формалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.5.3.1.3 Матеріали технічного завдання, зазначені в п. А.2.1, погоджені з уповноваженим державним органом.

Б.5.3.1.4 У матеріалах, зазначених у п. А.2.5, з використанням результатів структурованого аналізу продемонстровано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.5.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.5.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.5.3.2.2 Матеріали ескізного проекту, зазначені в п. А.2.2, погоджені з уповноваженим державним органом.

Б.5.3.2.3 У матеріалах, зазначених у п. А.2.6, з використанням результатів структурованого аналізу продемонстровано відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.5.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.5.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.5.3.3.2 Матеріали технічного проекту, зазначені в п. А.2.3, погоджені з уповноваженим державним органом.

Б.5.3.3.3 У матеріалах, зазначених у п. А.2.7, неформалізованим чином показано відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.5.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації має передбачати перевірку таких вимог:

Б.5.3.4.1 Розробником у матеріалах, зазначених у п. А.2.4, наведено вхідний код реалізації всього КЗЗ ОЕ.

Б.5.3.4.2 Матеріали робочого проекту, зазначені в п. А.2.4, погоджені з уповноваженим державним органом.

Б.5.3.4.3 У матеріалах, зазначених у п. А.2.8, неформалізованим чином показано відповідність між детальним проектом КЗЗ ОЕ та реалізацією всього КЗЗ ОЕ.

Б.5.4 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.5.4.1 Розробником подано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.5.4.2 Існує описана в матеріалах, зазначених у п. А.2.14, система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ ОЕ, яке поставляється замовнику, точно відповідає еталонній копії.

Б.5.5 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.5.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.5.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.5.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.5.6 Вимоги до програми перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.5.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.5.6.2 Програма та методика випробувань ФПБ, документована в матеріалах, зазначених у п. А.2.18, погоджена з уповноваженим державним органом.

Б.5.6.3 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, які можуть бути перевірені шляхом повторення тестування.

Б.5.6.4 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених “слабких місць” та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”.

Б.5.6.5 Надані розробником матеріали, зазначені в пп. А.2.19 та А.2.20, підтверджують факт виконання розробником тестів з подолання механізмів захисту та доводять, що КЗЗ ОЕ є відносно стійкий до такого роду атак з боку розробника.

Б.5.6.6 До складу приймальної комісії з проведення випробувань залучаються представники уповноваженого державного органу.

Б.6 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ

Б.6.1 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.6.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.6.1.2 Усі структурні компоненти КЗЗ ОЕ (модулі), описані в матеріалах, зазначених у п. А.2.3, є добре визначеними і максимально незалежними від інших модулів. Кожний із структурних компонентів (модулів) КЗЗ спроектовано відповідно до принципу мінімуму повноважень.

Б.6.1.3 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що критичні для безпеки структурні компоненти КЗЗ ОЕ (модулі) захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня.

Б.6.1.4 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що розробником вжито заходів, спрямованих на виключення з КЗЗ ОЕ компонентів, що не є критичними для безпеки. У матеріалах, зазначених у п. А.2.3, наведені підстави для включення до КЗЗ ОЕ будь-якого елемента, який не має відношення до захисту.

Б.6.1.5 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що: розробка ПЗ переважно була спрямована на мінімізацію складності КЗЗ ОЕ; КЗЗ спроектований і структурований так, щоб використовувати повний та концептуально простий механізм захисту з точно визначеною семантикою, який відіграє центральну роль у реалізації внутрішньої структури КЗЗ; під час розробки КЗЗ були задіяні такі підходи, як модульність побудови і приховання (локалізація видимості) даних.

Б.6.2 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.6.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, яка стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, яка стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.6.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.6.2.1.2 Розробником у матеріалах, зазначених у п. А.2.10, описано стандарти кодування, яких необхідно додержуватися в процесі реалізації, та гарантовано, що всі вхідні коди компілюються відповідно до цих стандартів. Усі використовувані під час реалізації мови програмування є добре визначеними. Усі залежні від реалізації параметри мов програмування або компіляторів документовані.

Б.6.2.1.3 Розробником розроблені, запроваджені та підтримуються в робочому стані документально оформлені в матеріалах, зазначених у п. А.2.11, методики забезпечення фізичної, технічної, організаційної і кадрової безпеки.

Б.6.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.6.2.2.1 Розробником розроблені, запроваджені і підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією базується на автоматизованих засобах. Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність

між всією документацією і реалізацією поточної версії КЗЗ.

Б.6.2.2.2 Запроваджена система керування конфігурацією використовується для генерації КЗЗ ОЕ з вхідного коду і обліку всіх змін з появою нових версій.

Б.6.2.2.3 Запроваджена система керування конфігурацією здатна видавати звіти про стан елементів конфігурації.

Б.6.2.2.4 Розробником використовується описана в матеріалах, зазначених у п. А.2.11, система заходів технічної, фізичної, організаційної та кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ ОЕ, від несанкціонованої модифікації або руйнування.

Б.6.3 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.6.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.6.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.6.3.1.2 Подані функціональні специфікації містять формалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.6.3.1.3 Матеріали технічного завдання, зазначені в п. А.2.1, погоджені з уповноваженим державним органом.

Б.6.3.1.4 У матеріалах, зазначених у п. А.2.5, з використанням результатів структурованого аналізу продемонстровано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.6.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.6.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у формалізованому вигляді. Поданий проект архітектури містить перелік та опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.6.3.2.2 Матеріали ескізного проекту, зазначені в п. А.2.2, погоджені з уповноваженим державним органом.

Б.6.3.2.3 У матеріалах, зазначених у п. А.2.6, формально доведено відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.6.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.6.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у частково формалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.6.3.3.2 Матеріали технічного проекту, зазначені в п. А.2.3, погоджені з уповноваженим

державним органом.

Б.6.3.3.3 У матеріалах, зазначених у п. А.2.7, з використанням результатів структурованого аналізу продемонстровано відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.6.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації має передбачати перевірку таких вимог:

Б.6.3.4.1 Розробником у матеріалах, зазначених у п. А.2.4, наведено вхідний код реалізації всього КЗЗ ОЕ.

Б.6.3.4.2 Матеріали робочого проекту, зазначені в п. А.2.4, погоджені з уповноваженим державним органом.

Б.6.3.4.3 У матеріалах, зазначених у п. А.2.8, неформалізованим чином показано відповідність між детальним проектом КЗЗ ОЕ та реалізацією всього КЗЗ ОЕ.

Б.6.4 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.6.4.1 Розробником подано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску ОЕ.

Б.6.4.2 Існує описана в матеріалах, зазначених у п. А.2.14, система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ ОЕ, яке поставляється замовнику, точно відповідає еталонній копії.

Б.6.4.3 Існує описана в матеріалах, зазначених у п. А.2.14, система керування розповсюдженням захищеного ОЕ, яка забезпечує підтримку відповідності між КЗЗ ОЕ, що поставляється замовнику, і його еталонною копією.

Б.6.5 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.6.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.6.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.6.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.6.6 Вимоги до програми перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.6.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для

підтвердження достатності тестового покриття.

Б.6.6.2 Програма та методика випробувань ФПБ, документована в матеріалах, зазначених у п. А.2.18, погоджена з уповноваженим державним органом.

Б.6.6.3 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, які можуть бути перевірені шляхом повторення тестування.

Б.6.6.4 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених "слабких місць" та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові "слабкі місця ".

Б.6.6.5 Надані розробником матеріали, зазначені в пп. А.2.19 та А.2.20, підтверджують факт виконання розробником тестів з подолання механізмів захисту та доводять, що КЗЗ ОЕ є абсолютно стійкий до такого роду атак з боку розробника.

Б.6.6.6 До складу приймальної комісії з проведення випробувань залучаються представники уповноваженого державного органу.

Б.7 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ

Б.7.1 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо архітектури

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо архітектури має передбачати перевірку таких вимог:

Б.7.1.1 КЗЗ ОЕ реалізує політику безпеки, визначену в матеріалах, зазначених у п. А.2.1. У матеріалах, зазначених у п. А.2.2, чітко визначені всі функціональні компоненти (підсистеми), а в матеріалах, зазначених у п. А.2.3 – всі структурні компоненти КЗЗ ОЕ (модулі).

Б.7.1.2 Усі структурні компоненти КЗЗ ОЕ (модулі), описані в матеріалах, зазначених у п. А.2.3, є добре визначеними і максимально незалежними від інших модулів. Кожний із структурних компонентів (модулів) КЗЗ спроектовано відповідно до принципу мінімуму повноважень.

Б.7.1.3 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що критичні для безпеки структурні компоненти КЗЗ ОЕ (модулі) захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня.

Б.7.1.4 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що розробником вжито заходів, спрямованих на виключення з КЗЗ ОЕ компонентів, що не є критичними для безпеки. У матеріалах, зазначених у п. А.2.3, наведені підстави для включення до КЗЗ ОЕ будь-якого елемента, який не має відношення до захисту.

Б.7.1.5 Зміст матеріалів, зазначених у п. А.2.3, підтверджує, що: розробка ПЗ переважно була спрямована на мінімізацію складності КЗЗ ОЕ; КЗЗ спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою, який відіграє центральну роль в реалізації внутрішньої структури КЗЗ; під час розробки КЗЗ були задіяні такі підходи, як модульність побудови і приховання (локалізація видимості) даних.

Б.7.2 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки

Б.7.2.1 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, має передбачати перевірку таких вимог:

Б.7.2.1.1 Розробником визначено всі стадії життєвого циклу ОЕ, розроблені, запроваджені та підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.9, методики діяльності на кожній стадії життєвого циклу ОЕ. У матеріалах, зазначених у п. А.2.9, документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги.

Б.7.2.1.2 Розробником у матеріалах, зазначених у п. А.2.10, описано стандарти кодування, яких необхідно додержуватися в процесі реалізації, та гарантовано, що всі вхідні коди компілюються відповідно до цих стандартів. Усі використовувані під час реалізації мови програмування є добре

визначеними. Усі залежні від реалізації параметри мов програмування або компіляторів документовані.

Б.7.2.1.3 Розробником розроблені, запроваджені і підтримуються в робочому стані документально оформлені в матеріалах, зазначених у п. А.2.11, методики забезпечення фізичної, технічної, організаційної та кадрової безпеки.

Б.7.2.2 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, яка стосується керування конфігурацією, має передбачати перевірку таких вимог:

Б.7.2.2.1 Розробником розроблені, запроваджені і підтримуються в робочому стані документовані в матеріалах, зазначених у п. А.2.12, методики щодо керування конфігурацією ОЕ на всіх стадіях його життєвого циклу (система керування конфігурацією). Система керування конфігурацією базується на автоматизованих засобах. Система керування конфігурацією забезпечує керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією гарантує постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Б.7.2.2.2 Запроваджена система керування конфігурацією використовується для генерації КЗЗ ОЕ з вхідного коду і обліку всіх змін з появою нових версій.

Б.7.2.2.3 Запроваджена система керування конфігурацією здатна видавати звіти про стан елементів конфігурації.

Б.7.2.2.4 Розробником використовується описана в матеріалах, зазначених у п. А.2.11, система заходів технічної, фізичної, організаційної та кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ ОЕ, від несанкціонованої модифікації або руйнування.

Б.7.3 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки

Б.7.3.1 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій має передбачати перевірку таких вимог:

Б.7.3.1.1 Розробником на стадії розроблення технічного завдання розроблено та в матеріалах, зазначених у п. А.2.1, наведено функціональні специфікації КЗЗ ОЕ. Подані функціональні специфікації містять неформалізований опис політики безпеки, що реалізується КЗЗ, а також перелік і опис ФПБ, що надаються КЗЗ ОЕ.

Б.7.3.1.2 Подані функціональні специфікації містять формалізований опис моделі політики безпеки, що реалізується КЗЗ ОЕ.

Б.7.3.1.3 Матеріали технічного завдання, зазначені в п. А.2.1, погоджені з уповноваженим державним органом.

Б.7.3.1.4 У матеріалах, зазначених у п. А.2.5, з використанням результатів структурованого аналізу продемонстровано відповідність між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки, що реалізується КЗЗ ОЕ.

Б.7.3.2 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури має передбачати перевірку таких вимог:

Б.7.3.2.1 Розробником на стадії розробки ескізного проекту розроблено та в матеріалах, зазначених у п. А.2.2, наведено проект архітектури КЗЗ ОЕ, викладений у формалізованому вигляді. Поданий проект архітектури містить перелік і опис функціональних компонентів (підсистем) КЗЗ і функцій, що реалізуються ними. У поданому проекті архітектури описані будь-які використовувані

зовнішні послуги безпеки. У поданому проекті архітектури в термінах винятків, повідомлень про помилки і кодів повернення описані зовнішні інтерфейси КЗЗ.

Б.7.3.2.2 Матеріали ескізного проекту, зазначені в п. А.2.2, погоджені з уповноваженим державним органом.

Б.7.3.2.3 У матеріалах, зазначених у п. А.2.6, формально доведено відповідність між моделлю політики безпеки, що реалізується КЗЗ ОЕ, та проектом архітектури КЗЗ ОЕ.

Б.7.3.3 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту має передбачати перевірку таких вимог:

Б.7.3.3.1 Розробником на стадії технічного проекту або робочого проекту розроблено та в матеріалах, зазначених у п. А.2.3, наведено детальний проект КЗЗ ОЕ, викладений у формалізованому вигляді. Поданий детальний проект містить перелік всіх структурних компонентів (модулів) КЗЗ ОЕ і точний опис функціонування всіх механізмів, використовуваних для реалізації цими компонентами ФПБ. У поданому детальному проекті описані призначення і параметри інтерфейсів всіх структурних компонентів (модулів).

Б.7.3.3.2 Матеріали технічного проекту, зазначені в п. А.2.3, погоджені з уповноваженим державним органом.

Б.7.3.3.3 У матеріалах, зазначених у п. А.2.7, формально доведено відповідність між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ.

Б.7.3.4 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації має передбачати перевірку таких вимог:

Б.7.3.4.1 Розробником у матеріалах, зазначених у п. А.2.4, наведено вхідний код реалізації всього КЗЗ ОЕ та всіх бібліотек часу виконання.

Б.7.3.4.2 Матеріали робочого проекту, зазначені в п. А.2.4, погоджені з уповноваженим державним органом.

Б.7.3.4.3 У матеріалах, зазначених у п. А.2.8, з використанням результатів структурованого аналізу продемонстровано відповідність між детальним проектом КЗЗ ОЕ та реалізацією всього КЗЗ ОЕ.

Б.7.4 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища функціонування

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища функціонування має передбачати перевірку таких вимог:

Б.7.4.1 Розробником подано описані в матеріалах, зазначених у пп. А.2.13 та А.2.16, засоби інсталяції, генерації та запуску ОЕ, які гарантують, що експлуатація ОЕ починається з безпечного стану. У матеріалах, зазначених у пп. А.2.13 та А.2.16, наведено перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

Б.7.4.2 Існує описана в матеріалах, зазначених у п. А.2.14, система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ ОЕ, яке поставляється замовнику, точно відповідає еталонній копії.

Б.7.4.3 Існує описана в матеріалах, зазначених у п. А.2.14, система керування розповсюдженням захищеного ОЕ, яка забезпечує підтримку відповідності між КЗЗ ОЕ, що поставляється замовнику, і його еталонною копією.

Б.7.5 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації має передбачати перевірку таких вимог:

Б.7.5.1 Розробником у матеріалах, зазначених у п. А.2.15, наведено опис ФПБ, що реалізуються КЗЗ ОЕ, в якому, зокрема, викладені основні необхідні для правильного використання ФПБ

принципи політики безпеки, що реалізується КЗЗ ОЕ, а також самі послуги.

Б.7.5.2 Розробником у матеріалах, зазначених у п. А.2.16, наведено настанови адміністратору щодо послуг безпеки, в яких, зокрема, міститься опис засобів інсталяції, генерації та запуску ОЕ, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ, опис властивостей ОЕ, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ ОЕ, а також інструкції щодо використання адміністратором ФПБ для підтримки політики безпеки, прийнятої в організації, що експлуатує ОЕ.

Б.7.5.3 Розробником у матеріалах, зазначених у п. А.2.17, наведено настанови користувачу щодо послуг безпеки, в яких, зокрема, містяться інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Б.7.6 Вимоги до програми перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Програма перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту має передбачати перевірку таких вимог:

Б.7.6.1 Надані розробником матеріали, зазначені в п. А.2.18, містять програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують ФПБ, а також аргументи для підтвердження достатності тестового покриття.

Б.7.6.2 Програма та методика випробувань ФПБ, документована в матеріалах, зазначених у п. А.2.18, погоджена з уповноваженим державним органом.

Б.7.6.3 Надані розробником матеріали, зазначені в п. А.2.19, містять докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, які можуть бути перевірені шляхом повторення тестування.

Б.7.6.4 Надані розробником матеріали, зазначені в п. А.2.19, підтверджують факт усунення або нейтралізації розробником усіх знайдених “слабких місць” та виконання повторного тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця”.

Б.7.6.5 Надані розробником матеріали, зазначені в пп. А.2.19 та А.2.20, підтверджують факт виконання розробником тестів з подолання механізмів захисту та доводять, що КЗЗ ОЕ є абсолютно стійкий до такого роду атак з боку розробника.

Б.7.6.6 До складу приймальної комісії з проведення випробувань залучаються представники уповноваженого державного органу.

Додаток В
Вимоги щодо змісту методики перевірки дотримання вимог різних рівнів гарантій коректності реалізації функціональних послуг безпеки
(рекомендований)

У Додатку у викладені специфічні вимоги щодо змісту методики перевірки дотримання вимог різних рівнів гарантій коректності реалізації ФПБ. Вимоги викладені з урахуванням вимог НД ТЗІ 2.5-004-99 щодо різних рівнів гарантій коректності реалізації ФПБ, а також з урахуванням рекомендацій щодо складу та змісту матеріалів (документів), які надаються розробником експерту для оцінювання рівня гарантій коректності реалізації ФПБ, наведених у додатку А, та вимог до змісту програми перевірки дотримання вимог різних рівнів гарантій коректності реалізації ФПБ, викладених у додатку Б.

В.1 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ

В.1.1 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо архітектури

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.1, має передбачати виконання експертом:

В.1.1.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі функціональні компоненти (підсистеми) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.1.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі структурні компоненти (модулі) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.1.1.3 Перевірки факту наявності в складі наданого на експертизу ОЕ всіх визначених у матеріалах, зазначених у п. А.2.3, структурних компонентів (модулів) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.1.2 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки

В.1.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.2.1, має передбачати виконання експертом:

В.1.2.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.9, опису використовуваної моделі життєвого циклу ОЕ з метою формулювання висновку про те, чи визначені в ньому всі етапи кожної стадії життєвого циклу ОЕ.

В.1.2.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи поширюються вони на всі задачі, вирішувані розробником у процесі розроблення та супроводження ОЕ, та чи надає їх застосування необхідний позитивний вплив на процеси розроблення і супроводження ОЕ, дозволяючи мінімізувати імовірність виникнення недоліків, що мають відношення до захищеності оброблюваної інформації.

В.1.2.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи забезпечує їх застосування достатній рівень захищеності ОЕ та безпеки середовища його розробки й експлуатації.

В.1.2.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на етапі експлуатації (супроводження) ОЕ з метою

формулювання обґрунтованого висновку про те, чи дозволяють вони в найкоротший термін та з мінімальним тимчасовим зниженням рівня захищеності усунути виявлені недоліки.

В.1.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.2.2, має передбачати виконання експертом:

В.1.2.2.1 Перевірки наданих матеріалів, зазначених у пп. А.2.1-А.2.4, А.2.12, А.2.13, А.2.15-А.2.18, з метою формулювання висновку про те, що всі вони позначені унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.1.2.2.2 Перевірки наданого на експертизу ОЕ з метою формулювання висновку про те, що він позначений унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.1.2.2.3 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить список елементів конфігурації.

В.1.2.2.4 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план керування конфігурацією.

В.1.2.2.5 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план приймання елементів конфігурації під керування системи керування конфігурацією.

В.1.2.2.6 Перевірки переліку наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить опис процедур компонування елементів конфігурації до складу ОЕ.

В.1.2.2.7 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входять вихідні матеріали системи керування конфігурацією.

В.1.2.2.8 Перевірки складу наданого списку елементів конфігурації з метою формулювання висновку про те, що в ньому унікально ідентифіковані всі елементи, які складають сферу дії системи керування конфігурацією.

В.1.2.2.9 Дослідження наданого списку елементів конфігурації з метою формулювання обґрунтованого висновку про те, що в ньому як елементи конфігурації ідентифіковані всі структурні компоненти (модулі) ОЕ, які входять до складу КЗЗ ОЕ.

В.1.2.2.10 Дослідження описаних у документації керування конфігурацією, зазначеної в п. А.2.12, правил унікальної ідентифікації елементів конфігурації з метою формулювання обґрунтованого висновку про те, що вони є несуперечливими та забезпечують однозначну ідентифікацію відповідних елементів конфігурації.

В.1.2.2.11 Дослідження наданого плану керування конфігурацією з метою формулювання обґрунтованого висновку про те, що описаний у ньому порядок використання системи керування конфігурацією забезпечує впевненість у цілісності елементів конфігурації ОЕ, починаючи від початкових етапів проектування та закінчуючи завершенням його експлуатації.

В.1.2.2.12 Дослідження наданого плану приймання елементів конфігурації під керування системи керування конфігурацією з метою формулювання обґрунтованого висновку про те, що в ньому визначені критерії та процедури введення розробленого або зміненого елемента конфігурації до складу поточної версії ОЕ.

В.1.2.2.13 Дослідження наданого опису процедур компонування елементів конфігурації до складу ОЕ з метою формулювання обґрунтованого висновку про те, що він у достатньому обсязі містить відомості про всі необхідні дії, які мають бути виконані за допомогою використовуваних інструментальних засобів розробки при веденні створеного або модифікованого елемента конфігурації до складу ОЕ.

В.1.2.2.14 Дослідження наданих вихідних матеріалів системи керування конфігурацією з

метою формулювання обґрунтованого висновку про те, що система керування конфігурацією використовується згідно з планом керування конфігурацією.

В.1.2.2.15 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ процедур системи керування конфігурацією стосовно елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації, з метою формулювання висновку про факт застосування системи керування конфігурацією.

В.1.3 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.1.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.3.1, має передбачати виконання експертом:

В.1.3.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній викладені вимоги до КЗЗ ОЕ у вигляді набору вимог до реалізованих ФПБ.

В.1.3.1.2 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що вимоги до КЗЗ ОЕ викладені в ній оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99.

В.1.3.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені в ній згідно з вимогами НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.1.3.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про її внутрішню несуперечність.

В.1.3.1.5 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про повноту викладення вимог до ФПБ з точки зору вимог НД ТЗІ 2.5-004-99 до відповідних ФПБ відповідних рівнів.

В.1.3.1.6 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені з урахуванням необхідних умов, визначених у НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.1.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.3.2, має передбачати виконання експертом:

В.1.3.2.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних функціональних компонентів (підсистем).

В.1.3.2.2 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного функціонального компонента (підсистеми) КЗЗ у частині, що стосується реалізації ФПБ.

В.1.3.2.3 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ.

В.1.3.2.4 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься

опис усіх функцій, підтримуваних механізмами захисту, реалізованими базовими апаратними, програмно-апаратними та/або програмними засобами.

В.1.3.2.5 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ.

В.1.3.2.6 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.1.3.2.7 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому для кожного інтерфейсу функціонального компонента (підсистеми) наведені призначення, методи використання інтерфейсу, повідомлення про помилки, коди повернення з деталізацією, за необхідності, результатів використання та можливих позаштатних ситуацій (винятків).

В.1.3.2.8 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс) міститься опис порядку захищеного функціонування цього компонента (підсистеми) КЗЗ ОЕ, що містить опис будь-яких операцій, виконання яких може бути призначено функціональному компоненту (підсистемі) КЗЗ, з огляду на його функції та його вплив на захищений стан ОЕ.

В.1.3.2.9 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті, що не входить до складу КЗЗ ОЕ, у відповідь на ініціюючий вплив на відповідний інтерфейс) описані всі використовувані функціональними компонентами (підсистемами) КЗЗ ОЕ зовнішні послуги безпеки.

В.1.3.2.10 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому визначений порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.1.3.2.11 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.1.3.2.12 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ ОЕ викладено в неформалізованому вигляді оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99.

В.1.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.3.3, має передбачати виконання експертом:

В.1.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.1.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.1.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними

компонентами (модулями), що входять до складу КЗЗ.

В.1.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ.

В.1.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.1.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.1.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.1.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.1.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.1.3.3.10 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено в неформалізованому вигляді оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99.

В.1.4 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища функціонування

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.4, має передбачати виконання експертом:

В.1.4.1 Перевірки документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання висновку про те, що в складі ОЕ наявні засоби, які реалізують ці процедури.

В.1.4.2 Перевірки факту працездатності засобів, які реалізують процедури безпечної інсталяції, генерації та запуску ОЕ, документовані в матеріалах, зазначених у пп. А.2.13 та А.2.16.

В.1.4.3 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що в них визначені всі можливі параметри конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

В.1.4.4 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що застосування цих процедур та засобів їх реалізації гарантує, що експлуатація ОЕ починається з безпечного стану.

В.1.5 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації

В.1.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.5.1, має передбачати виконання експертом:

В.1.5.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання висновку про те, що в ньому відображені вимоги до апаратного середовища функціонування ОЕ та існуючі обмеження на використовувані в ньому апаратні засоби.

В.1.5.1.2 Перевірки документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання висновку про те, що в ньому відображені вимоги до програмного середовища функціонування ОЕ та існуючі обмеження на використовувані в ньому програмні засоби.

В.1.5.1.3 Перевірки документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання висновку про те, що в ньому визначені проблеми (цілі) забезпечення безпеки інформації, вирішення яких покладається на ОЕ.

В.1.5.1.4 Перевірки документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання висновку про те, що в ньому визначені завдання захисту, вирішення яких забезпечується ОЕ.

В.1.5.1.5 Дослідження документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання обґрунтованого висновку про те, що в ньому міститься високорівневе визначення переліку та політики ФПБ, заявлених розробником як такі, що призначені для вирішення визначених завдань захисту.

В.1.5.1.6 Дослідження документованого в матеріалах, зазначених у п. А.2.15, опису послуг безпеки, реалізованих КЗЗ оцінюваного ОЕ, з метою формулювання обґрунтованого висновку про те, що в ньому міститься неформалізований опис порядку реалізації кожної ФПБ на рівні деталізації, необхідному для розуміння основних принципів її реалізації.

В.1.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.5.2, має передбачати виконання експертом:

В.1.5.2.1 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них містяться інструкції з використання послуг безпеки для кожної адміністративної ролі, підтримуваної КЗЗ ОЕ.

В.1.5.2.2 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них містяться інструкції адміністратору з виконання функцій адміністрування, використовуваних у процесі інсталяції, генерації та запуску ОЕ.

В.1.5.2.3 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них містяться інструкції адміністратору з виконання функцій адміністрування, використовуваних у штатному режимі функціонування ОЕ.

В.1.5.2.4 Дослідження документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання обґрунтованого висновку про те, що наведені в ньому інструкції адміністратору з виконання функцій адміністрування містять інформацію про метод (методи) виклику інтерфейсу до використовуваних ним засобів КЗЗ ОЕ.

В.1.5.2.5 Дослідження документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання обґрунтованого висновку про те, що наведені в них інструкції адміністратору з виконання функцій адміністрування містять інформацію про параметри, які встановлюються адміністратором при викликах інтерфейсу до засобів КЗЗ ОЕ, їх допустимих значеннях та значеннях за замовченням.

В.1.5.2.6 Дослідження документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання обґрунтованого висновку про те, що наведені в них інструкції адміністратору з виконання функцій адміністрування містять інформацію про повідомлення або коди повернення, які формуються КЗЗ ОЕ у відповідь на виклики інтерфейсу до засобів КЗЗ ОЕ.

В.1.5.2.7 Перевірки факту реалізації в ОЕ інтерфейсу до використовуваних адміністратором засобів КЗЗ ОЕ, документованих у матеріалах, зазначених у п. А.2.16.

В.1.5.2.8 Дослідження документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання обгрунтованого висновку про те, що в них міститься опис усіх параметрів безпеки, контрольованих адміністратором, із зазначенням, за необхідності, їх безпечних значень.

В.1.5.2.9 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них міститься опис вимог до порядку роботи з ОЕ користувачів – не адміністраторів (або користувачів, призначених на інші адміністративні ролі), дотримання яких має контролюватися адміністратором.

В.1.5.2.10 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них містяться попередження щодо функцій та привілеїв, використання яких користувачами – не адміністраторами (або користувачами, призначеними на інші адміністративні ролі) слід контролювати з метою забезпечення безпечного функціонування ОЕ.

В.1.5.2.11 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них міститься опис усіх типів подій, що мають відношення до безпеки та реєструються КЗЗ, у тому числі події, пов'язані з виконанням функцій адміністрування, наявність яких має контролюватися адміністратором, із зазначенням дій, які необхідно виконати (якщо буде потрібно) для підтримання безпечного функціонування ОЕ.

В.1.5.2.12 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них міститься опис засобів ОЕ та реалізованих ними функцій, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ.

В.1.5.2.13 Перевірки документованих у матеріалах, зазначених у п. А.2.16, настанов адміністратору з послуг безпеки з метою формулювання висновку про те, що в них міститься опис усіх вимог безпеки до середовища функціонування ОЕ, які повинні контролюватися адміністратором організаційними заходами.

В.1.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.5.3, має передбачати виконання експертом:

В.1.5.3.1 Перевірки документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання висновку про те, що в них містяться інструкції з використання послуг безпеки для кожної користувальницької ролі, підтримуваної КЗЗ ОЕ.

В.1.5.3.2 Перевірки документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання висновку про те, що в них міститься опис усіх функціональних можливостей ОЕ, що стосуються забезпечення безпеки, реалізованих функцій захисту та інтерфейсів до цих функцій, доступних користувачу.

В.1.5.3.3 Дослідження документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання обгрунтованого висновку про те, що наведені в них інструкції користувачу містять інформацію про метод (методи) виклику інтерфейсу до використовуваних ним засобів КЗЗ ОЕ.

В.1.5.3.4 Дослідження документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання обгрунтованого висновку про те, що наведені в них інструкції користувачу містять інформацію про параметри, які встановлюються користувачем при викликах інтерфейсу до засобів КЗЗ ОЕ, їх допустимих значеннях та значеннях за замовченням.

В.1.5.3.5 Дослідження документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання обгрунтованого висновку про те, що наведені в них інструкції користувачу містять інформацію про повідомлення або коди повернення, які формуються КЗЗ ОЕ у відповідь на виклики інтерфейсу до засобів КЗЗ ОЕ.

В.1.5.3.6 Перевірки факту реалізації в ОЕ інтерфейсу до використовуваних користувачем засобів КЗЗ ОЕ, документованих у матеріалах, зазначених у п. А.2.16.

В.1.5.3.7 Дослідження документованих у матеріалах, зазначених у п. А.2.17, настанов

користувачу з послуг безпеки з метою формулювання обґрунтованого висновку про те, що в них міститься опис вимог до порядку роботи користувачів з ОЕ, який містить роз'яснення ролі користувачів у процесі підтримання безпечного функціонування ОЕ, а також зміст обов'язків користувачів із забезпечення безпечного функціонування ОЕ.

В.1.5.3.8 Перевірки документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання висновку про те, що в них містяться попередження щодо доступних користувачу функцій та привілеїв, які слід контролювати в безпечному середовищі експлуатації.

В.1.5.3.9 Дослідження документованих у матеріалах, зазначених у п. А.2.17, настанов користувачу з послуг безпеки з метою формулювання обґрунтованого висновку про те, що в них містяться рекомендації щодо ефективного використання функцій захисту.

В.1.6 Вимоги до методики перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Методика перевірки дотримання вимог рівня Г-1 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.1.6, має передбачати виконання експертом:

В.1.6.1 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться процедури випробувань засобів, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

В.1.6.2 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99 до політики та порядку функціонування засобів, що реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих ФПБ та охопленням усіх об'єктів КЗЗ та засобів (компонентів) КЗЗ, на які поширюється ця політика.

В.1.6.3 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99, які стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, зазначених у функціональній специфікації КЗЗ ОЕ.

В.1.6.4 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться відомості, які підтверджують, що перевірялися засоби реалізації всіх ФПБ, зазначених у функціональній специфікації КЗЗ.

В.1.6.5 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ.

В.1.6.6 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

В.1.6.7 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них, з посиланням на відповідні пункти програми та методики випробувань, наведені 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 КЗЗ ОЕ певних ФПБ.

В.1.6.8 Вибіркових перевірок ФПБ, передбачених програмою та методикою випробувань, документованою в матеріалах, зазначених у п. А.2.18, з метою формулювання висновку про те, що отримані результати виконаних перевірок відповідають наведеним у протоколах випробувань, документованих у матеріалах, зазначених у п. А.2.19.

В.2 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ

В.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо архітектури

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.1, повністю співпадають з вимогами, викладеними в п. В.1.1.

В.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки

В.2.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.2.1, повністю співпадають з вимогами, викладеними в п. В.1.2.1.

В.2.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.2.2, повністю співпадають з вимогами, викладеними в п. В.1.2.2.

В.2.3 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.2.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Методика перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.3.1, має передбачати виконання експертом:

В.2.3.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній викладені вимоги до КЗЗ ОЕ у вигляді набору вимог до реалізованих ФПБ.

В.2.3.1.2 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що вимоги до КЗЗ ОЕ викладені в ній оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99.

В.2.3.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені в ній згідно з вимогами НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.2.3.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про її внутрішню несуперечність.

В.2.3.1.5 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про повноту викладення вимог до ФПБ з точки зору вимог НД ТЗІ 2.5-004-99 до відповідних ФПБ відповідних рівнів.

В.2.3.1.6 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені з урахуванням необхідних умов, визначених у НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.2.3.1.7 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису моделі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній наявні

моделі політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.2.3.1.8 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що в моделях політик усіх ФПБ чітко визначені характеристики модельованого режиму захищеного функціонування ОЕ.

В.2.3.1.9 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що модельований режим захищеного функціонування ОЕ не суперечить політикам ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.2.3.1.10 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про повноту модельованого режиму захищеного функціонування ОЕ відносно політик ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.2.3.1.11 Перевірки документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що описи моделей політик ФПБ викладені в неформалізованому вигляді оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99.

В.2.3.1.12 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком описаних у політиці безпеки та промодельованих ФПБ.

В.2.3.1.13 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.2.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Методика перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.3.2, має передбачати виконання експертом:

В.2.3.2.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних функціональних компонентів (підсистем).

В.2.3.2.2 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного функціонального компонента (підсистеми) КЗЗ у частині, що стосується реалізації ФПБ.

В.2.3.2.3 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ.

В.2.3.2.4 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис усіх функцій, підтримуваних механізмами захисту, реалізованими базовими апаратними, програмно-апаратними та/або програмними засобами.

В.2.3.2.5 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси

функціональних компонентів (підсистем) КЗЗ ОЕ.

В.2.3.2.6 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.2.3.2.7 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу функціонального компонента (підсистеми) наведені призначення, методи використання інтерфейсу, повідомлення про помилки, коди повернення з деталізацією, за необхідності, результатів використання та можливих позаштатних ситуацій (винятків).

В.2.3.2.8 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс) міститься опис порядку захищеного функціонування цього компонента (підсистеми) КЗЗ ОЕ, що містить опис будь-яких операцій, виконання яких може бути призначено функціональному компоненту (підсистемі) КЗЗ, з огляду на його функції та його вплив на захищений стан ОЕ.

В.2.3.2.9 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті, що не входить до складу КЗЗ ОЕ, у відповідь на ініціююче вплив на відповідний інтерфейс) описані всі використовувані функціональними компонентами (підсистемами) КЗЗ ОЕ зовнішні послуги безпеки.

В.2.3.2.10 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.2.3.2.11 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.2.3.2.12 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ ОЕ викладено в неформалізованому вигляді оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99.

В.2.3.2.13 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком промодельованих ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ.

В.2.3.2.14 Дослідження документованих у матеріалах, зазначених у п. А.2.6, результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.2.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.3.3, має передбачати виконання експертом:

В.2.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.2.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.2.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), що входять до складу КЗЗ.

В.2.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ.

В.2.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.2.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.2.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.2.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначений порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.2.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.2.3.3.10 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено в неформалізованому вигляді оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99.

В.2.3.3.11 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем.

В.2.3.3.12 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.2.4 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності

реалізації ФПБ щодо середовища функціонування

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.4, повністю співпадають з вимогами, викладеними в п. В.1.4.

В.2.5 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації

В.2.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.2.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.2.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.2.6 Вимоги до методики перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Методика перевірки дотримання вимог рівня Г-2 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.2.6, має передбачати виконання експертом:

В.2.6.1 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться процедури випробувань засобів, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

В.2.6.2 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99 до політики та порядку функціонування засобів, що реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих ФПБ та охопленням усіх об'єктів КЗЗ та засобів (компонентів) КЗЗ, на які поширюється ця політика.

В.2.6.3 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99, які стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, зазначених у функціональній специфікації КЗЗ ОЕ.

В.2.6.4 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться відомості, які підтверджують, що перевірялися засоби реалізації всіх ФПБ, зазначених у функціональній специфікації КЗЗ.

В.2.6.5 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ.

В.2.6.6 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході

виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

В.2.6.7 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них, з посиланням на відповідні пункти програми та методики випробувань, наведені 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 КЗЗ ОЕ певних ФПБ.

В.2.6.8 Вибіркових перевірок ФПБ, передбачених програмою та методикою випробувань, документованою в матеріалах, зазначених у п. А.2.18, з метою формулювання висновку про те, що отримані результати виконаних перевірок відповідають наведеним у протоколах випробувань, документованих у матеріалах, зазначених у п. А.2.19.

В.2.6.9 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них, з посиланням на відповідні пункти програми та методики випробувань, наведені підстави, які дають або не дають змоги дійти висновку щодо успішності здійснення перевірок для всіх ФПБ, наведених у функціональній специфікації КЗЗ ОЕ, у тому числі тих ФПБ, попередні перевірки яких були визнані неуспішними.

В.3 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ

В.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо архітектури

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.1, має передбачати виконання експертом:

В.3.1.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі функціональні компоненти (підсистеми) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.3.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі структурні компоненти (модулі) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.3.1.3 Перевірки факту наявності в складі наданого на експертизу ОЕ всіх визначених у матеріалах, зазначених у п. А.2.3, структурних компонентів (модулів) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.3.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ наведено його призначення, реалізовані функції, інтерфейси, залежності від інших модулів та порядок реалізації всіх ФПБ, до реалізації яких має відношення цей компонент (модуль), а також порядок взаємодії з іншими модулями.

В.3.1.5 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою уникнення зайвої взаємодії з іншими модулями) максимальна незалежність цього компонента (модуля) від інших модулів.

В.3.1.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою мінімізації імовірності використання порушником надлишкових повноважень) реалізація вимог мінімуму повноважень.

В.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки

В.3.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.2.1, має передбачати виконання експертом:

В.3.2.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.9, опису використовуваної моделі життєвого циклу ОЕ з метою формулювання висновку про те, чи визначені в ньому всі етапи кожної стадії життєвого циклу ОЕ.

В.3.2.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи поширюються вони на всі завдання, вирішувані розробником у процесі розроблення та супроводження ОЕ, та чи надає їх застосування необхідний позитивний вплив на процеси розроблення і супроводження ОЕ, дозволяючи мінімізувати імовірність виникнення недоліків, що мають відношення до захищеності оброблюваної інформації.

В.3.2.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи забезпечує їх застосування достатній рівень захищеності ОЕ та безпеки середовища його розробки й експлуатації.

В.3.2.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на етапі експлуатації (супроводження) ОЕ з метою формулювання обґрунтованого висновку про те, чи дозволяють вони в найкоротший термін та з мінімальним тимчасовим зниженням рівня захищеності усунути виявлені недоліки.

В.3.2.1.5 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, що в ній визначені всі стандарти кодування, реалізовані інструментальними засобами, які використовуються для розроблення, аналізу та реалізації ОЕ.

В.3.2.1.6 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, що всі мови програмування й інструментальні засоби, використовувані для розроблення, аналізу і реалізації ОЕ, добре визначені.

В.3.2.1.7 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи однозначно визначені в ній значення всіх конструкцій, використовуваних у вхідному коді програмного забезпечення КЗЗ ОЕ, та чи надано для кожної такої конструкції чітке й однозначне визначення її призначення та результатів її виконання.

В.3.2.1.8 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи однозначно визначене в ній використання всіх залежних від конкретної реалізації інструментальних засобів параметрів мов програмування та/або компіляторів, що можуть уплинути на виконуваний код або відрізняються від стандарту використовуваної мови.

В.3.2.1.9 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи описані в ній усі параметри розроблювальних апаратних засобів, що впливають на результати застосування цих інструментальних засобів.

В.3.2.1.10 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи підтримують використовувані інструментальні засоби можливість коректної реалізації ОЕ згідно з визначеними в ній стандартами кодування.

В.3.2.1.11 Дослідження матеріалів робочого проекту (реалізації), зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, чи застосовувалися в процесі їх розроблення інструментальні засоби та стандарти кодування, документовані в матеріалах, зазначених у п. А.2.10.

В.3.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації

ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.2.2, повністю співпадають з вимогами, викладеними в п. В.1.2.2.

В.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.3.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.3.1, має передбачати виконання експертом:

В.3.3.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній викладені вимоги до КЗЗ ОЕ у вигляді набору вимог до реалізованих ФПБ.

В.3.3.1.2 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що вимоги до КЗЗ ОЕ викладені в ній оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99.

В.3.3.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені в ній згідно з вимогами НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.3.3.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про її внутрішню несуперечність.

В.3.3.1.5 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про повноту викладення вимог до ФПБ з точки зору вимог НД ТЗІ 2.5-004-99 до відповідних ФПБ відповідних рівнів.

В.3.3.1.6 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені з урахуванням необхідних умов, визначених у НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.3.3.1.7 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису моделі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній наявні моделі політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.3.3.1.8 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що в моделях політик усіх ФПБ чітко визначені характеристики модельованого режиму захищеного функціонування ОЕ.

В.3.3.1.9 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що модельований режим захищеного функціонування ОЕ не суперечить політикам ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.3.3.1.10 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про повноту модельованого режиму захищеного функціонування ОЕ відносно політик ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.3.3.1.11 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що описи моделей політик ФПБ викладені в частково формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному

допоміжними поясненнями, поданими в неформалізованому вигляді.

В.3.3.1.12 Перевірки матеріалів технічного завдання, зазначених у п. А.2.1, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.3.3.1.13 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком описаних у політиці безпеки та промодельованих ФПБ.

В.3.3.1.14 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.3.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.3.2, має передбачати виконання експертом:

В.3.3.2.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних функціональних компонентів (підсистем).

В.3.3.2.2 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного функціонального компонента (підсистеми) КЗЗ у частині, що стосується реалізації ФПБ.

В.3.3.2.3 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ.

В.3.3.2.4 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис усіх функцій, підтримуваних механізмами захисту, реалізованими базовими апаратними, програмно-апаратними та/або програмними засобами.

В.3.3.2.5 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ.

В.3.3.2.6 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.3.3.2.7 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу функціонального компонента (підсистеми) наведені призначення, методи використання інтерфейсу, повідомлення про помилки, коди повернення з деталізацією, за необхідності, результатів використання та можливих позаштатних ситуацій (винятків).

В.3.3.2.8 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс) міститься опис порядку захищеного функціонування цього компонента (підсистеми) КЗЗ ОЕ, що містить опис будь-яких операцій, виконання яких може бути призначено функціональному компоненту (підсистемі) КЗЗ, з огляду на його функції та його вплив на захищений стан ОЕ.

В.3.3.2.9 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті, що не входить до

складу КЗЗ ОЕ, у відповідь на ініціююче вплив на відповідний інтерфейс) описані всі використовувані функціональними компонентами (підсистемами) КЗЗ ОЕ зовнішні послуги безпеки.

В.3.3.2.10 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.3.3.2.11 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.3.3.2.12 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ ОЕ викладено в частково формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.3.3.2.13 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком промодельованих ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ.

В.3.3.2.14 Дослідження документованих у матеріалах, зазначених у п. А.2.6, результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.3.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.3.3, повністю співпадають з вимогами, викладеними в п. В.2.3.3.

В.3.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.3.4, має передбачати виконання експертом:

В.3.3.4.1 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що процес створення (компонування) з цих матеріалів екземпляра ОЕ є цілком визначеним та не вимагає подальших проектних рішень.

В.3.3.4.2 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що обсяг переданих матеріалів досить репрезентативний для аналізу.

В.3.3.4.3 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що створені (скомпоновані) з наданого вхідного коду структурні компоненти (модулі) КЗЗ коректно, у повному обсязі та згідно з наведеним у детальному проекті описом порядку їх захищеного функціонування реалізують вимоги функціональної специфікації.

В.3.3.4.4 Дослідження документованих у матеріалах, зазначених у п. А.2.8, описів результатів аналізу відповідності між детальним проектом КЗЗ ОЕ та його реалізацією з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом

реалізації цих модулів.

В.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища функціонування

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.4, має передбачати виконання експертом:

В.3.4.1 Перевірки документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання висновку про те, що в складі ОЕ наявні засоби, які реалізують ці процедури.

В.3.4.2 Перевірки факту працездатності засобів, які реалізують процедури безпечної інсталяції, генерації та запуску ОЕ, документовані в матеріалах, зазначених у пп. А.2.13 та А.2.16.

В.3.4.3 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що в них визначені всі можливі параметри конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

В.3.4.4 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що застосування цих процедур та засобів їх реалізації гарантує, що експлуатація ОЕ починається з безпечного стану.

В.3.4.5 Перевірки документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання висновку про те, що в них відображене використання технічних, організаційних та фізичних заходів безпеки при постачанні ОЕ споживачу.

В.3.4.6 Дослідження документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання обґрунтованого висновку про те, що використання описаних у них технічних, організаційних та фізичних заходів безпеки гарантує підтримку цілісності ОЕ та виявлення модифікації чи підміни ОЕ (або забезпечення неможливості такої модифікації чи підміни).

В.3.4.7 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ застосування документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання висновку про факт застосування відповідних процедур.

В.3.5 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації

В.3.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.3.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.3.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.3.6 Вимоги до методики перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Методика перевірки дотримання вимог рівня Г-3 гарантій коректності реалізації ФПБ щодо

випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.3.6.1, має передбачати виконання експертом:

В.3.6.1 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться процедури випробувань засобів, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

В.3.6.2 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99 до політики та порядку функціонування засобів, що реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих ФПБ та охопленням усіх об'єктів КЗЗ та засобів (компонентів) КЗЗ, на які поширюється ця політика.

В.3.6.3 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99, які стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, зазначених у функціональній специфікації КЗЗ ОЕ.

В.3.6.4 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться відомості, які підтверджують, що перевірялися засоби реалізації всіх ФПБ, зазначених у функціональній специфікації КЗЗ.

В.3.6.5 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ.

В.3.6.6 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

В.3.6.7 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що вона погоджена з уповноваженим державним органом.

В.3.6.8 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені 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 КЗЗ ОЕ певних ФПБ.

В.3.6.9 Вибіркових перевірок ФПБ, передбачених програмою та методикою випробувань, документованою в матеріалах, зазначених у п. А.2.18, з метою формулювання висновку про те, що отримані результати виконаних перевірок відповідають наведеним у протоколах випробувань, документованих у матеріалах, зазначених у п. А.2.19.

В.3.6.10 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені підстави, які дають або не дають змоги дійти висновку щодо успішності здійснення перевірок для всіх ФПБ, наведених у функціональній специфікації КЗЗ ОЕ, у тому числі тих ФПБ, попередні перевірки яких були визнані неуспішними.

В.4 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ

В.4.1 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо архітектури

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.1, має передбачати виконання експертом:

В.4.1.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису архітектури

КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі функціональні компоненти (підсистеми) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.4.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі структурні компоненти (модулі) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.4.1.3 Перевірки факту наявності в складі наданого на експертизу ОЕ всіх визначених у матеріалах, зазначених у п. А.2.3, структурних компонентів (модулів) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.4.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ наведено його призначення, реалізовані функції, інтерфейси, залежності від інших модулів та порядок реалізації всіх ФПБ, до реалізації яких має відношення цей компонент (модуль), а також порядок взаємодії з іншими модулями.

В.4.1.5 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою уникнення зайвої взаємодії з іншими модулями) максимальна незалежність цього компонента (модуля) від інших модулів.

В.4.1.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою мінімізації імовірності використання порушником надлишкових повноважень) реалізація вимог мінімуму повноважень.

В.4.1.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко показано розподіл архітектури КЗЗ ОЕ на рівні.

В.4.1.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ відображено ступінь його критичності з погляду забезпечення безпеки.

В.4.1.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного критичного з погляду забезпечення безпеки модуля КЗЗ ОЕ показано, яким чином з використанням механізмів захисту, що реалізуються модулями КЗЗ більш низького рівня, забезпечується захист цього компонента (модуля) від модулів того ж рівня, не критичних з точки зору забезпечення безпеки.

В.4.2 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки

В.4.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.2.1, має передбачати виконання експертом:

В.4.2.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.9, опису використовуваної моделі життєвого циклу ОЕ з метою формулювання висновку про те, чи визначені в ньому всі етапи кожної стадії життєвого циклу ОЕ.

В.4.2.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи поширюються вони на всі питання, вирішувані розробником у процесі розроблення та супроводження ОЕ, та чи надає їх застосування необхідний позитивний вплив на процеси розроблення і супроводження ОЕ, дозволяючи мінімізувати імовірність виникнення недоліків, що мають відношення до захищеності оброблюваної

інформації.

В.4.2.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на всіх етапах кожної стадії життєвого циклу ОЕ з метою формулювання обґрунтованого висновку про те, чи забезпечує їх застосування достатній рівень захищеності ОЕ та безпеки середовища його розробки й експлуатації.

В.4.2.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.9, опису використовуваних методик діяльності розробника на етапі експлуатації (супроводження) ОЕ з метою формулювання обґрунтованого висновку про те, чи дозволяють вони в найкоротший термін та з мінімальним тимчасовим зниженням рівня захищеності усунути виявлені недоліки.

В.4.2.1.5 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, що в ній визначені всі стандарти кодування, реалізовані інструментальними засобами, які використовуються для розроблення, аналізу та реалізації ОЕ.

В.4.2.1.6 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, що всі мови програмування й інструментальні засоби, використовувані для розроблення, аналізу і реалізації ОЕ, добре визначені.

В.4.2.1.7 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи однозначно визначені в ній значення всіх конструкцій, використовуваних у вхідному коді програмного забезпечення КЗЗ ОЕ, та чи надано для кожної такої конструкції чітке й однозначне визначення її призначення та результатів її виконання.

В.4.2.1.8 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи однозначно визначене в ній використання всіх залежних від конкретної реалізації інструментальних засобів параметрів мов програмування та/або компіляторів, що можуть вплинути на виконуваний код або відрізняються від стандарту використовуваної мови.

В.4.2.1.9 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи описані в ній усі параметри розроблювальних апаратних засобів, що впливають на результати застосування цих інструментальних засобів.

В.4.2.1.10 Дослідження документації інструментальних засобів, зазначеної в п. А.2.10, з метою формулювання обґрунтованого висновку про те, чи підтримують використовувані інструментальні засоби можливість коректної реалізації ОЕ згідно з визначеними в ній стандартами кодування.

В.4.2.1.11 Дослідження матеріалів робочого проекту (реалізації), зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, чи застосовувалися в процесі їх розроблення інструментальні засоби та стандарти кодування, документовані в матеріалах, зазначених у п. А.2.10.

В.4.2.1.12 Дослідження опису методик забезпечення безпеки в процесі розроблення та виробництва ОЕ, зазначених у п. А.2.11, з метою формулювання обґрунтованого висновку про те, що в ньому міститься докладний опис суті та порядку використання в процесі розроблення ОЕ заходів безпеки, спрямованих на захист конфіденційності та цілісності проектних документів і вхідного коду реалізації ОЕ.

В.4.2.1.13 Дослідження опису методик забезпечення безпеки в процесі розроблення та виробництва ОЕ, зазначених у п. А.2.11, з метою формулювання обґрунтованого висновку про достатність описаних у ньому заходів безпеки для забезпечення конфіденційності та цілісності проектних документів та вхідного коду реалізації ОЕ.

В.4.2.1.14 Дослідження опису методик забезпечення безпеки в процесі розроблення та виробництва ОЕ, зазначених у п. А.2.11, з метою формулювання обґрунтованого висновку про наявність та адекватність передбачених процедур перегляду та аудиту використовуваних заходів безпеки.

В.4.2.1.15 Перевірки опису методик забезпечення безпеки в процесі розроблення та виробництва ОЕ, зазначених у п. А.2.11, з метою формулювання висновку про формування документальних підтверджень фактів застосування відповідних заходів безпеки згідно з встановленим порядком їх застосування.

В.4.2.1.16 Вибіркової перевірки під час відвідування підприємства - розробника ОЕ наданих документальних підтверджень фактів застосування відповідних заходів безпеки згідно з встановленим порядком їх застосування з метою формулювання висновку про факт застосування

зазначених заходів.

В.4.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.2.2, має передбачати виконання експертом:

В.4.2.2.1 Перевірки наданих матеріалів, зазначених у пп. А.2.1-А.2.4, А.2.12, А.2.13, А.2.15-А.2.18, з метою формулювання висновку про те, що всі вони позначені унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.4.2.2.2 Перевірки наданого на експертизу ОЕ з метою формулювання висновку про те, що він позначений унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.4.2.2.3 Перевірки складу наданих матеріалів із керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить список елементів конфігурації.

В.4.2.2.4 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план керування конфігурацією.

В.4.2.2.5 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план приймання елементів конфігурації під керування системи керування конфігурацією.

В.4.2.2.6 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить опис процедур компонування елементів конфігурації до складу ОЕ.

В.4.2.2.7 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входять вихідні матеріали системи керування конфігурацією.

В.4.2.2.8 Перевірки складу наданого списку елементів конфігурації з метою формулювання висновку про те, що в ньому унікально ідентифіковані всі елементи, які складають сферу дії системи керування конфігурацією.

В.4.2.2.9 Дослідження наданого списку елементів конфігурації з метою формулювання обґрунтованого висновку про те, що в ньому як елементи конфігурації ідентифіковані всі структурні компоненти (модулі) ОЕ, які входять до складу КЗЗ ОЕ.

В.4.2.2.10 Дослідження описаних у документації керування конфігурацією, зазначеної в п. А.2.12, правил унікальної ідентифікації елементів конфігурації з метою формулювання обґрунтованого висновку про те, що вони є несуперечливими та забезпечують однозначну ідентифікацію відповідних елементів конфігурації.

В.4.2.2.11 Дослідження наданого плану керування конфігурацією з метою формулювання обґрунтованого висновку про те, що описаний у ньому порядок використання системи керування конфігурацією забезпечує впевненість у цілісності елементів конфігурації ОЕ, починаючи від початкових етапів проектування та закінчуючи завершенням його експлуатації.

В.4.2.2.12 Дослідження наданого плану приймання елементів конфігурації під керування системи керування конфігурацією з метою формулювання обґрунтованого висновку про те, що в ньому визначені критерії та процедури введення розробленого або зміненого елемента конфігурації до складу поточної версії ОЕ.

В.4.2.2.13 Дослідження наданого опису процедур компонування елементів конфігурації до складу ОЕ з метою формулювання обґрунтованого висновку про те, що він у достатньому обсязі містить відомості про всі необхідні дії, які мають бути виконані за допомогою використовуваних інструментальних засобів розробки при введенні створеного або модифікованого елемента конфігурації до складу ОЕ.

В.4.2.2.14 Дослідження наданих вихідних матеріалів системи керування конфігурацією з метою формулювання обґрунтованого висновку про те, що система керування конфігурацією використовується згідно з планом керування конфігурацією.

В.4.2.2.15 Перевірки змісту наданого опису процедур компонування елементів конфігурації до складу ОЕ з метою формулювання висновку про те, що в ньому описаний порядок використання автоматизованих засобів підтримки генерації (компіляції, компонування) виконуваного коду структурних модулів КЗЗ з вхідного коду їх реалізації.

В.4.2.2.16 Дослідження наданого опису порядку використання автоматизованих засобів підтримки генерації (компіляції, компонування) виконуваного коду структурних модулів КЗЗ з вхідного коду їх реалізації з метою формулювання обґрунтованого висновку про те, що зазначений порядок забезпечує можливість генерації (з використанням відповідних інструментальних засобів) виконуваного коду структурних модулів КЗЗ з вихідного коду їх реалізації.

В.4.2.2.17 Перевірки наданого плану керування конфігурацією з метою формулювання висновку про те, що в ньому описаний порядок використання автоматизованих засобів керування доступом до елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації.

В.4.2.2.18 Перевірки описаних у плані керування конфігурацією автоматизованих засобів керування доступом до елементів конфігурації ОЕ з метою формулювання обґрунтованого висновку про підтримку цими засобами можливості аудиту всіх змін елементів конфігурації ОЕ з реєстрацією в протоколі аудиту, як мінімум, ініціатора, дати та часу модифікації.

В.4.2.2.19 Перевірки змісту наданого плану приймання елементів конфігурації під керування системи керування конфігурацією з метою формулювання висновку про те, що в ньому описаний порядок використання автоматизованих засобів, які забезпечують видачу звітів про стан елементів конфігурації у вигляді, що дозволяє контролювати, як мінімум, ініціатора, дату та час кожної модифікації елемента конфігурації ОЕ.

В.4.2.2.20 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ процедур системи керування конфігурацією стосовно елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації, з метою формулювання висновку про факт застосування системи керування конфігурацією.

В.4.2.2.21 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ застосування автоматизованих засобів підтримки генерації та автоматизованих засобів керування доступом щодо елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації, з метою формулювання висновку про факт застосування відповідних засобів.

В.4.3 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.4.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.3.1, має передбачати виконання експертом:

В.4.3.1.1 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній викладені вимоги до КЗЗ ОЕ у вигляді набору вимог до реалізованих ФПБ.

В.4.3.1.2 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що вимоги до КЗЗ ОЕ викладені в ній оригінальною мовою спілкування без використання будь-яких нотаційних або спеціальних обмежень, відмінних від загальноприйнятих правил використовуваної мови, а використовувана термінологія відповідає НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-004-99.

В.4.3.1.3 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені в ній згідно з вимогами НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.4.3.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.1, опису політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про її внутрішню несуперечність.

В.4.3.1.5 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про повноту викладення вимог

до ФПБ з точки зору вимог НД ТЗІ 2.5-004-99 до відповідних ФПБ відповідних рівнів.

В.4.3.1.6 Дослідження документованих у матеріалах, зазначених у п. А.2.1, вимог до всіх реалізованих ФПБ з метою формулювання обґрунтованого висновку про те, що вимоги до всіх реалізованих ФПБ викладені з урахуванням необхідних умов, визначених у НД ТЗІ 2.5-004-99 для відповідних ФПБ відповідних рівнів.

В.4.3.1.7 Перевірки документованого в матеріалах, зазначених у п. А.2.1, опису моделі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання висновку про те, що в ній наявні моделі політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.4.3.1.8 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що в моделях політик усіх ФПБ чітко визначені характеристики модельованого режиму захищеного функціонування ОЕ.

В.4.3.1.9 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що модельований режим захищеного функціонування ОЕ не суперечить політикам ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.4.3.1.10 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про повноту модельованого режиму захищеного функціонування ОЕ відносно політик ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ.

В.4.3.1.11 Дослідження документованих у матеріалах, зазначених у п. А.2.1, описів моделей політик усіх ФПБ, вимоги до яких викладені в описі політики безпеки, реалізованої КЗЗ ОЕ, з метою формулювання обґрунтованого висновку про те, що описи моделей політик ФПБ викладені у формалізованому вигляді з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.4.3.1.12 Перевірки матеріалів технічного завдання, зазначених у п. А.2.1, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.4.3.1.13 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком описаних у політиці безпеки та промодельованих ФПБ.

В.4.3.1.14 Дослідження документованих у матеріалах, зазначених у п. А.2.5, описів результатів аналізу відповідності між політикою безпеки КЗЗ ОЕ та моделлю політики безпеки КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ з використанням результатів структурованого аналізу продемонстрована наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу.

В.4.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.3.2, повністю співпадають з вимогами, викладеними в п. В.3.3.2.

В.4.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.3.3, має передбачати виконання експертом:

В.4.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому

наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.4.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.4.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), що входять до складу КЗЗ.

В.4.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ.

В.4.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.4.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.4.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.4.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.4.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.4.3.3.10 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено в частково формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.4.3.3.11 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем.

В.4.3.3.12 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.4.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій

коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.3.4, повністю співпадають з вимогами, викладеними в п. В.3.3.4.

В.4.4 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища функціонування

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.4, повністю співпадають з вимогами, викладеними в п. В.3.4.

В.4.5 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації

В.4.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.4.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.4.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.4.6 Вимоги до методики перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Методика перевірки дотримання вимог рівня Г-4 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.4.6.1, має передбачати виконання експертом:

В.4.6.1 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться процедури випробувань засобів, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

В.4.6.2 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99 до політики та порядку функціонування засобів, що реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих ФПБ та охопленням усіх об'єктів КЗЗ та засобів (компонентів) КЗЗ, на які поширюється ця політика.

В.4.6.3 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99, які стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, зазначених у функціональній специфікації КЗЗ ОЕ.

В.4.6.4 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться відомості,

які підтверджують, що перевірялися засоби реалізації всіх ФПБ, зазначених у функціональній специфікації КЗЗ.

В.4.6.5 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ.

В.4.6.6 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

В.4.6.7 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що вона погоджена з уповноваженим державним органом.

В.4.6.8 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені 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 КЗЗ ОЕ певних ФПБ.

В.4.6.9 Вибіркових перевірок ФПБ, передбачених програмою та методикою випробувань, документованою в матеріалах, зазначених у п. А.2.18, з метою формулювання висновку про те, що отримані результати виконаних перевірок відповідають наведеним у протоколах випробувань, документованих у матеріалах, зазначених у п. А.2.19.

В.4.6.10 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені підстави, які дають або не дають змоги дійти висновку щодо успішності здійснення перевірок для всіх ФПБ, наведених у функціональній специфікації КЗЗ ОЕ, у тому числі тих ФПБ, попередні перевірки яких були визнані неуспішними.

В.4.6.11 Перевірки протоколів випробувань ФПБ, зазначених у п. А.2.19, з метою формулювання висновку про те, що вони підтверджують факт залучення до складу приймальної комісії представників уповноваженого державного органу.

В.4.6.12 Дослідження документованого в матеріалах, зазначених у п. А.2.20, опису результатів аналізу стійкості КЗЗ ОЕ до атак з боку розробника з метою формулювання обґрунтованого висновку про те, що в ньому (з урахуванням документованих у матеріалах, зазначених у п. А.2.19, результатів проведених перевірок засобів реалізації ФПБ при виконанні спроб НСД з використанням невидимих ззовні внутрішньосистемних інтерфейсів) наведені аргументи на користь того, що КЗЗ є відносно стійким до атак з боку розробника з можливостями, які відповідають третьому рівню класифікації рівнів можливостей порушників, наведеної в НД ТЗІ 1.1-002-99.

В.5 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ

В.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо архітектури

Методика перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.1, має передбачати виконання експертом:

В.5.1.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі функціональні компоненти (підсистеми) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.5.1.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко визначені всі структурні компоненти (модулі) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.5.1.3 Перевірки факту наявності в складі наданого на експертизу ОЕ всіх визначених у матеріалах, зазначених у п. А.2.3, структурних компонентів (модулів) КЗЗ, які реалізують усі ФПБ, визначені в матеріалах, зазначених у п. А.2.1.

В.5.1.4 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ наведено його призначення, реалізовані функції, інтерфейси, залежності від інших модулів та порядок реалізації всіх ФПБ, до реалізації яких має відношення цей компонент (модуль), а також порядок взаємодії з іншими модулями.

В.5.1.5 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою уникнення зайвої взаємодії з іншими модулями) максимальна незалежність цього компонента (модуля) від інших модулів.

В.5.1.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ показано, яким чином забезпечується (з метою мінімізації імовірності використання порушником надлишкових повноважень) реалізація вимог мінімуму повноважень.

В.5.1.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому чітко показано розподіл архітектури КЗЗ ОЕ на рівні.

В.5.1.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного модуля КЗЗ ОЕ відображено ступінь його критичності з погляду забезпечення безпеки.

В.5.1.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису характеристик структурних компонентів (модулів) КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного критичного з погляду забезпечення безпеки модуля КЗЗ ОЕ показано, яким чином з використанням механізмів захисту, що реалізуються модулями КЗЗ більш низького рівня, забезпечується захист цього компонента (модуля) від модулів того ж рівня, не критичних з точки зору забезпечення безпеки.

В.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки

В.5.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.2.1, повністю співпадають з вимогами, викладеними в п. В.4.5.1.

В.5.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.2.2, повністю співпадають з вимогами, викладеними в п. В.4.2.2.

В.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.5.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення

вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.3.1, повністю співпадають з вимогами, викладеними в п. В.4.3.2.

В.5.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Методика перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.3.2, має передбачати виконання експертом:

В.5.3.2.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних функціональних компонентів (підсистем).

В.5.3.2.2 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного функціонального компонента (підсистеми) КЗЗ у частині, що стосується реалізації ФПБ.

В.5.3.2.3 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ.

В.5.3.2.4 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис усіх функцій, підтримуваних механізмами захисту, реалізованими базовими апаратними, програмно-апаратними та/або програмними засобами.

В.5.3.2.5 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ.

В.5.3.2.6 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.5.3.2.7 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу функціонального компонента (підсистеми) наведені призначення, методи використання інтерфейсу, повідомлення про помилки, коди повернення з деталізацією, за необхідності, результатів використання та можливих позаштатних ситуацій (винятків).

В.5.3.2.8 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс) міститься опис порядку захищеного функціонування цього компонента (підсистеми) КЗЗ ОЕ, що містить опис будь-яких операцій, виконання яких може бути призначено функціональному компоненту (підсистемі) КЗЗ, з огляду на його функції та його вплив на захищений стан ОЕ.

В.5.3.2.9 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті, що не входить до складу КЗЗ ОЕ, у відповідь на ініціююче вплив на відповідний інтерфейс) описані всі використовувані функціональними компонентами (підсистемами) КЗЗ ОЕ зовнішні послуги безпеки.

В.5.3.2.10 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.5.3.2.11 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.5.3.2.12 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ ОЕ викладено в частково

формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.5.3.2.13 Перевірки матеріалів ескізного проекту, зазначених у п. А.2.2, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.5.3.2.14 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком промодельованих ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ.

В.5.3.2.15 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ з використанням результатів структурованого аналізу продемонстровано наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу.

В.5.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.3.3, має передбачати виконання експертом:

В.5.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.5.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.5.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), що входять до складу КЗЗ.

В.5.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ.

В.5.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.5.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.5.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.5.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.5.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису

детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.5.3.3.10 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено в частково формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.5.3.3.11 Перевірки матеріалів технічного проекту, зазначених у п. А.2.3, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.5.3.3.12 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем.

В.5.3.3.13 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ неформальним чином показана наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу.

В.5.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Методика перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.3.4, має передбачати виконання експертом:

В.5.3.4.1 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що процес створення (компонування) з цих матеріалів екземпляра ОЕ є цілком визначеним та не вимагає подальших проектних рішень.

В.5.3.4.2 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що обсяг переданих матеріалів відповідає всім структурним компонентам (модулям) КЗЗ ОЕ.

В.5.3.4.3 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що створені (скомпоновані) з наданого вхідного коду структурні компоненти (модулі) КЗЗ коректно, у повному обсязі та згідно з наведеним у детальному проекті описом порядку їх захищеного функціонування реалізують вимоги функціональної специфікації.

В.5.3.4.4 Перевірки матеріалів робочого проекту, зазначених у п. А.2.4, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.5.3.4.5 Дослідження документованих у матеріалах, зазначених у п. А.2.8, описів результатів аналізу відповідності між детальним проектом КЗЗ ОЕ та його реалізацією з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів.

В.5.4 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища функціонування

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.4, повністю співпадають з вимогами, викладеними в п. В.3.3.

В.5.5 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації

В.5.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.5.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.5.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.5.6 Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Вимоги до методики перевірки дотримання вимог рівня Г-5 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.5.6.1, повністю співпадають з вимогами, викладеними в п. В.4.6.

В.6 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ

В.6.1 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо архітектури

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.1, повністю співпадають з вимогами, викладеними в п. В.5.1.

В.6.2 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки

В.6.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.2.1, повністю співпадають з вимогами, викладеними в п. В.4.2.1.

В.6.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Методика перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.2.2, має передбачати виконання експертом:

В.6.2.2.1 Перевірки наданих матеріалів, зазначених у пп. А.2.1-А.2.4, А.2.12, А.2.13, А.2.15-

А.2.18, з метою формулювання висновку про те, що всі вони позначені унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.6.2.2.2 Перевірки наданого на експертизу ОЕ з метою формулювання висновку про те, що він позначений унікальним маркіруванням, яке відповідає описаним у документації керування конфігурацією, зазначеної в п. А.2.12, правилам унікальної ідентифікації елементів конфігурації.

В.6.2.2.3 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить список елементів конфігурації.

В.6.2.2.4 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план керування конфігурацією.

В.6.2.2.5 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить план приймання елементів конфігурації під керування системи керування конфігурацією.

В.6.2.2.6 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входить опис процедур компонування елементів конфігурації до складу ОЕ.

В.6.2.2.7 Перевірки складу наданих матеріалів з керування конфігурацією, зазначених у п. А.2.12, з метою формулювання висновку про те, що до їх складу входять вихідні матеріали системи керування конфігурацією.

В.6.2.2.8 Перевірки складу наданого списку елементів конфігурації з метою формулювання висновку про те, що в ньому унікально ідентифіковані всі елементи, які складають сферу дії системи керування конфігурацією.

В.6.2.2.9 Дослідження наданого списку елементів конфігурації з метою формулювання обґрунтованого висновку про те, що в ньому як елементи конфігурації ідентифіковані всі структурні компоненти (модулі) ОЕ, які входять до складу КЗЗ ОЕ.

В.6.2.2.10 Дослідження описаних у документації керування конфігурацією, зазначеної в п. А.2.12, правил унікальної ідентифікації елементів конфігурації з метою формулювання обґрунтованого висновку про те, що вони є несуперечливими та забезпечують однозначну ідентифікацію відповідних елементів конфігурації.

В.6.2.2.11 Дослідження наданого плану керування конфігурацією з метою формулювання обґрунтованого висновку про те, що описаний у ньому порядок використання системи керування конфігурацією забезпечує впевненість у цілісності елементів конфігурації ОЕ, починаючи від початкових етапів проектування та закінчуючи завершенням його експлуатації.

В.6.2.2.12 Дослідження наданого плану приймання елементів конфігурації під керування системи керування конфігурацією з метою формулювання обґрунтованого висновку про те, що в ньому визначені критерії та процедури введення розробленого або зміненого елемента конфігурації до складу поточної версії ОЕ.

В.6.2.2.13 Дослідження наданого опису процедур компонування елементів конфігурації до складу ОЕ з метою формулювання обґрунтованого висновку про те, що він у достатньому обсязі містить відомості про всі необхідні дії, які мають бути виконані за допомогою використовуваних інструментальних засобів розробки при введенні створеного або модифікованого елемента конфігурації до складу ОЕ.

В.6.2.2.14 Дослідження наданих вихідних матеріалів системи керування конфігурацією з метою формулювання обґрунтованого висновку про те, що система керування конфігурацією використовується згідно з планом керування конфігурацією.

В.6.2.2.15 Перевірки змісту наданого опису процедур компонування елементів конфігурації до складу ОЕ з метою формулювання висновку про те, що в ньому описано порядок використання автоматизованих засобів підтримки генерації (компіляції, компонування) виконуваного коду структурних модулів КЗЗ з вхідного коду їх реалізації.

В.6.2.2.16 Дослідження наданого опису порядку використання автоматизованих засобів підтримки генерації (компіляції, компонування) виконуваного коду структурних модулів КЗЗ з вхідного коду їх реалізації з метою формулювання обґрунтованого висновку про те, що зазначений порядок забезпечує можливість генерації (з використанням відповідних інструментальних засобів) виконуваного коду структурних модулів КЗЗ з вихідного коду їх реалізації.

В.6.2.2.17 Перевірки наданого плану керування конфігурацією з метою формулювання висновку про те, що в ньому описано порядок використання автоматизованих засобів керування доступом до елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації.

В.6.2.2.18 Перевірки описаних у плані керування конфігурацією автоматизованих засобів керування доступом до елементів конфігурації ОЕ з метою формулювання обгрунтованого висновку про підтримання цими засобами можливості аудиту всіх змін елементів конфігурації ОЕ з реєстрацією в протоколі аудиту, як мінімум, ініціатора, дати та часу модифікації.

В.6.2.2.19 Перевірки змісту наданого плану приймання елементів конфігурації під керування системи керування конфігурацією з метою формулювання висновку про те, що в ньому описано порядок використання автоматизованих засобів, які забезпечують видачу звітів про стан елементів конфігурації у вигляді, що дозволяє контролювати, як мінімум, ініціатора, дату та час кожної модифікації елемента конфігурації ОЕ.

В.6.2.2.20 Дослідження документованого в матеріалах, зазначених у п. А.2.11, опису політики забезпечення цілісності використовуваних для генерації ОЕ елементів конфігурації з метою формулювання обгрунтованого висновку про те, що в ній відображено, які саме елементи конфігурації мають бути захищені від несанкціонованої модифікації для збереження цілісності ОЕ, кому з персоналу розробника дозволено модифікувати такі елементи конфігурації, а також те, яким чином здійснюється перевірка цілісності відповідних елементів конфігурації перед виконанням генерації ОЕ.

В.6.2.2.21 Дослідження описаних у плані керування конфігурацією автоматизованих засобів керування доступом до елементів конфігурації ОЕ з метою формулювання обгрунтованого висновку про ефективність використання зазначених засобів для запобігання несанкціонованій модифікації елементів конфігурації ОЕ згідно з прийнятою політикою забезпечення цілісності елементів конфігурації ОЕ.

В.6.2.2.22 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ процедур системи керування конфігурацією стосовно елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації, з метою формулювання висновку про факт застосування системи керування конфігурацією.

В.6.2.2.23 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ застосування автоматизованих засобів підтримки генерації та автоматизованих засобів керування доступом щодо елементів конфігурації ОЕ, ідентифікованих у списку елементів конфігурації, з метою формулювання висновку про факт застосування відповідних засобів.

В.6.2.2.24 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ застосування описаних у матеріалах, зазначених у п. А.2.11, заходів фізичної, організаційної та кадрової безпеки для захисту всіх засобів та матеріалів, використовуваних для генерації ОЕ, від несанкціонованої модифікації або руйнування з метою формулювання висновку про факт застосування відповідних заходів.

В.6.3 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.6.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Вимоги щодо методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.3.1, повністю співпадають з вимогами, викладеними в п. В.4.3.1.

В.6.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Методика перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.3.2, має передбачати виконання експертом:

В.6.3.2.1 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обгрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних функціональних компонентів (підсистем).

В.6.3.2.2 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного функціонального компонента (підсистеми) КЗЗ у частині, що стосується реалізації ФПБ.

В.6.3.2.3 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі базові апаратні, програмно-апаратні та/або програмні засоби, необхідні для реалізації КЗЗ ОЕ.

В.6.3.2.4 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис усіх функцій, підтримуваних механізмами захисту, реалізованими базовими апаратними, програмно-апаратними та/або програмними засобами.

В.6.3.2.5 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ.

В.6.3.2.6 Перевірки документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси функціональних компонентів (підсистем) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.6.3.2.7 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу функціонального компонента (підсистеми) наведені призначення, методи використання інтерфейсу, повідомлення про помилки, коди повернення з деталізацією, за необхідності, результатів використання та можливих позаштатних ситуацій (виключень).

В.6.3.2.8 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті (підсистемі) КЗЗ у відповідь на ініціюючий вплив на відповідний інтерфейс) міститься опис порядку захищеного функціонування цього компонента (підсистеми) КЗЗ ОЕ, що містить опис будь-яких операцій, виконання яких може бути призначено функціональному компоненту (підсистемі) КЗЗ, з огляду на його функції та його вплив на захищений стан ОЕ.

В.6.3.2.9 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному функціональному компоненті, що не входить до складу КЗЗ ОЕ, у відповідь на ініціююче вплив на відповідний інтерфейс) описані всі використовувані функціональними компонентами (підсистемами) КЗЗ ОЕ зовнішні послуги безпеки.

В.6.3.2.10 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.6.3.2.11 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування компонентів (підсистем) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.6.3.2.12 Дослідження документованого в матеріалах, зазначених у п. А.2.2, опису проекту архітектури КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного функціонального компонента (підсистеми) КЗЗ ОЕ викладено у формалізованому вигляді з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.6.3.2.13 Перевірки матеріалів ескізного проекту, зазначених у п. А.2.2, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.6.3.2.14 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком промодельованих ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ.

В.6.3.2.15 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів

результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ з використанням результатів структурованого аналізу продемонстровано наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу.

В.6.3.2.16 Дослідження документованих у матеріалах, зазначених у п. А.2.6, описів результатів аналізу відповідності між моделлю політики безпеки КЗЗ ОЕ та проектом архітектури КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ наведені формальні докази відповідності між правилами реалізації ФПБ та порядком захищеного функціонування підсистем КЗЗ, викладеними, відповідно, у моделі політики безпеки КЗЗ ОЕ та проекті архітектури.

В.6.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.3.3, має передбачати виконання експертом:

В.6.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.6.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.6.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), що входять до складу КЗЗ.

В.6.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ.

В.6.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.6.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.6.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.6.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.6.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.6.3.3.10 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису

детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено в частково формалізованому вигляді мовою з обмеженим синтаксисом, супроводжуваному допоміжними поясненнями, поданими в неформалізованому вигляді.

В.5.3.3.11 Перевірки матеріалів технічного проекту, зазначених у п. А.2.3, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.6.3.3.12 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показано наявність відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем.

В.6.3.3.13 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ з використанням результатів структурованого аналізу продемонстровано наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та всіма використовуваними атрибутами об'єктів КЗЗ різного типу.

В.6.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.3.4, повністю співпадають з вимогами, викладеними в п. В.5.3.4.

В.6.4 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища функціонування

Методика перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.4, має передбачати виконання експертом:

В.6.4.1 Перевірки документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання висновку про те, що в складі ОЕ наявні засоби, які реалізують ці процедури.

В.6.4.2 Перевірки факту працездатності засобів, які реалізують процедури безпечної інсталяції, генерації та запуску ОЕ, документовані в матеріалах, зазначених у пп. А.2.13 та А.2.16.

В.6.4.3 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що в них визначені всі можливі параметри конфігурації, які можуть використовуватися в процесі інсталяції, генерації та запуску ОЕ.

В.6.4.4 Дослідження документованих у матеріалах, зазначених у пп. А.2.13 та А.2.16, описів процедур безпечної інсталяції, генерації та запуску ОЕ з метою формулювання обґрунтованого висновку про те, що застосування цих процедур та засобів їх реалізації гарантує, що експлуатація ОЕ починається з безпечного стану.

В.6.4.5 Перевірки документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання висновку про те, що в них відображене використання технічних, організаційних та фізичних заходів безпеки при постачанні ОЕ споживачу.

В.6.4.6 Дослідження документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання обґрунтованого висновку про те, що використання описаних у них технічних, організаційних та фізичних заходів безпеки гарантує підтримання цілісності ОЕ та виявлення модифікації чи підміни ОЕ (або забезпечення неможливості такої модифікації чи підміни).

В.6.4.7 Перевірки документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання висновку про те, що в них відображене використання технічних, організаційних та фізичних заходів безпеки при постачанні вироблених розробником модифікацій (оновлень) ОЕ.

В.6.4.8 Дослідження документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання обґрунтованого висновку про те, що використання описаних у них технічних, організаційних та фізичних заходів безпеки гарантує виявлення модифікації чи підміни вироблених розробником модифікацій (оновлень) ОЕ (або забезпечення неможливості такої модифікації чи підміни).

В.6.4.9 Дослідження документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ з метою формулювання обґрунтованого висновку про те, що використання описаних у них технічних, організаційних та фізичних заходів безпеки дозволяє виявити спроби підміни відправника, навіть у тих випадках, коли розробник нічого не відправляв замовнику, і, таким чином, гарантує, що одержаний замовником ОЕ (або його оновлення) переданий йому саме розробником.

В.6.4.10 Вибіркової перевірки під час відвідування підприємства – розробника ОЕ застосування документованих у матеріалах, зазначених у п. А.2.14, описів процедур постачання ОЕ та його модифікацій (оновлень) з метою формулювання висновку про факт застосування відповідних процедур.

В.6.5 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації

В.6.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.6.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.6.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.6.6 Вимоги до методики перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту

Методика перевірки дотримання вимог рівня Г-6 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.6.1, має передбачати виконання експертом:

В.6.6.1 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться процедури випробувань засобів, які реалізують усі ФПБ, зазначені у функціональній специфікації КЗЗ ОЕ.

В.6.6.2 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99 до політики та порядку функціонування засобів, що реалізують усі ФПБ, наведені у функціональній специфікації КЗЗ ОЕ, з урахуванням політики цих ФПБ та охопленням усіх об'єктів КЗЗ та засобів (компонентів) КЗЗ, на які поширюється ця політика.

В.6.6.3 Дослідження документованої в матеріалах, зазначених у п.А.2.18, програми та методики випробувань ФПБ з метою формулювання обґрунтованого висновку про те, що вона передбачає перевірку всіх вимог НД ТЗІ 2.5-004-99, які стосуються реалізації необхідних умов (у вигляді ФПБ або рівня гарантій коректності їх реалізації) для всіх ФПБ, зазначених у функціональній специфікації КЗЗ ОЕ.

В.6.6.4 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що в ній містяться відомості, які підтверджують, що перевірялися засоби реалізації всіх ФПБ, зазначених у функціональній специфікації КЗЗ.

В.6.6.5 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обгрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі видимі ззовні інтерфейси КЗЗ.

В.6.6.6 Дослідження документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання обгрунтованого висновку про те, що в ході виконання перевірок різних ФПБ були задіяні всі функціональні компоненти КЗЗ (підсистеми), документовані в проекті архітектури, а також усі структурні компоненти КЗЗ (модулі), документовані в детальному проекті.

В.6.6.7 Перевірки документованої в матеріалах, зазначених у п. А.2.18, програми та методики випробувань ФПБ з метою формулювання висновку про те, що вона погоджена з уповноваженим державним органом.

В.6.6.8 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обгрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені 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 КЗЗ ОЕ певних ФПБ.

В.6.6.9 Вибіркових перевірок ФПБ, передбачених програмою та методикою випробувань, документованою в матеріалах, зазначених у п. А.2.18, з метою формулювання висновку про те, що отримані результати виконаних перевірок відповідають наведеним у протоколах випробувань, документованих у матеріалах, зазначених у п. А.2.19.

В.6.6.10 Дослідження документованих у матеріалах, зазначених у п. А.2.19, протоколів випробувань ФПБ з метою формулювання обгрунтованого висновку про те, що в них з посиланням на відповідні пункти програми та методики випробувань наведені підстави, які дають або не дають змоги дійти висновку щодо успішності здійснення перевірок для всіх ФПБ, наведених у функціональній специфікації КЗЗ ОЕ, у тому числі тих ФПБ, попередні перевірки яких були визнані неуспішними.

В.6.6.11 Перевірки протоколів випробувань ФПБ, зазначених у п. А.2.19, з метою формулювання висновку про те, що вони підтверджують факт залучення до складу приймальної комісії представників уповноваженого державного органу.

В.6.6.12 Дослідження документованого в матеріалах, зазначених у п. А.2.20, опису результатів аналізу стійкості КЗЗ ОЕ до атак з боку розробника з метою формулювання обгрунтованого висновку про те, що в ньому з урахуванням документованих у матеріалах, зазначених у п. А.2.19, результатів проведених перевірок засобів реалізації ФПБ при виконанні спроб НСД з використанням невидимих ззовні внутрішньосистемних інтерфейсів наведені аргументи на користь того, що КЗЗ є відносно стійким до атак з боку розробника з можливостями, які відповідають третьому рівню класифікації рівнів можливостей порушників, наведеної в НД ТЗІ 1.1-002-99.

В.6.6.13 Дослідження документованого в матеріалах, зазначених у п. А.2.20, опису результатів аналізу стійкості КЗЗ ОЕ до атак з боку розробника з метою формулювання обгрунтованого висновку про те, що в ньому з урахуванням документованих у матеріалах, зазначених у п. А.2.19, результатів проведених перевірок засобів реалізації ФПБ при виконанні спроб НСД з використанням недовірених (спеціально розроблених) структурних модулів КЗЗ ОЕ, які навмисно вводяться до складу КЗЗ, наведені аргументи на користь того, що КЗЗ є абсолютно стійким до атак з боку розробника з можливостями, які відповідають четвертому рівню класифікації рівнів можливостей порушників, наведеної в НД ТЗІ 1.1-002-99.

В.7 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ

В.7.1 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо архітектури

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації

ФПБ щодо архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.1, повністю співпадають з вимогами, викладеними в п. В.5.1.

В.7.2 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки

В.7.2.1 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується організації процесу розробки, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.2.1, повністю співпадають з вимогами, викладеними в п. В.4.2.1.

В.7.2.2 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища розробки в частині, що стосується керування конфігурацією, з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.2.2, повністю співпадають з вимогами, викладеними в п. В.6.2.2.

В.7.3 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки

В.7.3.1 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині функціональних специфікацій з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.3.1, повністю співпадають з вимогами, викладеними в п. В.4.3.1.

В.7.3.2 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині проекту архітектури з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.3.2, повністю співпадають з вимогами, викладеними в п. В.6.3.2.

В.7.3.3 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту

Методика перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині детального проекту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.3.3, має передбачати виконання експертом:

В.7.3.3.1 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому наведено опис КЗЗ у термінах основних структурних компонентів (модулів).

В.7.3.3.2 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому міститься опис призначення та функціональних можливостей кожного структурного компонента (модуля) КЗЗ ОЕ.

В.7.3.3.3 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому на рівні зовнішніх інтерфейсів модулів, потоків даних, керування тощо однозначно визначені взаємозв'язки між усіма структурними компонентами (модулями), що входять до складу КЗЗ.

В.7.3.3.4 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому визначені всі інтерфейси

структурних компонентів (модулів) КЗЗ ОЕ.

В.7.3.3.5 Перевірки документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що в ньому зазначені всі інтерфейси структурних компонентів (модулів) КЗЗ ОЕ, які є видимими ззовні КЗЗ.

В.7.3.3.6 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому для кожного інтерфейсу структурного компонента (модуля) наведені призначення, імена точок входу, методи використання та параметри інтерфейсу, результати виконання, повідомлення про помилки, коди повернення.

В.7.3.3.7 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому (у термінах послідовностей дій, які виконуються в кожному структурному компоненті (модулі) КЗЗ у відповідь на ініціюючий вплив з боку інших модулів на відповідний інтерфейс) наведено опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ, який містить алгоритми реалізації механізмів захисту, а також необхідні для розуміння їх реалізації внутрішні структури даних та інтерфейси.

В.7.3.3.8 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в ньому визначено порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ при реалізації всіх викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.7.3.3.9 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що визначений у ньому порядок захищеного функціонування структурних компонентів (модулів) КЗЗ ОЕ в повному обсязі забезпечує реалізацію викладених у функціональній специфікації КЗЗ вимог до всіх ФПБ.

В.7.3.3.10 Дослідження документованого в матеріалах, зазначених у п. А.2.3, опису детального проекту КЗЗ ОЕ з метою формулювання висновку про те, що опис порядку захищеного функціонування кожного структурного компонента (модуля) КЗЗ ОЕ викладено у формалізованому вигляді з використанням формалізованої нотації, заснованої на чітко визначених математичних поняттях, супроводжуваної допоміжними поясненнями, поданими в неформалізованому вигляді.

В.7.3.3.11 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах неформальним чином показана наявність відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем.

В.7.3.3.12 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ з використанням результатів структурованого аналізу продемонстровано наявність відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та всіма використовуваними атрибутами об'єктів КЗЗ різного типу.

В.7.3.3.13 Дослідження документованих у матеріалах, зазначених у п. А.2.7, описів результатів аналізу відповідності між проектом архітектури КЗЗ ОЕ та детальним проектом КЗЗ ОЕ з метою формулювання обґрунтованого висновку про те, що в цих матеріалах для всіх ФПБ наведені формальні докази відповідності між порядком захищеного функціонування підсистем КЗЗ та порядком захищеного функціонування модулів КЗЗ, що входять до складу цих підсистем, викладеними, відповідно, у проекті архітектури та детальному проекті.

В.7.3.4 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації

Методика перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо послідовності розробки в частині реалізації з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.3.4, має передбачати виконання експертом:

В.7.3.4.1 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що процес створення (компонування) з цих матеріалів екземпляра

ОЕ є цілком визначеним та не вимагає подальших проектних рішень.

В.7.3.4.2 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що обсяг переданих матеріалів відповідає всім структурним компонентам (модулям) КЗЗ ОЕ та всім бібліотекам часу виконання операційної системи (ядра операційної системи).

В.7.3.4.3 Дослідження матеріалів, зазначених у п. А.2.4, з метою формулювання обґрунтованого висновку про те, що створені (скомпоновані) з наданого вхідного коду структурні компоненти (модулі) КЗЗ коректно, у повному обсязі та згідно з наведеним у детальному проекті описом порядку їх захищеного функціонування реалізують вимоги функціональної специфікації.

В.7.3.4.4 Перевірки матеріалів робочого проекту, зазначених у п. А.2.4, з метою формулювання висновку про те, що вони погоджені з уповноваженим державним органом.

В.7.3.4.5 Дослідження документованих у матеріалах, зазначених у п. А.2.8, описів результатів аналізу відповідності між детальним проектом КЗЗ ОЕ та його реалізацією з метою формулювання обґрунтованого висновку про те, що в цих матеріалах з використанням результатів структурованого аналізу продемонстровано наявність відповідності між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів.

В.7.3.4.6 Дослідження документованих у матеріалах, зазначених у п. А.2.8, описів результатів аналізу відповідності між детальним проектом КЗЗ ОЕ та його реалізацією з метою формулювання обґрунтованого висновку про те, що в цих матеріалах з використанням результатів структурованого аналізу продемонстровано наявність відповідності між наведеними в детальному проекті характеристиками (реалізованими функціями, параметрами інтерфейсів) процедур, що містяться в бібліотеках часу виконання операційної системи (ядрі операційної системи), використовуваних у процесі функціонування всіх структурних компонентів (модулів) КЗЗ, та наданим розробником вхідним кодом реалізації цих процедур.

В.7.4 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища функціонування

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо середовища функціонування з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.4, повністю співпадають з вимогами, викладеними в п. В.6.4.

В.7.5 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації

В.7.5.1 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині опису послуг безпеки з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.6.5.1, повністю співпадають з вимогами, викладеними в п. В.1.5.1.

В.7.5.2 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині настанов адміністратору з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.5.2, повністю співпадають з вимогами, викладеними в п. В.1.5.2.

В.7.5.3 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо документації в частині настанов користувачу з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.5.3, повністю співпадають з вимогами, викладеними в п. В.1.5.3.

В.7.6 Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності

реалізації ФПБ щодо випробувань комплексу засобів захисту

Вимоги до методики перевірки дотримання вимог рівня Г-7 гарантій коректності реалізації ФПБ щодо випробувань комплексу засобів захисту з метою забезпечення вимог програми перевірки рівня гарантій, розробленої з урахуванням вимог п. Б.7.6.1, повністю співпадають з вимогами, викладеними в п. В.6.6.

Додаток Г
Рекомендації щодо відвідування підприємств з метою перевірки умов розроблення, виробництва та постачання об'єкта експертизи
(рекомендований)

У Додатку Г наведено рекомендації з виконання перевірки дотримання певних вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, безпосередньо на підприємствах, які розробляють та виробляють ОЕ. Ці рекомендації стосуються як організації робіт, так і виконання певних дій, пов'язаних з перевіркою вимог критеріїв гарантій.

Г.1 Основні питання, що вирішуються в ході відвідування підприємств з метою перевірки умов розроблення, виробництва та постачання ОЕ

Основні питання, що вирішуються експертом у ході відвідування підприємства – розробника ОЕ з метою перевірки умов його розроблення, виробництва та постачання, визначаються необхідністю формулювання висновку про факт застосування заявлених розробником та описаних у наданих експерту матеріалах, зазначених у пп. А.2.11, А.2.12, А.2.14:

- заходів безпеки в процесі розроблення та виробництва ОЕ;
- системи керування конфігурацією ОЕ;
- процедур постачання ОЕ замовнику.

Ці питання передбачають вибіркову перевірку та документальну фіксацію фактів застосування/не застосування відповідних заходів, засобів та процедур.

Г.2 Рекомендації з організації та проведення робіт у ході відвідування підприємств з метою перевірки умов розроблення, виробництва та постачання ОЕ

Г.2.1 Загальні рекомендації з організації відвідувань підприємств

Г.2.1.1 Для досягнення максимального ефекту роботу на підприємстві, яке є розробником ОЕ, рекомендується організувати в такий спосіб:

- провести попередню нараду за участю керівництва підприємства або осіб, відповідальних за виконання процедур (процесів), що підлягають перевірці;
- виконати одне або декілька відвідувань, у ході яких провести перевірки фактів застосування/не застосування заявлених розробником ОЕ відповідних заходів, засобів та процедур, а також фіксацію їх результатів;
- провести заключну нараду за участю керівництва підприємства або осіб, відповідальних за виконання процедур (процесів), що підлягали перевірці.

Г.2.1.2 Основною метою попередньої наради є усвідомлення відповідальними особами розробника ОЕ переліку та змісту запланованих перевірок, відомості щодо яких мають бути надані експертом та ґрунтуватися на переданих йому матеріалах, зазначених у пп. А.2.11, А.2.12, А.2.14, узгодження графіка виконання подальших робіт та призначення з числа співробітників розробника осіб, які супроводжують експерта. Головними вимогами до осіб, які супроводжують експерта, є компетентність стосовно заходів, засобів та процедур, що передбачається перевіряти.

Г.2.1.3 При виконанні відвідувань, у ході яких проводиться перевірка різних заходів, засобів та процедур, рекомендується:

- поєднувати відвідування для перевірки застосування заходів безпеки, системи керування конфігурацією та процедур постачання ОЕ замовнику;
- усі перевірки виконувати лише в присутності осіб, які супроводжують;
- зберігати всі вихідні матеріали, які дозволяють підтвердити або спростувати факт застосування/не застосування певних заходів, засобів та процедур;
- за результатами виконаних перевірок підготувати стислий звіт, в якому з посиланням на зібрані матеріали обґрунтувати зроблені висновки, а також, якщо це доцільно, надати рекомендації щодо удосконалення застосовуваних заходів, засобів та процедур.

Г.2.1.4 Основною метою заключної наради є ознайомлення відповідальних осіб розробника ОЕ зі зробленими експертом висновками та, можливо, з рекомендаціями щодо удосконалення застосовуваних заходів, засобів та процедур. При цьому, у випадку виникнення протиріч, які стосуються результатів виконаних перевірок, можна погодитися на повторне їх виконання, але вже з більш поглибленим документуванням та подальшим аналізом отриманих результатів.

Г.2.2 Рекомендації з виконання перевірки застосування заходів безпеки в процесі розроблення та виробництва ОЕ

При проведенні перевірки фактів застосування заходів фізичної, технічної, організаційної та кадрової безпеки в процесі розроблення ОЕ (для заявлених рівнів гарантій Г-4 … Г-7) та в процесі виробництва (генерації) ОЕ (для заявлених рівнів гарантій Г-6 … Г-7) експерту рекомендується з урахуванням змісту наданих йому матеріалів, зазначених у п. А.2.11, а також змісту наданих документальних підтверджень фактів застосування відповідних заходів:

- провести спостереження за застосуванням відповідних заходів з метою, по-перше, переконатися в самому факті їх застосування, по-друге, оцінити, наскільки порядок застосування різних заходів відповідає викладеному в матеріалах, зазначених у п. А.2.11;
- провести бесіду з персоналом підприємства – розробника ОЕ, задіяним у реалізації різних заходів, з метою перевірки рівня знань ним вимог заходів безпеки та своїх обов'язків;
- на підставі зібраних відомостей сформулювати та зафіксувати в звіті висновки про факти застосування зазначених заходів.

Г.2.3 Рекомендації з виконання перевірки застосування системи керування конфігурацією ОЕ

При проведенні перевірки фактів застосування системи керування конфігурацією в процесі розробки і виробництва (генерації) ОЕ експерту рекомендується, з урахуванням змісту наданих йому матеріалів із керування конфігурацією, зазначених у п. А.2.12, а також змісту наданих вихідних матеріалів системи керування конфігурацією:

- для декількох елементів конфігурації, що відносяться до кожного ідентифікованого в плані керування конфігурацією типу елементів конфігурації (наприклад, проектної документації, вхідного коду реалізації, тестової документації, експлуатаційної документації), перевірити вихідні матеріали системи керування конфігурацією (для заявлених рівнів гарантій Г-4 … Г-7 мають бути згенеровані з використанням автоматизованих засобів), які охоплюють кожен тип операцій з відповідними елементами конфігурації (наприклад, створення, модифікація, видалення, повернення до попередньої версії), з метою, по-перше, переконатися в самому факті їх застосування, а, по-друге, оцінити, наскільки порядок застосування різних процедур відповідає викладеному в матеріалах, зазначених у п. А.2.12;
- виконати (для заявлених рівнів гарантій Г-4…Г-7) з використанням автоматизованих та інструментальних засобів, описаних у матеріалах з керування конфігурацією, зазначених у п. А.2.12, процедури компонування декількох елементів конфігурації, ідентифікованих у плані керування конфігурацією, що відповідають різним структурним компонентам (модулям) ОЕ, з метою, по-перше, переконатися в самому факті їх застосування, а, по-друге, оцінити, наскільки порядок застосування різних процедур відповідає викладеному в матеріалах, зазначених у п. А.2.12;
- виконати (для заявлених рівнів гарантій Г-4…Г-7) перевірку використовуваних у системі керування конфігурацією автоматизованих засобів керування доступом стосовно декількох елементів конфігурації різного типу, ідентифікованих у списку елементів конфігурації, з метою, по-перше, переконатися у факті наявності цих засобів, а, по-друге, оцінити, наскільки порядок застосування відповідних засобів та процедур відповідає викладеному в матеріалах, зазначених у п. А.2.12, та забезпечує захист цілісності елементів конфігурації від несанкціонованої модифікації;
- виконати (для заявлених рівнів гарантій Г-4…Г-7) перевірку вмісту створених автоматизованими засобами керування доступом записів протоколів аудиту, що відповідають операціям, виконаним з різними елементами конфігурації, з метою переконатися у факті їх наявності та збереженні в них необхідної інформації;
- на підставі зібраних відомостей сформулювати та зафіксувати в звіті висновки про факти застосування зазначених засобів та процедур.

Г.2.4 Рекомендації з виконання перевірки застосування процедур постачання ОЕ замовнику

При проведенні перевірки фактів застосування процедур постачання ОЕ замовнику експерту рекомендується, з урахуванням змісту наданих йому матеріалів щодо процедур постачання ОЕ, зазначених у п. А.2.14:

- провести спостереження за застосуванням відповідних заходів та процедур з метою, по-перше, переконатися в самому факті їх застосування, а, по-друге, оцінити, наскільки порядок застосування різних заходів та процедур відповідає викладеному в матеріалах, зазначених у п. А.2.14;
- провести бесіду з персоналом підприємства – розробника ОЕ, задіяним у постачанні ОЕ споживачу, з метою перевірки рівня знань ним вимог заходів безпеки при постачанні ОЕ та своїх обов'язків;
- на підставі зібраних відомостей сформулювати та зафіксувати в звіті висновки про факти застосування зазначених заходів та процедур.

Додаток Д
Рекомендації щодо аналізу моделей політики безпеки
(рекомендований)

У Додатку Д наведено рекомендації з виконання аналізу описів моделей політик безпеки, реалізованих КЗЗ оцінюваних ОЕ. Рекомендації викладені з урахуванням вимог критеріїв гарантій, наведених у НД ТЗІ 2.5-004-99, щодо змісту описів моделей політик безпеки та стосуються основних дій, які має виконувати експерт у процесі аналізу таких моделей.

Д.1 Зміст моделі політики безпеки

Д.1.1 Під моделлю політики безпеки слід розуміти абстрактний опис політики безпеки інформації, що реалізується КЗЗ ОЕ (тобто, сукупність політик усіх ФПБ, реалізованих КЗЗ ОЕ), певного ступеня формалізації. Модель політики безпеки повинна містити:

- визначення режиму захищеного (безпечного) функціонування ОЕ;
- визначення правил виконання операцій над захищеними об'єктами.

Д.1.2 Визначення режиму захищеного функціонування має містити опис обмежень на допустимі характеристики (набори атрибутів) усіх об'єктів, які знаходяться під керуванням КЗЗ (об'єктів-користувачів, об'єктів-процесів, пасивних об'єктів) для всіх ідентифікованих у політиці безпеки ФПБ. Опис обмежень має містити як обмеження, які задаються стосовно зовнішніх (тобто, видимих ззовні) інтерфейсів засобів реалізації ФПБ, так і внутрішньосистемні обмеження.

Д.1.3 Визначення правил виконання операцій над захищеними об'єктами має містити опис правил абстрактних взаємодій між компонентами КЗЗ та всіма об'єктами, що знаходяться під керуванням КЗЗ (об'єктами-процесами, об'єктами-користувачами, пасивними об'єктами) у частині, що стосується реалізації ФПБ за допомогою відповідних механізмів.

Д.1.4 Опис моделі політики безпеки надається розробником експерту в складі матеріалів, що зазначені в п. А.2.1 та містять функціональні специфікації КЗЗ ОЕ. Додатково при аналізі моделі політики безпеки і співставленні її характеристик з вимогами реалізованої політики безпеки рекомендується також користуватися зазначеним у п. А.2.5 описом результатів аналізу відповідності між політикою безпеки, що реалізується КЗЗ ОЕ, та моделлю політики безпеки, реалізованою КЗЗ ОЕ.

Д.2 Рекомендації з виконання аналізу моделі політики безпеки

Д.2.1 Основні зусилля експерта в процесі виконання аналізу наданого опису моделі політики безпеки, реалізованої КЗЗ ОЕ, мають бути спрямовані на пошук аргументів (підтверджень, свідоцтв), що дозволяють йому сформулювати та обґрунтувати висновки:

- про чіткість визначення в описі моделі політики безпеки характеристик модельованого режиму захищеного функціонування ОЕ для всіх ФПБ, ідентифікованих в описі політики безпеки;
- про несуперечливість модельованого режиму захищеного функціонування ОЕ та вимог щодо політик ФПБ, викладених в описі політики безпеки;
- про повноту модельованого режиму захищеного функціонування ОЕ стосовно політик ФПБ, вимоги щодо яких викладені в описі політики безпеки.

Д.2.2 Для формулювання обґрунтованого висновку про чіткість визначення характеристик модельованого режиму захищеного функціонування ОЕ відповідні аргументи повинні підтверджувати, що в моделі політики безпеки для розглянутого ОЕ визначено поняття захищеності, ідентифіковані набори атрибутів всіх об'єктів, що знаходяться під керуванням КЗЗ (об'єктів-користувачів, об'єктів-процесів, пасивних об'єктів), та визначені всі дії компонентів КЗЗ, які реалізують різні ФПБ і можуть змінювати або використовувати значення цих атрибутів.

Примітка. Наприклад, якщо політика безпеки передбачає реалізацію ФПБ "Адміністративна цілісність" певного рівня, в описі моделі політики безпеки для цієї ФПБ має бути:

- визначено поняття цілісності в межах оцінюваного ОЕ;
- ідентифіковано ті типи пасивних об'єктів, для яких КЗЗ ОЕ має реалізовувати зазначену ФПБ;
- ідентифіковано ті типи об'єктів-користувачів та/або об'єктів-процесів, які повинні мати потенційну можливість модифікації пасивних об'єктів певного типу;
- ідентифіковано набори атрибутів об'єктів-користувачів, об'єктів-процесів та пасивних об'єктів, які стосуються реалізації зазначеної ФПБ;
- ідентифіковано правила, згідно з якими засоби КЗЗ повинні надавати доступ об'єктам-

користувачам та/або об'єктам-процесам з метою модифікації пасивних об'єктів певного типу;

- ідентифіковано правила, згідно з якими засоби КЗЗ повинні обробляти запити адміністраторів або спеціально уповноважених користувачів з метою зміни атрибутів об'єктів-користувачів, об'єктів-процесів та пасивних об'єктів, які стосуються реалізації зазначеної ФПБ.

Д.2.3 Для формулювання обґрунтованого висновку про несуперечливість модельованого режиму захищеного функціонування ОЕ та вимог політик ФПБ, викладених в описі політики безпеки, відповідні аргументи мають підтверджувати, що опис кожного правила або характеристики в моделі політики безпеки точно відображає вимоги щодо політик відповідних ФПБ.

Примітка. Наприклад, якщо політикою безпеки ФПБ установлено, що керування доступом має здійснюватися на рівні окремих користувачів, то модель політики безпеки, яка описує захищений режим функціонування ОЕ при реалізації цієї ФПБ в контексті керування доступом на рівні груп користувачів, не може вважатися узгодженою з політикою безпеки. Аналогічно, якщо політикою безпеки встановлено, що керування доступом має здійснюватися на рівні груп користувачів, то модель політики безпеки ОЕ, яка описує захищений режим функціонування ОЕ при реалізації цієї ФПБ в контексті керування доступом на рівні окремих користувачів, також не може вважатися узгодженою з політикою безпеки.

Д.2.4 Для формулювання обґрунтованого висновку про повноту модельованого режиму захищеного функціонування ОЕ стосовно політик ФПБ, вимоги щодо яких викладені в описі політики безпеки, експерт має розглянути правила та характеристики моделі політики безпеки та зіставити їх з правилами та характеристиками політик безпеки відповідних ФПБ. Отримані в результаті такого зіставлення аргументи мають підтверджувати, що для всіх політик ФПБ, які мають бути змодельовані, у моделі політики безпеки ОЕ наведено опис пов'язаних з ними правил та/або характеристик.

Додаток Е
Рекомендації щодо перевірки відповідності специфікацій об'єкта експертизи різного рівня деталізації та ступеня формалізації
(рекомендований)

У Додатку Е викладені рекомендації з виконання перевірки відповідності специфікацій КЗЗ ОЕ різного рівня деталізації та ступеня формалізації. Рекомендації викладені з урахуванням вимог критеріїв гарантій, наведених у НД ТЗІ 2.5-004-99, щодо підтвердження відповідності специфікацій КЗЗ ОЕ різного рівня деталізації та ступеня формалізації. Рекомендації стосуються основних дій, які має виконувати експерт у процесі виконання такої перевірки.

Е.1 Мета та питання, що вирішуються в процесі перевірки відповідності специфікацій КЗЗ ОЕ різного рівня деталізації та ступеня формалізації

Е.1.1 Основною метою виконання перевірки відповідності специфікацій КЗЗ ОЕ різного рівня деталізації (політики безпеки, моделі політики безпеки, проекту архітектури, детального проекту, реалізації) та різного ступеня формалізації є забезпечення правильного та повного відображення вимог щодо КЗЗ ОЕ в усіх, до найменш абстрактної з наданих Експерту специфікацій (представлень) КЗЗ. Підтвердження наявності такої відповідності, виконане шляхом неформального показу, демонстрації з використанням структурованого аналізу або формального доказу, є однією з необхідних умов реалізації вимог критеріїв гарантій, встановлених НД ТЗІ 2.5-004-99, у частині, що стосується послідовності розробки ОЕ.

Е.1.2 З урахуванням цієї мети, основними питаннями, що вирішуються експертом у процесі виконання зазначених перевірок, є аналіз наданих розробником описів результатів аналізу відповідності між специфікаціями КЗЗ ОЕ різного рівня деталізації та різного ступеня формалізації, зазначених у пп. А.2.5-А.2.8, з метою формулювання обґрунтованого висновку про їх повноту та коректність. При цьому експерт може, за необхідності, використовувати також матеріали, зазначені в пп. А.2.1-А.2.4, в яких наведені специфікації КЗЗ ОЕ різного рівня деталізації.

Е.2 Рекомендації з виконання перевірки результатів аналізу відповідності специфікацій ОЕ різного рівня деталізації

Е.2.1 Рекомендації з виконання перевірки результатів аналізу відповідності моделі політики безпеки політиці безпеки, реалізованій КЗЗ ОЕ

Е.2.1.1 Основні зусилля експерта в процесі виконання перевірки результатів аналізу відповідності моделі політики безпеки політиці безпеки, реалізованій КЗЗ ОЕ, мають бути спрямовані на пошук аргументів (підтверджень, свідоцтв), які дозволяють йому сформулювати та обґрунтувати висновки:

- про показ розробником наявності відповідності між переліком описаних у політиці безпеки та переліком промодельованих ФПБ;
- про показ розробником (для заявлених рівнів гарантій Г-2 … Г-3) наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації цих ФПБ та використовуваними при цьому основними (такими, що мають безпосереднє відношення до розглянутих ФПБ) атрибутами об'єктів КЗЗ різного типу;
- про демонстрацію розробником (для заявлених рівнів гарантій Г-4 … Г-7) наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації цих ФПБ та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу.

Е.2.1.2 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком описаних у політиці безпеки та переліком промодельованих ФПБ відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.5, ідентифіковані всі ФПБ, які описані в політиці безпеки, реалізованій КЗЗ ОЕ. При цьому експерт має з використанням матеріалів, зазначених у п. А.2.1, визначити перелік ФПБ, описаних у політиці безпеки, реалізованої КЗЗ ОЕ, після чого переконатися в наявності посилань на всі ці ФПБ у матеріалах, зазначених у п. А.2.5.

Е.2.1.3 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та використовуваними при цьому основними атрибутами об'єктів КЗЗ відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.5, для відповідних ФПБ показано (в оповідній формі, з використанням таблиць або іншим неструктурованим чином), що:

- у моделі політики безпеки, реалізованої КЗЗ ОЕ, та в описі політики безпеки ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика ФПБ;
- у моделі політики безпеки, реалізованої КЗЗ ОЕ, для різних об'єктів КЗЗ, на які поширюється політика ФПБ, ідентифіковані ті ж самі основні (такі, що мають безпосереднє відношення до розглянутих ФПБ) атрибути, що і в описі політики безпеки;
- модель політики безпеки, реалізованої КЗЗ ОЕ, забезпечує виконання тих самих правил реалізації ФПБ, що і політика безпеки.

При цьому експерт має для кожної ФПБ:

- визначити з використанням матеріалів, зазначених у п. А.2.1, перелік об'єктів КЗЗ, на які поширюється політика цієї ФПБ, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до розглянутої ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.1, перелік основних атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до відповідних об'єктів у межах політики розглянутої ФПБ;
- визначити з використанням матеріалів, зазначених у п. А.2.1, правила реалізації засобами КЗЗ ОЕ відповідної ФПБ, після чого переконатися в наявності посилань на ці правила в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до розглянутої ФПБ, а також у відсутності неузгодженостей або протиріч у викладенні відповідних правил в описі політики безпеки та в моделі політики безпеки, реалізованої КЗЗ ОЕ.

Е.2.1.4 Для формулювання обґрунтованого висновку про демонстрацію розробником наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та всіма використовуваними при цьому атрибутами об'єктів КЗЗ відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.5, для відповідних ФПБ продемонстровано (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями), що:

- у моделі політики безпеки, реалізованої КЗЗ ОЕ, та в описі політики безпеки ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика ФПБ;
- у моделі політики безпеки, реалізованої КЗЗ ОЕ, для різних об'єктів КЗЗ, на які поширюється політика ФПБ, ідентифіковані ті ж самі атрибути, що і в описі політики безпеки;
- модель політики безпеки, реалізованої КЗЗ ОЕ, забезпечує виконання тих самих правил реалізації ФПБ, що і політика безпеки.

При цьому експерт має для кожної ФПБ:

- визначити з використанням матеріалів, зазначених у п. А.2.1, перелік об'єктів КЗЗ, на які поширюється політика цієї ФПБ, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до розглянутої ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.1, перелік всіх атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до відповідних об'єктів у межах політики розглянутої ФПБ;
- визначити з використанням матеріалів, зазначених у п. А.2.1, правила реалізації засобами КЗЗ ОЕ відповідної ФПБ, після чого переконатися в наявності посилань на ці правила в тій частині матеріалів, зазначених у п. А.2.5, що мають відношення до розглянутої ФПБ, а також (з використанням наведених результатів структурованого аналізу) у відсутності непогодженостей або протиріч у викладенні відповідних правил в описі політики безпеки та в моделі політики безпеки, реалізованої КЗЗ ОЕ.

Е.2.2 Рекомендації з виконання перевірки результатів аналізу відповідності проекту архітектури КЗЗ ОЕ моделі політики безпеки, реалізованої КЗЗ ОЕ

Е.2.2.1 Основні зусилля експерта в процесі виконання перевірки результатів аналізу відповідності проекту архітектури КЗЗ ОЕ моделі політики безпеки, реалізованої КЗЗ ОЕ, мають бути спрямовані на пошук аргументів (підтверджень, свідоцтв), які дозволяють йому сформулювати та обґрунтувати висновки:

- про показ розробником наявності відповідності між переліком промодельованих у моделі політики безпеки ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ;

- про показ розробником (для заявлених рівнів гарантій Г-2 … Г-4) або демонстрацію розробником (для заявлених рівнів гарантій Г-5 … Г-7) наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ (порядком захищеного функціонування підсистем КЗЗ) та використовуваними при цьому основними (для заявлених рівнів гарантій Г-2 … Г-4) або всіма (для заявлених рівнів гарантій Г-5 … Г-7) атрибутами об'єктів КЗЗ різного типу;
- про доказ розробником (для заявлених рівнів гарантій Г-6 … Г-7) наявності відповідності між правилами реалізації певних ФПБ та порядком захищеного функціонування підсистем КЗЗ при реалізації цих ФПБ, викладеними, відповідно, у моделі політики безпеки, реалізованої КЗЗ ОЕ, та в проекті архітектури.

Е.2.2.2 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком промодельованих у моделі політики безпеки ФПБ та переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.6, ідентифіковані всі ФПБ, описані в політиці безпеки, реалізованій КЗЗ ОЕ, а також показано відображення цих ФПБ на функціональні компоненти (підсистеми) КЗЗ ОЕ, описані в проекті архітектури. При цьому експерт повинен з використанням матеріалів, зазначених у п. А.2.1, визначити перелік ФПБ, промодельованих у моделі політики безпеки, реалізованої КЗЗ ОЕ, з використанням матеріалів, зазначених у п. А.2.2, визначити перелік функціональних компонентів (підсистем), які складають КЗЗ ОЕ, після чого переконатися у наявності (в оповідній формі, з використанням таблиць або іншим неструктурованим чином) у матеріалах, зазначених у п. А.2.6, відображення кожної з цих ФПБ на будь-яку підсистему КЗЗ.

Е.2.2.3 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та використовуваними при цьому основними атрибутами об'єктів КЗЗ різного типу відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.6, для відповідних ФПБ показано (в оповідній формі, з використанням таблиць або іншим неструктурованим чином), що:

- в описі функціональних можливостей підсистем КЗЗ, що стосуються реалізації ФПБ, наведеному в проекті архітектури КЗЗ ОЕ, та в описі моделі політики безпеки, реалізованої КЗЗ ОЕ, ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика ФПБ;
- в описі функціональних можливостей підсистем КЗЗ, які стосуються реалізації ФПБ, наведеному в проекті архітектури КЗЗ ОЕ, для різних об'єктів КЗЗ, на які поширюється політика ФПБ, ідентифіковані ті ж самі основні (такі, що мають безпосереднє відношення до розглянутої ФПБ) атрибути, що і в моделі політики безпеки;
- опис порядку захищеного функціонування функціональних компонентів (підсистем) КЗЗ, наведений у проекті архітектури КЗЗ ОЕ, забезпечує виконання тих самих правил реалізації ФПБ, що і модель політики безпеки.

При цьому експерт має для кожної ФПБ:

- визначити з використанням матеріалів, зазначених у п. А.2.1, перелік об'єктів КЗЗ, на які поширюється політика цієї ФПБ, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.6, що мають відношення до підсистем КЗЗ, які реалізують розглянуту ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.1, перелік основних атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.6, що мають відношення до підсистем КЗЗ, які реалізують розглянуту ФПБ стосовно відповідних об'єктів;
- визначити з використанням матеріалів, зазначених у п. А.2.1, правила реалізації засобами КЗЗ ОЕ відповідної ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.2, порядок захищеного функціонування підсистем КЗЗ при реалізації розглянутої ФПБ, після чого переконатися у наявності (в оповідній формі, з використанням таблиць або іншим неструктурованим чином) у матеріалах, зазначених у п. А.2.6, відповідності порядку функціонування підсистем КЗЗ цим правилам, а також у відсутності неузгодженостей або протиріч між викладенням відповідних правил у моделі політики безпеки та описом порядку функціонування підсистем КЗЗ при реалізації цих правил.

Е.2.2.4 Для формулювання обґрунтованого висновку про демонстрацію розробником наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика певних ФПБ, правилами реалізації ФПБ та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу

відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.6, для відповідних ФПБ продемонстровано (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями), що:

- в описі функціональних можливостей підсистем КЗЗ, які стосуються реалізації ФПБ, наведеному в проекті архітектури КЗЗ ОЕ, та в описі моделі політики безпеки, реалізованої КЗЗ ОЕ, ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика ФПБ;
- в описі функціональних можливостей підсистем КЗЗ, які стосуються реалізації ФПБ, наведеному в проекті архітектури КЗЗ ОЕ, для різних об'єктів КЗЗ, на які поширюється політика ФПБ, ідентифіковані ті ж самі атрибути, що і в моделі політики безпеки;
- опис порядку захищеного функціонування функціональних компонентів (підсистем) КЗЗ, наведений у проекті архітектури КЗЗ ОЕ, забезпечує виконання тих самих правил реалізації ФПБ, що і модель політики безпеки.

При цьому експерт має для кожної ФПБ:

- визначити з використанням матеріалів, зазначених у п. А.2.1, перелік об'єктів КЗЗ, на які поширюється політика цієї ФПБ, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.6, що мають відношення до підсистем КЗЗ, які реалізують розглянуту ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.1, перелік всіх атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.6, що мають відношення до підсистем КЗЗ, які реалізують розглянуту ФПБ стосовно відповідних об'єктів;
- визначити з використанням матеріалів, зазначених у п. А.2.1, правила реалізації засобами КЗЗ ОЕ відповідної ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.2, порядок захищеного функціонування підсистем КЗЗ при реалізації розглянутої ФПБ, після чого переконатися в демонстрації (з використанням наведених результатів структурованого аналізу) у матеріалах, зазначених у п. А.2.6, відповідності порядку функціонування підсистем КЗЗ цим правилам, а також у відсутності неузгодженостей або протиріч між викладенням відповідних правил у моделі політики безпеки та описом порядку функціонування підсистем КЗЗ при реалізації цих правил.

Е.2.2.5 Для формулювання обґрунтованого висновку про доказ розробником наявності відповідності між правилами реалізації певних ФПБ та порядком захищеного функціонування підсистем КЗЗ при реалізації цих ФПБ відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.6, містяться необхідні докази та що вони є коректними. При цьому експерт повинен з використанням матеріалів, зазначених у п. А.2.1, визначити правила реалізації засобами КЗЗ ОЕ певної ФПБ, з використанням матеріалів, зазначених у п. А.2.2, визначити порядок захищеного функціонування підсистем КЗЗ при реалізації цієї ФПБ, після чого переконатися у наявності в матеріалах, зазначених у п. А.2.6, формальних доказів відповідності порядку функціонування підсистем КЗЗ цим правилам, а також переконатися (шляхом верифікації) у коректності наведених доказів.

Е.2.3 Рекомендації з виконання перевірки результатів аналізу відповідності детального проекту КЗЗ ОЕ проекту архітектури КЗЗ ОЕ

Е.2.3.1 Основні зусилля експерта в процесі виконання перевірки результатів аналізу відповідності детального проекту КЗЗ ОЕ та проекту архітектури КЗЗ ОЕ мають бути спрямовані на пошук аргументів (підтверджень, свідоцтв), які дозволяють йому сформулювати та обґрунтувати висновки:

- про показ розробником наявності відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем;
- про показ розробником (для заявлених рівнів гарантій Г-2 … Г-5) або демонстрацію розробником (для заявлених рівнів гарантій Г-6 … Г-7) наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними (для заявлених рівнів гарантій Г-2 … Г-5) або всіма (для заявлених рівнів гарантій Г-6 … Г-7) атрибутами об'єктів КЗЗ різного типу;
- про доказ розробником (для заявленого рівня гарантій Г-7) наявності відповідності між

порядком захищеного функціонування підсистем КЗЗ та порядком захищеного функціонування модулів КЗЗ, які входять до складу цих підсистем, викладеними, відповідно, у проекті архітектури та детальному проекті.

Е.2.3.2 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком ФПБ, реалізованих функціональними компонентами (підсистемами) КЗЗ ОЕ, та переліком ФПБ, реалізованих структурними компонентами (модулями) КЗЗ ОЕ, які функціонують у складі відповідних підсистем, відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.7, ідентифіковані функціональні компоненти (підсистеми), описані в проекті архітектури КЗЗ ОЕ, а також показано відображення цих підсистем на структурні компоненти (модулі) КЗЗ ОЕ, описані в детальному проекті. При цьому експерт повинен з використанням матеріалів, зазначених у п. А.2.2, визначити перелік функціональних компонентів (підсистем), які складають КЗЗ ОЕ, та ФПБ, реалізованих ними, з використанням матеріалів, зазначених у п. А.2.3, визначити перелік структурних компонентів (модулів), що складають кожну підсистему КЗЗ ОЕ, та ФПБ, до реалізації яких має відношення кожен модуль, після чого переконатися у наявності (в оповідній формі, з використанням таблиць або іншим неструктурованим чином) у матеріалах, зазначених у п. А.2.7, відображення кожної з підсистем та реалізованих ними ФПБ на відповідні модулі КЗЗ.

Е.2.3.3 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та використовуваними при цьому основними атрибутами об'єктів КЗЗ різного типу відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.7, для відповідних ФПБ та відповідних підсистем/модулів показано (в оповідній формі, з використанням таблиць або іншим неструктурованим чином), що:

- в описі функціональних можливостей усіх модулів КЗЗ, що входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведеному в детальному проекті, та в описі функціональних підсистем КЗЗ, до складу яких входять ці модулі, наведеному в проекті архітектури, ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ;
- в описі функціональних можливостей усіх модулів КЗЗ, що входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведеному в детальному проекті, та в описі функціональних підсистем КЗЗ, до складу яких входять ці модулі, наведеному в проекті архітектури, для різних об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ, ідентифіковані ті ж самі основні (такі, що мають безпосереднє відношення до розглянутої ФПБ) атрибути;
- опис порядку захищеного функціонування всіх модулів КЗЗ, які входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведений у детальному проекті, забезпечує виконання тих самих правил реалізації ФПБ, що й опис порядку захищеного функціонування цієї підсистеми КЗЗ, наведений у проекті архітектури КЗЗ ОЕ.

При цьому експерт має для кожної ФПБ, що реалізується певною підсистемою КЗЗ:

- визначити з використанням матеріалів, зазначених у п. А.2.2, перелік об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ, що реалізується цією підсистемою, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.7, які мають відношення до модулів КЗЗ, що входять до складу цієї підсистеми та задіяні в реалізації розглянутої ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.2, перелік основних атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.7, які мають відношення до модулів КЗЗ, що входять до складу цієї підсистеми та задіяні в реалізації розглянутої ФПБ стосовно відповідних об'єктів;
- визначити з використанням матеріалів, зазначених у п. А.2.2, правила реалізації відповідною підсистемою КЗЗ ОЕ розглянутої ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.3, порядок захищеного функціонування при реалізації розглянутої ФПБ модулів КЗЗ, що входять до складу цієї підсистеми, після чого переконатися у наявності (в оповідній формі, з використанням таблиць або іншим неструктурованим чином) у матеріалах, зазначених у п. А.2.7, відповідності порядку функціонування модулів КЗЗ, що входять до складу підсистеми, цим правилам, а також у відсутності неузгодженостей або протиріч між описом порядку функціонування підсистеми КЗЗ та описом порядку функціонування модулів КЗЗ при реалізації цих правил.

Е.2.3.4 Для формулювання обґрунтованого висновку про демонстрацію розробником наявності

відповідності між переліком об'єктів КЗЗ, на які поширюється політика реалізованих підсистемою/модулем ФПБ, правилами реалізації підсистемою/модулем ФПБ (порядком захищеного функціонування модулів КЗЗ) та всіма використовуваними при цьому атрибутами об'єктів КЗЗ різного типу відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.7, для відповідних ФПБ та відповідних підсистем/модулів продемонстровано (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями), що:

- в описі функціональних можливостей усіх модулів КЗЗ, які входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведеному в детальному проекті, та в описі функціональних підсистем КЗЗ, до складу яких входять ці модулі, наведеному в проекті архітектури, ідентифіковані ті ж самі переліки об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ;
- в описі функціональних можливостей усіх модулів КЗЗ, які входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведеному в детальному проекті, та в описі функціональних підсистем КЗЗ, до складу яких входять ці модулі, наведеному в проекті архітектури, для різних об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ, ідентифіковані ті ж самі атрибути;
- опис порядку захищеного функціонування всіх модулів КЗЗ, які входять у певну підсистему та стосуються реалізації розглянутої ФПБ, наведений у детальному проекті, забезпечує виконання тих самих правил реалізації ФПБ, що й опис порядку захищеного функціонування цієї підсистеми КЗЗ, наведений у проекті архітектури КЗЗ ОЕ.

При цьому експерт повинен для кожної ФПБ, що реалізується певною підсистемою КЗЗ:

- визначити з використанням матеріалів, зазначених у п. А.2.2, перелік об'єктів КЗЗ, на які поширюється політика розглянутої ФПБ, що реалізується цією підсистемою, після чого переконатися в наявності посилань на всі ці об'єкти в тій частині матеріалів, зазначених у п. А.2.7, які мають відношення до модулів КЗЗ, що входять до складу цієї підсистеми та задіяні в реалізації розглянутої ФПБ;
- для різних об'єктів КЗЗ, на які поширюється політика ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.2, перелік всіх атрибутів, після чого переконатися в наявності посилань на всі ці атрибути в тій частині матеріалів, зазначених у п. А.2.7, які мають відношення до модулів КЗЗ, що входять до складу цієї підсистеми та задіяні в реалізації розглянутої ФПБ стосовно відповідних об'єктів;
- визначити з використанням матеріалів, зазначених у п. А.2.2, правила реалізації відповідною підсистемою КЗЗ ОЕ розглянутої ФПБ, визначити з використанням матеріалів, зазначених у п. А.2.3, порядок захищеного функціонування при реалізації розглянутої ФПБ модулів КЗЗ, що входять до складу цієї підсистеми, після чого переконатися в демонстрації (з використанням наведених результатів структурованого аналізу) у матеріалах, зазначених у п. А.2.7, відповідності порядку функціонування модулів КЗЗ, що входять до складу підсистеми, цим правилам, а також у відсутності неузгодженостей або протиріч між описом порядку функціонування підсистеми КЗЗ та описом порядку функціонування модулів КЗЗ при реалізації цих правил.

Е.2.3.5 Для формулювання обґрунтованого висновку про доказ розробником наявності відповідності між порядком захищеного функціонування підсистем КЗЗ та порядком захищеного функціонування модулів КЗЗ, що входять до складу цих підсистем, відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.7, містяться необхідні докази, та що вони є коректними. При цьому експерт повинен з використанням матеріалів, зазначених у п. А.2.2, визначити порядок захищеного функціонування підсистем КЗЗ при реалізації різних ФПБ, з використанням матеріалів, зазначених у п. А.2.3, визначити порядок захищеного функціонування при реалізації розглянутих ФПБ модулів КЗЗ, що входять до складу відповідних підсистем, після чого переконатися у наявності в матеріалах, зазначених у п. А.2.7, формальних доказів відповідності порядку захищеного функціонування підсистем КЗЗ та порядку захищеного функціонування модулів КЗЗ, що входять до складу цих підсистем, при реалізації різних ФПБ, а також переконатися (шляхом верифікації) в коректності наведених доказів.

Е.2.4 Рекомендації з виконання перевірки результатів аналізу відповідності реалізації КЗЗ ОЕ детальному проекту КЗЗ ОЕ

Е.2.4.1 Основні зусилля експерта в процесі виконання перевірки результатів аналізу відповідності реалізації КЗЗ ОЕ детальному проекту КЗЗ ОЕ повинні бути спрямовані на пошук аргументів (підтверджень, свідоцтв), що дозволяють йому сформулювати та обґрунтувати висновки:

- про показ розробником (для заявлених рівнів гарантій Г-3 … Г-6) або демонстрацію розробником (для заявленого рівня гарантій Г-7) наявності відповідності між наведеними в детальному проекті характеристиками (порядком захищеного функціонування, використовуваними атрибутами об'єктів КЗЗ, параметрами інтерфейсів) структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів;
- про демонстрацію розробником (для заявленого рівня гарантій Г-7) наявності відповідності між наведеними в детальному проекті характеристиками (реалізованими функціями, параметрами інтерфейсів) процедур, що містяться в бібліотеках часу виконання операційної системи (ядрі операційної системи) та використовуються в процесі функціонування всіх структурних компонентів (модулів) КЗЗ, і наданим розробником вхідним кодом реалізації цих процедур.

Е.2.4.2 Для формулювання обґрунтованого висновку про показ розробником наявності відповідності між наведеними в детальному проекті характеристиками структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.8, для відповідних модулів та вхідного коду їх реалізації показано (в оповідній формі, з використанням таблиць або іншим неструктурованим чином), що:

- наданий вхідний код реалізує вимоги щодо інтерфейсів модулів КЗЗ (які стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), викладені в детальному проекті;
- наданий вхідний код забезпечує реалізацію викладеного в детальному проекті порядку захищеного функціонування модулів КЗЗ з використанням атрибутів об'єктів КЗЗ, визначених у детальному проекті.

При цьому експерт має для кожного структурного компонента (модуля) КЗЗ, вхідний код реалізації якого наданий розробником:

- визначити з використанням матеріалів, зазначених у п. А.2.3, перелік вимог до характеристик його інтерфейсів (які стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), після чого переконатися в наявності посилань на всі ці характеристики в тій частині матеріалів, зазначених у п. А.2.8, що мають відношення до розглянутого модуля КЗЗ;
- визначити з використанням матеріалів, зазначених у п. А.2.3, порядок захищеного функціонування модуля, після чого переконатися у наявності (в оповідній формі, з використанням таблиць або іншим неструктурованим чином) у матеріалах, зазначених у п. А.2.8, факту повної та коректної реалізації цього порядку в наданому вхідному коді.

Е.2.4.3 Для формулювання обґрунтованого висновку про демонстрацію розробником наявності відповідності між наведеними в детальному проекті характеристиками структурних компонентів (модулів) КЗЗ ОЕ та наданим розробником вхідним кодом реалізації цих модулів відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.8, для відповідних модулів та вхідного коду їх реалізації продемонстровано (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями), що:

- наданий вхідний код реалізує вимоги щодо інтерфейсів модулів КЗЗ (які стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), викладені в детальному проекті;
- наданий вхідний код забезпечує реалізацію викладеного в детальному проекті порядку захищеного функціонування модулів КЗЗ з використанням атрибутів об'єктів КЗЗ, визначених у детальному проекті.

При цьому експерт повинен для кожного структурного компонента (модуля) КЗЗ, вхідний код реалізації якого наданий розробником:

- визначити з використанням матеріалів, зазначених у п. А.2.3, перелік вимог до характеристик його інтерфейсів (що стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), після чого переконатися в наявності посилань на всі ці характеристики в тій частині матеріалів, зазначених у п. А.2.8, які мають відношення до розглянутого модуля КЗЗ;
- визначити з використанням матеріалів, зазначених у п. А.2.3, порядок захищеного функціонування модуля, після чого переконатися в демонстрації (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями) у матеріалах, зазначених у п. А.2.8, факту повної та

коректної реалізації цього порядку в наданому вхідному коді.

Е.2.4.4 Для формулювання обґрунтованого висновку про демонстрацію розробником наявності відповідності між наведеними в детальному проекті характеристиками (реалізованими функціями, параметрами інтерфейсів) процедур, що містяться в бібліотеках часу виконання операційної системи (ядрі операційної системи) та використовуються в процесі функціонування всіх структурних компонентів (модулів) КЗЗ, та наданим розробником вхідним кодом реалізації цих процедур відповідні аргументи повинні підтверджувати, що в матеріалах, зазначених у п. А.2.8, для відповідних процедур та вхідного коду їх реалізації продемонстровано (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями), що:

- наданий вихідний код реалізує вимоги щодо інтерфейсів використовуваних процедур (які стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), викладені в детальному проекті;
- наданий вхідний код забезпечує реалізацію вимог детального проекту до функцій, що реалізуються розглянутими процедурами.

При цьому експерт повинен для кожної процедури, яка міститься в бібліотеках часу виконання операційної системи (ядрі операційної системи), вхідний код реалізації якої наданий розробником:

- визначити з використанням матеріалів, зазначених у п. А.2.3, перелік вимог до характеристик інтерфейсу процедури (які стосуються імен точок входу, призначення, методів використання, параметрів, результатів, повідомлень про помилки та кодів повернення), після чого переконатися в наявності посилань на всі ці характеристики в тій частині матеріалів, зазначених у п. А.2.8, які мають відношення до розглянутої процедури;
- визначити з використанням матеріалів, зазначених у п. А.2.3, вимоги до функцій, що реалізуються розглянутою процедурою, після чого переконатися в демонстрації (з використанням результатів структурованого аналізу у вигляді, наприклад, структурованого набору таблиць або діаграм відповідності, супроводжуваного поясненнями) у матеріалах, зазначених у п. А.2.8, факту повної та коректної реалізації цих функцій наданим вхідним кодом.