НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Департамент спеціальних телекомунікаційних систем та
захисту інформації Служби безпеки України

Київ 1999

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та захисту
інформації Служби безпеки України
від “ 28 ” квітня 1999 р. № 22
із змінами згідно наказу Адміністрації
Держспецзв'язку від 28.12.2012 № 806

Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

НД ТЗІ 2.5-004-99

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО товариством з обмеженою відповідальністю «Інститут комп'ютерних технологій»

2 ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

3 ВВЕДЕНО ВПЕРШЕ

Зміст

КРИТЕРІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Чинний від 1999-07-01

1 Галузь використання

Цей нормативний документ (далі — Критерії) — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обгрунтованості документ є відкритим для включення до його складу Адміністрацією Державної служби спеціального зв'язку та захисту інформації України нових послуг.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

ДСТУ 3230-95. Управління якістю і забезпечення якості. Терміни і визначення.

ДСТУ 2853-94. Програмні засоби ЭОМ. Підготовка і проведення випробувань.

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

НД ТЗІ 1.1-004-99. 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.

3 Визначення

В цьому нормативному документі використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99 “Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу“.

4 Позначення і скорочення

В цьому нормативному документі використовуються такі позначення і скорочення:

Загальні терміни:

АС — автоматизована система;

КС — комп'ютерна система;

КЗЗ — комплекс засобів захисту;

НСД — несанкціонований доступ;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

ПЗП — постійний запам’ятовуючий пристрій;

ПРД — правила розмежування доступу;

Позначення послуг:

КД — довірча конфіденційність;

КА — адміністративна конфіденційність;

КО — повторне використання об'єктів;

КК — аналіз прихованих каналів;

КВ — конфіденційність при обміні;

ЦД — довірча цілісність;

ЦА — адміністративна цілісність;

ЦО — відкат;

ЦВ — цілісність при обміні;

ДР — використання ресурсів;

ДВ — стійкість до відмов;

ДЗ — гаряча заміна;

ДВ — відновлення після збоїв;

НР — реєстрація;

НИ — ідентифікація і автентифікація;

НК — достовірний канал;

НО — розподіл обов'язків;

НЦ — цілісність КЗЗ;

НТ — самотестування;

НВ — автентифікація при обміні;

НА — автентифікація відправника;

НП — автентифікація одержувача.

5 Побудова і структура критеріїв захищеності інформації

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

вимоги до функцій захисту (послуг безпеки);

вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення *n*, де *n* — унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі “Критерії цілісності”. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі “Критерії доступності”. В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги

треба шукати у розділі “Критерії спостереженості”. В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру Критеріїв показано на рисунку 1.

Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги *аналіз прихованих каналів* залежність між функціональними послугами і гарантіями відсутня. **Рівень послуги *цілісність комплексу засобів захисту* НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.**

Порядок оцінки комп'ютерної системи на предмет відповідності цим Критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

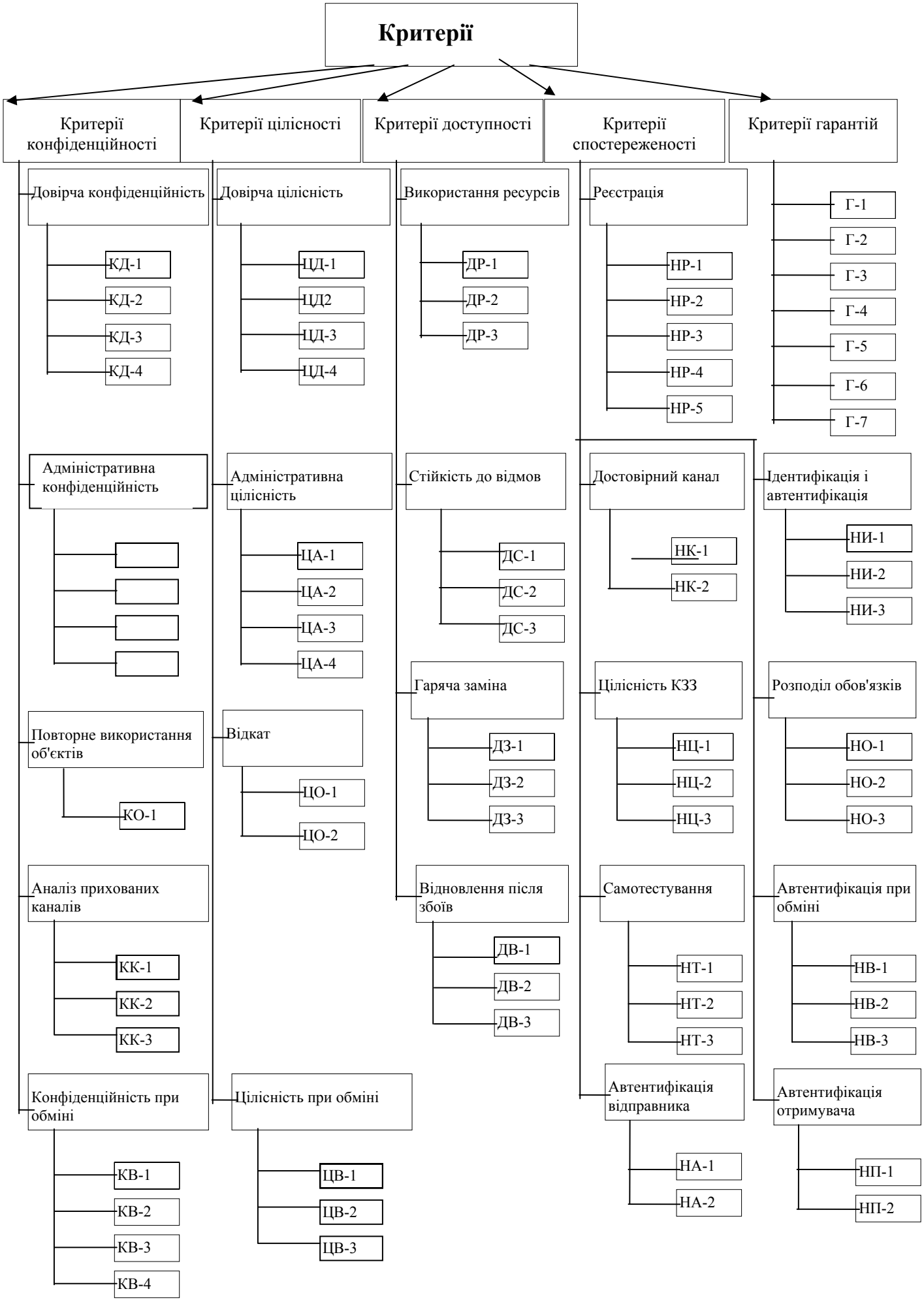

Рисунок 1 - Структура критеріїв

6 Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

6.1 Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

6.2 Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості управління.

<table>
<tr><th>КА-1. Мінімальна адміністративна конфіденційність</th><th>КА-2. Базова адміністративна конфіденційність</th><th>КА-3. Повна адміністративна конфіденційність</th><th>КА-4. Абсолютна адміністративна конфіденційність</th></tr>
<tr><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НО-1, НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1</td></tr>
</table>

6.3 Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

6.4 Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ран жируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

<table>
<tr><th>КК-1. Виявлення прихованих каналів</th><th>КК-2. Контроль прихованих каналів</th><th>КК-3. Перекриття прихованих каналів</th></tr>
<tr><td colspan="3">Повинен бути виконаний аналіз прихованих каналів</td></tr>
<tr><td colspan="2">Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані
Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів
Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність</td><td rowspan="2">Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені</td></tr>
<tr><td>—</td><td>КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: КО-1, Г-3</td><td>НЕОБХІДНІ УМОВИ: КО-1, НР-1, Г-3</td><td>НЕОБХІДНІ УМОВИ: КО-1, Г-3</td></tr>
</table>

6.5 Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КВ-1. Мінімальна конфіденційність при обміні</th><th>КВ-2. Базова конфіденційність при обміні</th><th>КВ-3. Повна конфіденційність при обміні</th><th>КВ-4. Абсолютна конфіденційність при обміні</th></tr>
<tr><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься</td><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів</td></tr>
<tr><td colspan="4">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="4">КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається</td></tr>
<tr><td>—</td><td colspan="3">Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і приймальника об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і джерела об'єкта</td></tr>
<tr><td colspan="2">—</td><td colspan="2">Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника</td></tr>
</table>

			Політика конфіденційності при обміні повинна включати опис інформації , яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані. Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення
НЕОБХІДНІ УМОВИ: НЕМАЄ	НО-1	НО-1, НВ-1	НО-1, НВ-1, НР-1, Г-3

7 Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

7.1 Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦД-1. Мінімальна довірча цілісність</th><th>ЦД-2. Базова довірча цілісність</th><th>ЦД-3. Повна довірча цілісність</th><th>ЦД-4. Абсолютна довірча цілісність</th></tr>
<tr><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

7.2 Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦА-1. Мінімальна адміністративна цілісність</th><th>ЦА-2. Базова адміністративна цілісність</th><th>ЦА-3. Повна адміністративна цілісність</th><th>ЦА-4. Абсолютна адміністративна цілісність</th></tr>
<tr><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НО-1, НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1</td></tr>
</table>

7.3 Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ран жируються на підставі множини операцій, для яких забезпечується відкат.

<table>
<tr><th>ЦО-1. Обмежений відкат</th><th>ЦО-2. Повний відкат</th></tr>
<tr><td colspan="2">Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td></tr>
<tr><td colspan="2">Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити</td></tr>
<tr><td>певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу</td><td>всі операції, виконані над захищеним об'єктом за певний проміжок часу</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

7.4 Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦВ-1: Мінімальна цілісність при обміні</th><th>ЦВ-2: Базова цілісність при обміні</th><th>ЦВ-3: Повна цілісність при обміні</th></tr>
<tr><td colspan="3">Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="3">КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається</td></tr>
<tr><td rowspan="2">—</td><td colspan="2">а також фактів його видалення або дублювання</td></tr>
<tr><td colspan="2">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—
і приймальника об'єкта</td></tr>
<tr><td>—</td><td colspan="2">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—
і джерела об'єкта</td></tr>
<tr><td>—</td><td colspan="2">Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="2">—</td><td>Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НЕМАЄ</td><td>НО-1</td><td>НО-1, НВ-1</td></tr>
</table>

8 Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

8.1 Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

<table>
<tr><th>ДР-1. Квоти</th><th colspan="2">ДР-2. Недопущення захоплення ресурсів</th><th>ДР-3. Пріоритетність використання ресурсів</th></tr>
<tr><td>Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="3">Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС</td></tr>
<tr><td colspan="4">Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються</td></tr>
<tr><td colspan="3">окремому користувачу</td><td>окремому користувачу і довільним групам користувачів</td></tr>
<tr><td colspan="4">Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку</td></tr>
<tr><td colspan="2">окремого користувача</td><td>окремого користувача і довільних груп користувачів</td></tr>
<tr><td colspan="4">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

8.2 Стійкість до відмов

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ран жируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

<table>
<tr><th>ДС-1. Стійкість при обмежених відмовах</th><th>ДС-2. Стійкість з погіршенням характеристик обслуговування</th><th>ДС-3. Стійкість без погіршення характеристик обслуговування</th></tr>
<tr><td colspan="3">Розробник повинен провести аналіз відмов компонентів КС</td></tr>
<tr><td>Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування</td><td colspan="2">Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів КС</td></tr>
<tr><td colspan="3">Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги</td></tr>
<tr><td colspan="2">Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування</td><td>Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування</td></tr>
<tr><td colspan="3">КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

8.3 Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ран жируються на підставі повноти реалізації.

ДЗ-1. Модернізація	**ДЗ-2. Обмежена гаряча заміна**	**ДЗ-3. Гаряча заміна будь-якого компонента**
Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування
Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	
НЕОБХІДНІ УМОВИ: НО-1	НЕОБХІДНІ УМОВИ: НО-1, ДС-1	

8.4 Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ран жируються на підставі міри автоматизації процесу відновлення.

<table>
<tr><th>ДВ-1. Ручне відновлення</th><th>ДВ-2. Автоматизоване відновлення</th><th>ДВ-3. Вибіркове відновлення</th></tr>
<tr><td colspan="3">Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС</td></tr>
<tr><td>Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td><td>Після відмови КС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення КС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути КС до нормального функціонування</td><td>Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності заново інсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування</td></tr>
<tr><td>—</td><td colspan="2">Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td></tr>
<tr><td colspan="2">Повинні існувати ручні процедури, за допомогою яких можна безпечним чином
повернути КС до нормального функціонування</td><td>повернути КС з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

9 Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

9.1 Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

<table>
<tr><td>НР-1. Зовнішній аналіз</td><td>НР-2. Захищений журнал</td><td>НР-3. Сигналізація про небезпеку</td><td>НР-4. Детальна реєстрація</td><td>НР-5. Аналіз в реальному часі</td></tr>
<tr><td colspan="5">Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються</td></tr>
<tr><td colspan="3">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки</td><td colspan="2">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки</td></tr>
<tr><td colspan="5">Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події</td></tr>
<tr><td>КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту</td><td colspan="4">КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.
Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації</td></tr>
<tr><td colspan="2">—</td><td colspan="3">КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій</td></tr>
<tr><td colspan="4">—</td><td>КЗЗ має бути здатним виявляти і аналізувати несанкціоновані дії в реальному часі</td></tr>
<tr><td>НИ-1</td><td colspan="4">НЕОБХІДНІ УМОВИ: НИ-1, НО-1</td></tr>
</table>

9.2 Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації.

<table>
<tr><th>НИ-1. Зовнішня ідентифікація і автентифікація</th><th>НИ-2. Одиночна ідентифікація і автентифікація</th><th>НИ-3. Множинна ідентифікація і автентифікація</th></tr>
<tr><td colspan="3">Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ</td></tr>
<tr><td colspan="3">Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен</td></tr>
<tr><td>з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача</td><td>автентифікувати цього користувача з використанням захищеного механізму</td><td>автентифікувати цього користувача з використанням захищених механізмів двох або більше типів</td></tr>
<tr><td>—</td><td colspan="2">КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НЕМАЄ</td><td colspan="2">НЕОБХІДНІ УМОВИ: НК-1</td></tr>
</table>

9.3 Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НК-1. Однонаправлений достовірний канал	**НК-2. Двонаправлений достовірний канал**
Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ	
Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ
—	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача
НЕОБХІДНІ УМОВИ: НЕМАЄ	

9.4 Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ран жируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

<table>
<tr><th>НО-1. Виділення адміністратора</th><th>НО-2. Розподіл обов'язків адміністраторів</th><th>НО-3. Розподіл обов'язків на підставі привілеїв</th></tr>
<tr><td colspan="3">Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції</td></tr>
<tr><td>—</td><td colspan="2">Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі</td></tr>
<tr><td colspan="2">—</td><td>Політика розподілу обов'язків повинна визначати множину ролей користувачів</td></tr>
<tr><td colspan="3">Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

9.5 Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

<table>
<tr><th>НЦ-1. КЗЗ з контролем цілісності</th><th colspan="2">НЦ-2. КЗЗ з гарантованою цілісністю</th><th>НЦ-3. КЗЗ з функціями диспетчера доступу</th></tr>
<tr><td>Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ</td><td colspan="3">Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів</td></tr>
<tr><td>В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td><td colspan="3">КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування</td></tr>
<tr><td colspan="2">Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ</td><td colspan="2">КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НР-1, НО-1</td><td colspan="3">НЕОБХІДНІ УМОВИ: НЕМАЄ</td></tr>
</table>

9.6 Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

<table>
<tr><th>НТ-1. Самотестування за запитом</th><th>НТ-2. Самотестування при старті</th><th>НТ-3. Самотестування в реальному часі</th></tr>
<tr><td colspan="3">Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ</td></tr>
<tr><td colspan="3">КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження,</td></tr>
<tr><td>—</td><td>при ініціалізації КЗЗ
—</td><td>і в процесі штатного функціонування</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

9.7 Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

<table>
<tr><th>НВ-1: Автентифікація вузла</th><th>НВ-2: Автентифікація джерела даних</th><th>НВ-3: Автентифікація з підтвердженням</th></tr>
<tr><td colspan="3">Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ
КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму
Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації</td></tr>
<tr><td>—</td><td colspan="2">КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується</td></tr>
<tr><td colspan="2">—</td><td>Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НЕМАЄ</td></tr>
</table>

9.8 Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ран жируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НА-1: Базова автентифікація відправника	**НА-2: Автентифікація відправника з підтвердженням**
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: НИ-1	

9.9 Автентифікація отримувача

Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ран жируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта
НЕОБХІДНІ УМОВИ: НИ-1	

10 Критерії гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

10.1 Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені	+	=	=	=	=	=	=
КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень	-	-	+	=	=	=	=
Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня	-	-	-	+	=	=	=
З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту	-	-	-	-	+	=	=
Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних	-	-	-	-	+	=	=

* В таблицях використовуються такі позначення: “-” — вимога відсутня; “+” — вимога з'являється; “=“ — вимога зберігається.

10.2 Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Процес розробки							
Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги	+	=	=	=	=	=	=
Розробник повинен описати стандарти кодування, яким необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані	-	-	+	=	=	=	=
Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки	-	-	-	+	=	=	=
Керування конфігурацією							
Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ	+	=	=	+ *	=	=	=
Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вихідного коду і обліку всіх змін з появою нових версій	-	-	-	+	=	=	=
Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації	-	-	-	+	=	=	=
Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування	-	-	-	-	-	+	=

* Починаючи з рівня Г-4 система керування конфігурацією повинна базуватися на автоматизованих засобах.

10.3 Послідовність розробки

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Функціональні специфікації (політика безпеки)							
На стадії розробки технічного завдання Розробник повинен розробити функціональні специфікації КС. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ	+	=	=	=	=	=	=
Функціональні специфікації (модель політики безпеки)							
Відповідність політиці безпеки	-	Показ		Демонстрація			
Функціональні специфікації повинні включати модель політики безпеки	-	+	=	=	=	=	=
Стиль специфікації: неформалізована	-						
частково формалізована	-						
формалізована	-						
Проект архітектури							
Відповідність моделі політики безпеки	-	Показ			Демонстрація	Доказ	
На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення	+	=	=	=	=	=	=
Стиль специфікації: неформалізована							
частково формалізована							

формалізована							
Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Детальний проект							
Відповідність проекту архітектури	-	Показ				Демонстрація	Доказ
На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ	+	=	=	=	=	=	=
Стиль специфікації: неформалізована		Весь КЗЗ *					
частково формалізована							
формалізована							
Реалізація							
Відповідність детальному проекту	-	-	Показ				Демонстрація
Розробник повинен подати вихідний код: частини КЗЗ	-	-	+	=	=	=	=
всього КЗЗ	-	-	-	-	+	=	=
всіх бібліотек часу виконання	-	-	-	-	-	-	+

* Для рівня Г-1 вимагається детальний проект компонентів КЗЗ, що мають безпосереднє відношення до безпеки.

10.4 Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску	+	=	=	=	=	=	=
Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії	-	-	+	=	=	=	=
Для підтримки відповідності між КЗЗ, що поставляється Замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеної КС	-	-	-	-	-	+	=

10.5 Документація

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

10.6 Випробування комплексу засобів захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=
Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

Додаток А

Функціональні послуги

В цьому додатку наводяться деякі пояснення вимог, викладених у функціональних критеріях, а також пояснення з приводу необхідних умов.

А.1 Критерії конфіденційності

В будь-якій КС інформація може переміщуватись в одному з двох напрямів: від користувача до об'єкта або від об'єкта до користувача. Шляхи переміщування, як і пристрої введення-виведення, можуть бути різноманітними. Конфіденційність забезпечується через додержання вимог політики безпеки щодо переміщення інформації від об'єкта до користувача або процесу. Правильне (допустиме) переміщення визначається як переміщення інформації до авторизованого користувача, можливо, через авторизований процес.

В цьому розділі Критеріїв зібрані послуги, реалізація яких дозволяє забезпечити захист інформації від несанкціонованого ознайомлення з нею (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою конфіденційності.

А.1.1 Довірча конфіденційність

Послуги довірча конфіденційність і адміністративна конфіденційність, довірча цілісність і адміністративна цілісність, а також деякою мірою — використання ресурсів, є класичними послугами, що безпосередньо реалізують ту частину політики безпеки, яка складає ПРД.

Основні особливості і відмінність довірчого і адміністративного керування доступом розглянуті в НД ТЗІ 1.1-004-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу". Система, яка реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи встановлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, яка реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

Послуга довірча конфіденційність дозволяє користувачеві керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Як правило, під об'єктами, що належать домену користувача, маються на увазі об'єкти, власником яких є користувач (створені користувачем).

Для відображення функціональності КС у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів КС, а як елементи матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двовимірною (наприклад, користувачі/пасивні об'єкти) або тривимірною

(користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих в даний час об’єктів КС даного типу, або частковою. Повна тривимірна матриця доступу дозволяє точно описати хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта) та який вид доступу може отримати.

Рівні послуги довірча конфіденційність ранжируются на підставі повноти захисту і вибірковості керування.

Мінімальна довірча конфіденційність (КД-1). Найбільш слабкою мірою гарантії захисту від несанкціонованого ознайомлення є накладення обмеження на одержання інформації процесами. На цьому рівні дозволені потоки інформації від об'єкта тільки до певних процесів. Хоч і не існує обмеження на те, хто може активізувати процес, тобто, хто може одержувати інформацію, КЗЗ обмежує потоки інформації фіксованому списку процесів, грунтуючись на атрибутах доступу об'єктів і процесів. Користувач, домену якого належить об’єкт, може змінювати список процесів, які можуть одержувати інформацію від об'єкта. Для такої системи можна побудувати часткову або повну матрицю доступу процесів до захищених об'єктів.

Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

Повна довірча конфіденційність (КД-3). Основна відміна від попереднього рівня це те, що КЗЗ повинен забезпечувати більш високу вибірковість керування тим, які користувачі можуть одержати інформацію від об'єкта або ініціювати процес. Користувач, домену якого належить об'єкт, може вказати права доступу для кожного конкретного користувача і групи користувачів. Є можливим включати або вилучати користувачів із списку доступу. Для такої системи можна побудувати повну матрицю доступу користувачів до захищених об'єктів і процесів. Така вибірковість керування може бути одержана, наприклад, за рахунок використання списків доступу.

Абсолютна довірча конфіденційність (КД-4). Даний рівень забезпечує повне керування потоками інформації в КС. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення користувачів, процесів і пар процес/користувач, які можуть отримати інформацію від об'єкта. Таким чином гарантується, що інформація надсилається об’єктом потрібному користувачеві через авторизований процес. Вимоги до вибірковості керування залишаються такими ж самими, як і для попереднього рівня. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, що цілком очевидно. Для рівнів КД-3 і КД-4 необхідною умовою є реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки, якщо при виділенні об'єкта користувачеві в цьому об'єкті міститься інформація, що залишилась від попереднього користувача, то це може призвести до витоку інформації, і всі зусилля щодо реалізації даних рівнів послуги будуть марні.

А.1.2 Адміністративна конфіденційність

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до

користувачів.

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію. Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування повністю аналогічне рівням послуги довірча конфіденційність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги довірча конфіденційність, для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 — рівня КО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути визначені ролі звичайного користувача і адміністратора.

А.1.3 Повторне використання об'єктів

КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття ".

Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

А.1.4 Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і вилучення потоків інформації, що існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Ніякого обмеження на смугу пропускання прихованих каналів і ніякої різниці між прихованими каналами з пам'яттю і тимчасовими прихованими каналами не робиться. Проте це не означає, що смуга пропускання прихованих каналів не повинна обмежуватись. На практиці, наприклад, може виявитись даремною реалізація послуг конфіденційності на рівнях КД-4 і КА-4, якщо в системі існують приховані канали з смугою пропускання у декілька сотень кілобайт за секунду.

Необхідною умовою для реалізації всіх рівнів даної послуги є рівень гарантій не нижче Г-3, оскільки розробник повинен виконати аналіз прихованих каналів на етапі проектування системи, а також реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки можливість одержання інформації, що залишилась в об'єкті від попереднього користувача, сама собою може розглядатися як прихований канал.

А.1.5 Конфіденційність при обміні

В розподіленому оточенні можуть взаємодіяти різні КЗЗ, які часто реалізують різні політики безпеки інформації. Послуги захисту інформації при обміні (конфіденційність при обміні, цілісність при обміні, ідентифікація і автентифікація при обміні, автентифікація відправника і автентифікація одержувача) дозволяють забезпечити безпеку обміну інформацією між такими КЗЗ через незахищене середовище.

КЗЗ розглядає ресурси КС в якості об'єктів і управляє взаємодією цих об'єктів відповідно до реалізованої політики безпеки інформації. Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне подання (форма, синтаксис). Об'єкт характеризується своїм станом (змістом), що в свою чергу характеризується атрибутами, і поводженням, яке визначає засоби зміни стану.

Локалізований КЗЗ (наприклад, операційна система з функціями захисту) розглядає тільки логічне подання об'єктів. Фізичне подання об'єктів захищене тільки від внутрішніх об'єктів, а не від впливу з боку зовнішніх сутностей (агентів). Захист від зовнішніх щодо КС загроз реалізується організаційними заходами і заходами фізичного захисту. До зовнішніх впливів схильні об'єкти, що зберігаються в енергонезалежній пам'яті (зовнішніх носіях).

У розподіленому оточенні не можна гарантувати, що зовнішній агент не може отримати доступ до фізичного подання об'єктів. Особливо це відноситься до ліній зв'язку (каналів взаємодії). Таким чином, необхідно, щоб об’єкти були захищені під час їх експорту із фізично безпечного оточення.

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Реалізація даної послуги на рівні КВ-2 дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити захист від компрометації за рахунок аналізу трафіку і від витоку інформації прихованими каналах обміну, що існують. Для реалізації даного рівня від розробника вимагається виконання аналізу прихованих каналів.

А.2 Критерії цілісності

Цілісність забезпечується дотриманням вимог політики безпеки щодо переміщення інформації до об’єкта з боку користувача або процесу. Правильне (допустиме) переміщення визначається як переміщення інформації до об’єкта від авторизованого користувача або

процесу

В даному розділі Критеріїв зібрані послуги, реалізація яких дозволяє забезпечити захист інформації від несанкціонованої модифікації (включаючи її знищення). Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні. Принципи, що лежать в основі реалізації послуг, визначаються політикою цілісності.

А.2.1 Довірча цілісність

Дана послуга дозволяє користувачеві керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність (ЦД-1). На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

Базова довірча цілісність (ЦД-2). Більш сильним методом запобігання неавторизованій модифікації є накладення обмежень на те, який процес або група процесів може модифікувати об’єкт. Користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку процесів і груп процесів. Для такої системи можна побудувати часткову матрицю доступу процесів до захищених об'єктів.

Повна довірча цілісність (ЦД-3). Основна відмінність між рівнями ЦД-2 і ЦД-3 полягає в тому, що на даному рівні надається більш висока вибірковість керування тим, які процеси можуть або не можуть модифікувати об'єкт. Для такої системи можна побудувати повну матрицю доступу процесів до захищених об'єктів.

Абсолютна довірча цілісність (ЦД-4). Реалізація послуги довірча цілісність на даному рівні забезпечує повне керування потоками інформації всередині системи. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення користувачів, процесів і пар процес/користувач, які можуть модифікувати об'єкт. Це гарантує, що модифікація об'єкта здійснюється авторизованим користувачем за допомогою авторизованого процесу. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/ процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, що цілком очевидно. Для рівнів ЦД-3 і ЦД-4 необхідною умовою є реалізація рівня КО-1 послуги повторне використання об'єктів, оскільки її відсутність може привести до того, що під час подання об'єкта користувачеві в цьому об'єкті вже міститься деяка інформація, джерело якої не визначено.

А.2.2 Адміністративна цілісність

Ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування аналогічно рівням послуги довірча цілісність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги довірча цілісність для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 — рівня ДО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути визначені ролі звичайного користувача і адміністратора.

А.2.3 Відкат

Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об’єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Мається на увазі, що відкат — завжди доступна автоматизована послуга. Використання відкладеного резервування, що вимагає втручання користувача для завантаження резервного носія, не є реалізацією відкату. Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі. Відміна операції не повинна приводити до видалення з журналу запису про операцію, яка пізніше була відмінена.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація

А.2.4 Цілісність при обміні

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє забезпечити виявлення випадкових або навмисних порушень цілісності не тільки окремих повідомлень, але і потоків повідомлень в цілому.

А.3 Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ КС, що оцінюється, повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації, на певному проміжку часу і гарантувати спроможність КС функціонувати в разі відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов,

гаряча заміна, відновлення після збоїв.

А.3.1 Використання ресурсів

Дана послуга дозволяє керувати використанням послуг і ресурсів користувачами. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процессора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів.

Рівень послуги ДР-2 являє собою реалізацію досконалішої форми квот. Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

Рівень послуги ДР-3 додатково дозволяє управляти пріоритетністю використання ресурсів. Користувачі групуються адміністратором так, щоб визначити пріоритетні групи. Таким чином, у разі високого завантаження КС може знаходитись в стані, коли тільки користувачі, які мають високий приорітет, можуть мати доступ до системи за рахунок інших користувачів.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків (і як наслідок, — рівня НИ-1 послуги ідентифікація і автентифікація).

А.3.2 Стійкість до відмов

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій чи КС в цілому) після відмови її компоненту. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість КС продовжувати функціонування залежно від кількості відмов і послуг, доступних після відмови.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, — рівня НИ-1 послуги ідентифікація і автентифікація).

А.3.3 Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти захисту. Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

Необхідною умовою для реалізації всіх рівнів даної послуги, є реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, — рівня НИ-1 послуги ідентифікація і автентифікація), а для рівнів ДЗ-2 і ДЗ-3 — рівня ДС-1 послуги стійкість до відмов, оскільки для того, щоб забезпечити можливість гарячої заміни компонента, система повинна

забезпечувати свою працездатність у разі відмови даного компонента.

А.3.4 Відновлення після збоїв

Дана послуга забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення. Відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації КЗЗ може продукувати відновлення працездатності автоматично. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Необхідною умовою для реалізації всіх рівнів даної послуги — реалізація рівня НО-1 послуги розподіл обов'язків (і, як наслідок, — рівня НИ-1 послуги ідентифікація і автентифікація).

А.2 Критерії спостереженості

Для того, щоб КС могла бути оцінена на відповідність критеріям спостереженості, КЗЗ повинен надавати послуги щодо забезпечення відповідальності користувача за свої дії і щодо підтримки спроможності КЗЗ виконувати свої функції. Спостережність забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

А.2.1 Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності виявлення потенційних порушень.

Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів.

Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації.

Для жодного з рівнів послуги не встановлюється ніякого фіксованого набору контрольованих подій, оскільки для кожної системи їх перелік може бути специфічним. Критична для безпеки подія визначається як подія, пов'язана з звертанням до якої-небудь послуги безпеки або результатів виконання якої-небудь функції КЗЗ, або як будь-яка інша подія, яка хоч прямо і не пов'язана з функціонуванням механізмів, які реалізують послуги безпеки, але може призвести до порушення політики безпеки. Остання група подій визначається як така, що має непряме відношення до безпеки. Для визначення ступеню небезпеки таких подій часто необхідним має бути їх аналіз у контексті інших подій, що відбулися.

Для реалізації найбільш високих рівнів даної послуги необхідна наявність засобів аналізу журналу реєстрації. Засоби аналізу — це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики

безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати події, що реєструються. Це може бути досягнено або через "передвибірки", або "поствибірки". Передвиборка подій, що реєструються, дозволяє виділити під час ініціалізації системи з всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файла. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

Для реалізації найбільш високого рівня даної послуги (НР-5) необхідно, щоб аналіз даних реєстрації здійснювався в реальному часі.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів вище НР-1 — рівня НО-1 послуги розподіл обов'язків.

А.2.2 Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. За результатами ідентифікації і автентифікації користувача система (КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві ввійти в систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації Відомі три основних типа автентифікації: щось, відоме користувачеві; щось, чим володіє користувач; щось, властиве користувачеві.

Пароль, персональний ³äåíòèô³êàö³éíèé номер або інша подібна інформація є прикладом того, що називається "дещо, відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Такі фізичні об'єкти як смарт-карта, магнітна картка, генератор запитів-відповідей, електронний ключ або фізично прошитий криптографічний ключ є прикладами того, що називається "дещо, чим володіє користувач". Основною перевагою даного типу автентифікації є складність або висока вартість дублювання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Результати таких біометричних вимірювань, як відбитки пальців, параметри райдужної оболонки ока або геометрія руки служать прикладами того, що називають "дещо, що властиве користувачеві". Реалізація даного типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для

використання даного механізму є висока вартість пристроїв автентифікації. Крім того, використання цих достатньо дорогих засобів автентифікації не гарантує безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може стати непридатним для деяких застосувань.

Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу для найбільш високого рівня даної послуги (НИ-3) вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад, введеного з клавіатури пароля і носимого ідентифікатора.

Для реалізації рівнів НИ-2 і НИ-3 даної послуги необхідною умовою є реалізація рівня НК-1 послуги достовірний канал.

А.2.3 Достовірний канал

Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Реалізація даної послуги є необхідною умовою для реалізації рівнів НИ-2 і НИ-3 послуги ідентифікація і автентифікація.

А.2.4 Розподіл обов'язків

Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача (рівень НО-1).

Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі специфічними наборами адміністративних обов'язків. Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів). Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов’язково мають бути абсолютно взаємовиключаючими, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам і т.ін.

Основною відмінністю рівня НО-3 від рівня НО-2 є необхідність визначення ролей для звичайних користувачів.

А.2.5 Цілісність комплексу засобів захисту

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може

вивести тільки адміністратор.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Для рівня НЦ-3 необхідно, щоб КЗЗ забезпечував керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ. Дана вимога є другою функціональною вимогою до реалізації диспетчера доступу.

Необхідною умовою для реалізації рівня НЦ-1 даної послуги є реалізація рівнів НО-1 послуги розподіл обов'язків і НР-1 послуги реєстрація, оскільки КЗЗ повинен мати можливість ставити до відома адміністратора про факти порушення своєї цілісності.

А.2.6 Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача, в процесі запуску або штатної роботи.

Необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків.

А.2.7 Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

Реалізація рівня НВ-2 даної послуги дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення.

Реалізація рівня НВ-3 даної послуги дозволяє виключити можливість деяких видів внутрішнього шахрайства.

А.2.8 Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Найширше для реалізації даної послуги, як і послуги автентифікації одержувача, використовується цифровий підпис, оскільки використання несиметричних криптоалгоритмів (на відміну від симетричних) дозволяє забезпечити захист від внутрішнього шахрайства і автентифікацію за взаємної недовіри сторін.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація.

А.2.9 Автентифікація одержувача

Ця послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація.

Додаток Б

Гарантії і процес оцінки

В процесі оцінки КС розглядаються вимоги двох видів:

вимоги до функцій (послуг) забезпечення безпеки;

вимоги до рівня гарантій.

Виконання вимог першого виду забезпечується Розробником в процесі проектування (розробки) і перевіряється Експертною комісією в процесі оцінки. Виконання вимог другого виду забезпечується як діями Розробника, проте вже на всіх стадіях життєвого циклу КС, так і спільними діями Розробника і Експертної комісії в процесі оцінки. Наведені в критеріях гарантій вимоги регламентують передусім дії Розробника. Дії Експертної комісії регламентуються іншими документами.

Більшість з вимог критеріїв гарантій являють собою конкретизацію вимог щодо створення КЗЗ КС стандартів серії ДСТУ ISO 9000 і для їх викладення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95).

Перевірка виконання Розробником вимог критеріїв гарантій вимагає активної роботи Експертної комісії не тільки на етапі оцінки, але, можливо, і на більш ранніх етапах. Якщо використовувані Розробником процедури і методики (наприклад, супроводження проекту) відрізняються від стандартних чи загальноприйнятих, то вони вимагають перевірки і затвердження Експертною комісією. Чим вищий припустимий рівень гарантій, тим вища складність використовуваних процедур і методик і, отже, тим вищий рівень зусиль, які необхідно докласти Експертній комісії, що зумовлює в свою чергу необхідність більш тісної взаємодії Розробника з Експертною комісією, починаючи з найбільш ранніх етапів проектування.

В залежності від конкретної КС та інших умов Експертна комісія має право конкретизувати і поглиблювати певні вимоги критеріїв гарантій.

Б.1 Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки і більшою мірою відносяться до архітектури ПЗ. Додержання цих вимог забезпечується Розробником на стадіях проектування КЗЗ. Передусім, вимоги до архітектури покликані забезпечити структурованість КЗЗ відповідно до принципів “хорошого" проектування ПЗ (модульність, інкапсуляція і приховування даних).

Для самих низьких рівнів критеріїв гарантій від Розробника вимагається просто описати складові компоненти КЗЗ та їх призначення.

Для більш високих (проміжних) рівнів вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, критичних для безпеки. Внутрішні деталі і дані, використовувані всередині кожного модуля, повинні бути приховані від усіх зовнішніх об'єктів. Послуги КЗЗ повинні бути доступні тільки через зовнішній документований інтерфейс.

Для самих верхніх рівнів Розробник під час проектування ПЗ повинен зосередити зусилля на зменшенні обсягу КЗЗ до мінімального набору компонентів. Мінімізація обсягу є однією з вимог концепції диспетчера доступу і дозволяє виділити у складі КЗЗ ядро захисту.

Б.2 Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Процес розробки. Від Розробника вимагається визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги (вимоги, що повинні бути виконані раніше, ніж можна приступати до наступного етапу).

Крім того, повинні бути документовані стандарти, які використовувались під час розробки ПЗ. Використовувані мови програмування і компілятори мають відповідати вимогам національних, міждержавних або міжнародних стандартів. В іншому випадку слід надати повне визначення і опис мови, яка використовувалась. Додатково має бути документовано використання залежних від реалізації або апаратури опцій мови програмування.

Для більш високих рівнів гарантій вимоги до середовища розробки включають вимоги необхідності документування використовуваних методик фізичної, технічної, організаційної і кадрової безпеки.

Керування конфігурацією. Керування конфігурацією є необхідною і невід'ємною частиною будь-якої спроби розробки, а особливо захищених КС. Додержання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість Експертної комісії в тому, що Розробник може повністю керувати конфігурацією оцінюваної КС.

Розробник повинен розробити, запровадити і підтримувати в дієздатному стані документовані методики керування конфігурацією КС на всіх стадіях її життєвого циклу. При цьому Розробник може розробити і використати систему керування конфігурацією, що найкраще відображає і складність КС, і розміри організації Розробника. Критерії керування, можливе використання засобів автоматизації і належний рівень формалізації процедур і перевірок визначаються Розробником (і підтверджуються Експертною комісією) таким чином, щоб бути настільки сумісним з іншими компонентами середовища розробки, наскільки це можливо. Важливо, щоб усі процедури, ролі і відповідальність всього персоналу, задіяного в керуванні конфігурацією, були чітко визначені і документовані.

Система керування конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації, регулювання конфігурації, облік стану і перевірка якості конфігурації

Визначення конфігурації КС повинна ідентифікуватися в термінах своєї конфігурації: апаратне забезпечення, програмне забезпечення, програми ПЗП і документація на КС (наприклад, функціональні специфікації, технічний і робочий проекти, документація з тестування). Кожний елемент конфігурації одержує унікальне і значиме ім'я (ідентифікатор), під яким він існує в КС протягом всього її життєвого циклу. Повинні використовуватися загальні для всього проекту угоди щодо позначення, маркірування, нумерації і каталогізації елементів конфігурації Особливу увагу слід приділяти угодам щодо ПЗ (наприклад, для визначення того, є елемент вихідним чи об'єктним кодом).

Розмір елементів конфігурації може варіюватися відповідно до їх складності та очікуваної частоти зміни. Шляхом ретельного вибору розміру кожного елемента конфігурації система керування конфігурацією може краще ізолювати ті елементи, що змінюються частіше від тих, що змінюються рідше, ізолювати ті елементи, що є критичними для безпеки від тих, що не є такими, і групувати окремі малі елементи КС в єдиний великий елемент конфігурації для зменшення загального числа елементів конфігурації Ефективність контролю за змінами залежить від вдалого виділення елементів конфігурації: має досягатись

рівновага між керуванням великим числом малих елементів конфігурації і групуванням надто великого числа елементів КС в один елемент конфігурації

Регулювання конфігурації Керування (контроль за) внесенням будь-яких змін до КС є основною функцією системи керування конфігурацією Керування внесенням змін до конфігурації КС слід здійснювати протягом всього життєвого циклу КС. Процес внесення змін і набір використовуваних процедур мають бути визначені і документовані. Необхідно мати відповідальних осіб, роль і відповідальність яких має бути документована, які відповідали б за оцінку і затвердження запропонованих змін і безпосередньо за їх внесення. Це дозволяє гарантувати, що в разі необхідності елементи конфігурації можуть бути зафіксовані в певному стані і що ефекти від пропонованих змін будуть враховані раніше, ніж будуть затверджені дані зміни.

Облік стану. Завдання керування конфігурацією щодо обліку стану включає в себе фіксування інформації за статусом кожного елемента конфігурації Вона включає і вихідне визначення елемента, і будь-які зміни, внесені до елемента (наприклад, поширення, усунення помилок) протягом всього життєвого циклу. При збереженні записів за кожним елементом конфігурації поточний стан (статус) кожного елемента може бути доступним зацікавленому персоналу, а також можуть бути одержані історичні дані для використання в процесі перевірки конфігурації

Перевірка якості конфігурації Контроль за конфігурацією здійснюється шляхом взаємозв'язаних переглядів і перевірок інформації за станом всіх елементів конфігурації з метою одержання впевненості, що система керування конфігурацією працює належним чином. Контроль за конфігурацією робить можливим наступну адаптацію і настроювання процесу керування конфігурацією відповідно до умов, що змінюються (вхідними вимогами). Перегляди і перевірки також дають гарантію того, що стандарти, політика і процедури, прийняті в організації, присутні і в системі керування конфігурацією

Відповідно до Критеріїв система керування конфігурацією включає в себе технічні та організаційні заходи. Система керування конфігурацією повинна охоплювати розробку і супроводження програмного, апаратного, програмно-апаратного забезпечення, розробку документації, тестів і т.ін.

Для найнижчих рівнів критеріїв гарантій у Розробника має бути базова система керування конфігурацією, що дозволяє ідентифікувати оцінювану КС, керувати внесенням змін і вести архів цих змін. Система керування конфігурацією повинна включати технічні або організаційні документовані методики керування програмним, апаратним, програмно-апаратним забезпеченням, опрацюванням документації і тестів в необхідному обсязі.

Для більш високих рівнів критеріїв гарантій система керування конфігурацією повинна додатково мати можливість генерувати версію КЗЗ із вихідного коду і відзначати будь-які відмінності. Частиною системи мають бути засоби генерації звітів про помилки та інші проблеми, а також про їх усунення. Для даних рівнів система керування конфігурацією повинна використовувати засоби автоматизації та організаційні процедури, що їх доповнюють.

Для найбільш високих рівнів критеріїв гарантій система керування конфігурацією повинна додатково забезпечувати керування всіма засобами (наприклад, мовами програмування, компіляторами, бібліотеками часу виконання і т. ін.), які використовувались в процесі розробки КС.

Б.3 Послідовність розробки

Вимоги до процесу проектування забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним

вимогам (політиці безпеки).

Рівні деталізації. Вимоги до гарантій передбачають наявність чотирьох основних рівнів деталізації КС у процесі її створення: функціональна специфікація, проект архітектури, детальний проект, реалізація. Експертна комісія виконує аналіз для визначення коректності опису КС для кожного рівня деталізації і його відповідності опису попереднього рівня. Для кожної конкретної КС Експертна комісія і Розробник можуть спільно визначити необхідні рівні деталізації процесу розробки, які можна розглядати як функціональну специфікацію, проект архітектури і детальний проект. В документах, в яких наведені описи для кожного рівня деталізації, можуть використовуватись посилання на інші документи.

Стиль специфікації. В залежності від рівня гарантій і рівня деталізації передбачається можливість використання трьох способів (стилів) специфікації: неформалізований, частково формалізований і формалізований Неоднозначність специфікацій зменшується з використанням більш високого рівня формалізації.

Неформалізована специфікація має стиль текстового документа мовою повсякденного спілкування (російська, українська). Для неформалізованої специфікації вимагається представити визначення термінів, що використовуються в контексті, які відрізняються від звичайних, що використовуються у повсякденній мові.

Частково формалізована специфікація складається мовою з обмеженим синтаксисом і доповнюється поясненнями, написаними мовою повсякденного спілкування. Мова з обмеженим синтаксисом може являти собою повсякденну мову з жорсткою структурою речення і ключовими словами, що мають спеціальне значення, або бути діаграматичною (наприклад, діаграми потоків даних, станів або переходу). Для побудови частково формалізованої специфікації як на базі діаграм, так і на базі мови повсякденного спілкування, необхідно сформулювати набір угод, що визначають обмеження синтаксису.

Формалізовані специфікації мають представлення, яке базується на добре встановлених математичних концепціях, і супроводжуються поясненнями звичайною мовою. Ці математичні концепції використовуються для визначення синтаксису і семантики подань і несуперечливих правил доказу, які підтримуються логічними посиланнями. Властивості, критичні для безпеки, повинні виражатися мовою формалізованої специфікації. Формалізовані представлення повинні дозволяти описати і ефект (результат) виконання функції, і всі зв'язані з нею виняткові або помилкові умови. Якщо використовуються ієрархічні специфікації, то необхідно показати, що кожний рівень включає властивості, встановлені для попереднього рівня.

Вимоги до відповідності специфікацій рівня. Критерії гарантій включають вимоги до відповідності специфікацій рівня деталізації. Рівень зусиль, необхідних для досягнення такої відповідності, зростає разом з рівнем гарантій. Для його характеристики використовують терміни "показати", “продемонструвати" або "довести".

Якщо від Розробника вимагається показати повну відповідність між представленнями КС, це означає, що є необхідністю наявність відповідності тільки між основними елементами кожної специфікації. Прикладом може бути використання таблиці, елементи якої відображають відповідність, або використання належного представлення діаграми проекту.

Якщо від Розробника вимагається продемонструвати повну відповідність між представленнями КС, то вимагається наявність відповідності між більш дрібними елементами кожної специфікації. Демонстрація відповідності виконується на основі аналізу з використанням структурованого наукового підходу, що дає переконливі аргументи на користь того, що існує повна відповідність між елементами двох специфікацій.

Якщо від Розробника вимагається довести повну відповідність між представленнями КС, то необхідним є наявність відповідності між ще більш дрібними елементами кожної

специфікації. Відповідність між елементами має бути виражена формально.

Функціональні специфікації. Функціональні специфікації повинні описувати, які послуги надає КС у разі мінімуму або повної відсутності інформації про те, як вони представлені. Послуги безпеки описуються у формі політики безпеки і моделі політики безпеки.

Політика безпеки описує КС як набір послуг безпеки. Кожна послуга описується відповідно до вимог функціональних критеріїв для певного рівня даної послуги і з урахуванням необхідних умов. Для всіх рівнів гарантій політика безпеки подається у стилі неформалізованої специфікації і показується її відповідність більш деталізованій специфікації. Фактично, політика безпеки може бути визначена в технічному завданні на КС.

Модель політики безпеки дозволяє точніше виразити вимоги політики безпеки. Стиль специфікації моделі політики безпеки варіюється залежно від рівнів гарантій від неформалізованого до формалізованого. Для всіх рівнів гарантій показується відповідність моделі політики безпеки більш деталізованій специфікації.

Проект архітектури. Проект архітектури є старшим або верхнім рівнем специфікації проекту, який відображає функціональну специфікацію в основні компоненти проекту КС. Для кожного з основних компонентів КС проект архітектури описує його призначення і функції, визначає послуги безпеки, що реалізуються ним. Взаємодія всіх компонентів також визначається на даному етапі. Ця взаємодія представляється на рівні зовнішніх інтерфейсів, потоків даних, керування і т. ін. Проект архітектури описує, яку функцію виконує кожний компонент. Опис того, як компонент виконує свої функції всередині, не вимагається.

Детальний проект. Детальний проект є нижнім і найбільш детальним рівнем специфікації, який поділяє проект архітектури на менші за обсягом проекти його компонент. Детальний проект повинен мати достатню міру деталізації, щоб дозволити почати реалізацію. Для кожного компонента детальний проект повинен містити опис його призначення і функцій. Має бути визначений порядок взаємодії всіх компонентів. Ця взаємодія представляється на рівні зовнішніх інтерфейсів потоків даних, керування і т. ін. Детальний проект описує і те, яку функцію виконує кожний компонент, і те, як він це робить, включаючи алгоритми і внутрішні інтерфейси. Для детального проекту допускається наявність деяких проміжних специфікацій, кожна з яких характеризується більшою рівнем деталізації порівняно з попередніми.

Реалізація. Реалізація є завершальним представленням КС, що складаються з програмного, програмно-апаратного і апаратного забезпечення. Кожний компонент реалізації повинен бути створений і документований відповідно до вимог процесу проектування. Інтерфейси та інші компоненти, що згадуються, повинні бути описані в документації. Для найбільш високих рівнів гарантій вимагається представлення обраних дільниць вихідного коду.

Б.4 Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціалізується замовником так, як це передбачається Розробником. Оцінка КС забезпечує гарантії того, що КС правильно реалізує політику безпеки і правильно функціонує, і будується на припущенні, що функціонування КС починається з безпечного стану. Дотримання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість, що це припущення є правильним для всіх оцінюваних КС.

По-перше, Розробник повинен гарантувати, що конфігурація, яка поставляється замовнику даної КС, є сертифікованою конфігурацією.

По-друге, під час постачання Розробник повинен забезпечити захист КС від несанкціонованої модифікації. Цей захист за своєю природою може бути технічний, організаційний або фізичний. Технічний захист може полягати, наприклад, у використанні шифрування або криптографічних контрольних сум, паролів, що відкривають доступ до критичного ПЗ, перевірок на відповідність ПЗ еталону і т. ін. Організаційний захист може полягати, наприклад, у перевірці конфігурації для досягнення впевненості в тому, що замовнику поставлена потрібна версія, для чого можуть застосовуватися процедури керування якістю, задіяні Розробником при пакуванні КС. Фізичний захист може полягати, наприклад, у використанні вакуумної упаковки компонент ПЗ і документації і використанні інших оболонок, що запобігають або фіксують спроби фізичного доступу.

По-третє, коли КС доставлена і її цілісність перевірена, замовнику необхідні інструкції з інсталяції і ініціалізації КС. Наведені вказівки повинні описувати всі параметри конфігурування і можливі обмеження.

Б.5 Документація

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються КС для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

У складі експлуатаційної документації Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ оцінюваної КС, настанови адміністратору щодо послуг безпеки і настанови користувачу щодо послуг безпеки. Зміст цих документів залежить від політики безпеки, що реалізується КС. Ніяких особливих вимог до назв, формату або структур документів дані критерії не ставлять.

Документація може бути загальною або в ній можуть бути явно виділені документи (розділи), призначені для адміністратора безпеки і для звичайного користувача. В будь-якому випадку наведеної в документації інформації повинно бути достатньо для того, щоб і адміністратор, і звичайні користувачі мали змогу виконувати свої функції.

Б.6 Випробування комплексу засобів захисту

Для демонстрації того, що КЗЗ оцінюваної КС піддавався випробуванням, і доказу повноти цих випробувань Розробник повинен надати Експертній комісії документально оформлені результати випробувань. При організації випробувань послуг безпеки і механізмів захисту і документуванні їх результатів треба керуватися вимогами ДСТУ 2853-94, ДСТУ 2851-94 та ін. Вимоги до випробувань визначають такі основні елементи планування і проведення випробувань Розробником: план випробувань, програма і методика випробувань і результати випробувань (журнал випробувань, звіт, протокол випробувань).

В плані випробувань повинна бути викладена стратегія випробувань Розробника. План повинен надавати детальний опис всіх тестованих частин КЗЗ. Сюди входять зовнішні інтерфейси КЗЗ, всі політики, привілеї, механізми послуг захисту і специфічних викликів системних функцій, бібліотечного ПЗ і т. ін. План має також відображати середовище випробувань, будь-які особливі умови, що створюються для проведення випробувань, і засоби випробувань. Повинні бути наведені аргументи на користь повноти тестового покриття.

Програма і методика випробувань повинна визначати процедури тестування кожного елемента, визначеного у плані випробувань (наприклад, системних викликів). Для кожного окремого тесту має бути докладно описано використання засобів випробувань, необхідне оточення і особливі умови. Рівень деталізації процедур випробувань має бути достатнім для

наступного повторення випробувань Експертною комісією. Розробник повинен також описати очікувані результати кожного тесту.

Інформація, що міститься в документах, які представляють результати випробувань, дозволяє Експертній комісії оцінити реальну ефективність і повноту проведених випробувань, їх відповідність плану, програмі і методиці, а також організувати проведення сертифікаційних випробувань.