НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

Департамент спеціальних телекомунікаційних систем
та захисту інформації Служби безпеки України

Київ 2002

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено

наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

від “ 13 ” грудня 2002 р. № 84

Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

НД ТЗІ 2.5-008-2002

ДСТСЗІ СБ України

Київ

Передмова

1 РОЗРОБЛЕНО і ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

2 ВВЕДЕНО ВПЕРШЕ

Зміст

Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

Чинний від 2002-12-20

1 Галузь використання

Цей документ визначає вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 і установлює згідно з визначеними НД ТЗІ 2.5-004 специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їх реалізації у комплексах засобів захисту інформації (стандартний функціональний профіль захищеності).

Мета цього документа – надання нормативно-методологічної бази під час розроблення комплексів засобів захисту від НСД до конфіденційної інформації, яка обробляється в АС класу 2, створення комплексної системи захисту інформації в установі (організації), проведення аналізу та оцінки захищеності інформації від несанкціонованого доступу в системах такого класу, а також рекомендацій для визначення необхідного функціонального профілю захищеності інформації в конкретній АС.

Цей НД ТЗІ призначений для суб'єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов'язана з обробкою в автоматизованих системах конфіденційної інформації, розробників комплексних систем захисту інформації в автоматизованих системах, для постачальників компонентів АС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності АС на відповідність вимогам ТЗІ.

Вимоги цього НД ТЗІ є обов'язковими для державних органів, Збройних Сил, інших військових формувань, МВС, Ради Міністрів Автономної республіки Крим та органів місцевого самоврядування, а також підприємств, установ та організацій усіх форм власності, в АС яких обробляється конфіденційна інформація, що є власністю держави. Для конфіденційної інформації, що не є власністю держави, вимоги даного нормативного документа суб'єкти господарської діяльності можуть використовувати на власний розсуд.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

Інструкція про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджена постановою Кабінету Міністрів України від 27 листопада 1998 р. №1893;

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

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

НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

3 Визначення

У цьому НД ТЗІ використовуються терміни й визначення, які відповідають встановленим НД ТЗІ 1.1-003.

Крім того, використовуються такі поняття.

Сильнозв’язані об’єкти - сукупність наборів даних, що характеризується наявністю мінімальної надлишковості і допускають їх оптимальне використання одним чи декількома процесами як одночасно, так і в різні проміжки часу і вимагають безумовного забезпечення цілісності цих наборів даних як сукупності.

Фактично сильнозв’язаними об’єктами можуть бути бази даних, що підтримуються стандартними для галузі системами управління, сукупності наборів даних, які генеруються й модифікуються будь-якими функціональними або системними процесами і кожний з наборів даних, які складають цю множину, не може самостійно оброблятися, зберігатися і передаватися.

Слабозв’язані об’єкти – відносно незалежні набори даних, що генеруються, модифікуються, зберігаються й обробляються в АС.

Фактично слабозв’язані об’єкти - це інформаційні структури, представлені у вигляді окремих файлів, що підтримуються штатними операційними системами робочих станцій та серверів, і кожний з них може оброблятися, зберігатися й передаватися як самостійний об’єкт.

Далі у тексті будуть використовуватися як синонімічні поняття “автоматизована система” та “автоматизована система класу 2”, а також “конфіденційна інформація” та “інформація, якій за правовим режимом присвоєно гриф ДСК”.

4 Позначення та скорочення

У цьому НД ТЗІ використовуються такі позначення й скорочення:
АС – автоматизована система;
ДСК – для службового користування;
ЕОМ – електронна обчислювальна машина, комп'ютер;
КЗЗ – комплекс засобів захисту;
КСЗІ – комплексна система захисту інформації;
НД ТЗІ – нормативний документ системи технічного захисту інформації;
НСД – несанкціонований доступ;
ПЗП – постійний запам’ятовуючий пристрій;
ПЕОМ – персональна електронна обчислювальна машина, персональний комп'ютер;
СЗІ - служба захисту інформації;
СКБД - система керування базами даних.

Позначення послуг безпеки згідно з НД ТЗІ 2.5-004:
ДВ-1 - ручне відновлення;
ДЗ-1 – модернізація;
ДР-1 - квоти;
ДС-1 - стійкість при обмежених відмовах;
КА-2 - базова адміністративна конфіденційність;
КД-2 - базова довірча конфіденційність;
КО-1 - повторне використання об'єктів;
НИ-2 - одиночна ідентифікація та автентифікація;
НК-1 - однонаправлений достовірний канал;
НО-2 - розподіл обов'язків адміністраторів;

НТ-2 - самотестування при старті;
НР-2 - захищений журнал;
НЦ-2 - КЗЗ з гарантованою цілісністю;
ЦА-1 – мінімальна адміністративна цілісність;
ЦА-2 – базова адміністративна цілісність;
ЦД-1 - мінімальна довірча цілісність;
ЦО-1 - обмежений відкат.

5 Загальні вимоги із захисту конфіденційної інформації

5.1 Засади щодо захисту конфіденційної інформації визначаються Законами України "Про інформацію" і "Про захист інформації в автоматизованих системах", іншими нормативно-правовими актами, виданими у відповідності з цими законами, а також "Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави".

5.2 Впровадження заходів із захисту інформації в конкретній АС не повинно суттєво погіршувати основних її характеристик стосовно продуктивності, надійності, сумісності, керованості, розширюваності, масштабованості тощо.

5.3 Обробка в автоматизованій системі конфіденційної інформації здійснюється з використанням захищеної технології.

Технологія обробки інформації є захищеною, якщо вона містить програмно-технічні засоби захисту та організаційні заходи, що забезпечують виконання загальних вимог із захисту інформації. Загальні вимоги передбачають:

- наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці; у разі необхідності можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремих категорій користувачів та іншими класифікаційними ознаками;
- наявність визначеного (створеного) відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації (далі - служба захисту в АС, СЗІ);
- створення комплексної системи захисту інформації (далі - КСЗІ), яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, спрямованих на забезпечення захисту інформації під час функціонування АС;
- розроблення плану захисту інформації в АС, зміст якого визначено в додатку до НД ТЗІ 1.4-001;
- наявність атестата відповідності КСЗІ в АС нормативним документам із захисту інформації;
- можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів та декількох класифікаційних рівнів інформації;
- обов'язковість реєстрації в АС усіх користувачів та їхніх дій щодо конфіденційної інформації;
- можливість надання користувачам тільки за умови службової необхідності санкціонованого та контрольованого доступу до конфіденційної інформації, що обробляється в АС;
- заборону несанкціонованої та неконтрольованої модифікації конфіденційної інформації в АС;
- здійснення СЗІ обліку вихідних даних, отриманих під час вирішення функціональних задач у формі віддрукованих документів, що містять конфіденційну інформацію, у відповідності з "Інструкцією про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави";

- заборону несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації в електронному вигляді;

- забезпечення СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації в електронному вигляді;

- можливість здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;

- забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

6 Характеристика типових умов функціонування та вимог із захисту інформації в автоматизованій системі класу 2

До АС класу 2, згідно з встановленою НД ТЗІ 2.5-005 класифікацією, відносяться автоматизовані системи, створені на базі локалізованого багатомашинного багатокористувачевого комплексу.

До складу АС класу 2 входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, користувачі АС та оброблювана інформація, у тому числі й технологія її оброблення. Під час забезпечення захисту інформації необхідно враховувати всі характеристики зазначених складових частин, які мають вплив на реалізацію політики безпеки.

Цей розділ визначає типові умови функціонування усіх компонентів, які входять до складу АС, вводить окремі обмеження та вимоги із захисту інформації до окремих компонентів АС, встановлює класифікацію технологій оброблення інформації. Для визначеної таким чином типової схеми функціонування АС установлюються можливі варіанти для вибору функціональних профілів захищеності інформації від НСД.

6.1 Характеристика обчислювальної системи

6.1.1 Метою створення автоматизованих систем класу 2 є надання будь-якому користувачеві, у відповідності із захищеною технологією обробки інформації, потенційної можливості доступу до інформаційних ресурсів усіх комп’ютерів, що об’єднані в обчислювальну мережу.

Узагальнена функціонально-логічна структура обчислювальної системи АС класу 2 включає:

- підсистему обробки інформації;
- підсистему взаємодії користувачів з АС;
- підсистему обміну даними.

6.1.2 Підсистема обробки інформації реалізує головну цільову функцію АС і складається із засобів обробки інформації, які утворюють основу інформаційно-обчислювальних ресурсів АС, що надаються користувачам (обчислення, пошук, зберігання та оброблення інформації). Принциповими її особливостями є багатофункціональність і можливість доступу до неї для будь-яких робочих станцій АС. Можливі обмеження визначаються тільки специфікою технологій, технічними й організаційними особливостями функціонування АС.

Як компоненти підсистеми можуть використовуватися універсальні високопродуктивні ЕОМ (у тому числі й ПЕОМ), спеціалізовані сервери обробки даних або надання послуг (сервери баз даних, друку тощо).

6.1.3 Підсистема взаємодії користувачів з АС забезпечує користувачам доступ до засобів підсистеми обробки інформації і подання отриманого від них ресурсу у вигляді результату обчислення, інформаційного масиву або графічного зображення у зручній та зрозумілій для користувача формі.

Компоненти підсистеми у функціональному відношенні є автономно замкненими та, як правило, не передбачається доступ до їх внутрішніх обчислювальних ресурсів зі сторони інших компонентів АС.

Як компоненти підсистеми можуть використовуватися ПЕОМ, що укомплектовані засобами введення та відображення інформації (робочі станції), дисплейні станції.

6.1.4 Підсистема обміну даними забезпечує взаємодію робочих станцій із засобами підсистеми обробки інформації, а також робочих станцій між собою на основі визначених правил, процедур обміну даними з реалізацією фаз встановлення, підтримання та завершення з'єднання. Підсистема забезпечує інформаційну взаємодію різних компонентів АС і об'єднує їх в єдине ціле як у структурному, так і у функціональному відношенні.

Підсистема обміну даними складається з пасивної мережі для обміну даними (кабельна мережа), активного мережевого обладнання (комутаторів, концентраторів, маршрутизаторів, шлюзів тощо), що об'єднує в єдине ціле пасивну мережу з обладнанням інших підсистем для забезпечення інформаційної взаємодії.

Як різновид підсистеми обміну даними можна розглядати структуровану кабельну систему – набір стандартних комутаційних елементів (кабелів, з'єднувачів, коннекторів, кросових панелей і спеціальних шаф та ін.), які дозволяють створювати регулярні структури передачі даних, що відносно легко розширюються.

6.1.5 Обчислювальні системи, за допомогою яких реалізуються підсистема обробки інформації та підсистема взаємодії користувачів з АС, укомплектовані:

- засобами обчислювальної техніки;
- периферійним обладнанням - пристроями друку, зберігання інформації тощо;
- комплексом програмного забезпечення обчислювальної системи;
- комплексом програмно-апаратних засобів захисту інформації.

У разі необхідності засоби обчислювальної техніки додатково можуть комплектуватися сумісними периферійними пристроями і відповідними модулями системного програмного забезпечення.

6.1.6 Комплекс програмного забезпечення обчислювальної системи складають:

- операційні системи серверів;
- операційні системи універсальних високопродуктивних ЕОМ;
- операційні системи робочих станцій;
- операційні системи, що забезпечують виконання мережевих функцій;
- програмні засоби, що підтримують реалізацію протоколів передачі даних обчислювальної мережі;
- програмні засоби активних компонентів мережі, що реалізують спеціальні алгоритми управління мережею;
- системи керування базами даних серверів, високопродуктивних універсальних ЕОМ, робочих станцій;
- програмні засоби забезпечення КЗЗ;
- функціональне програмне забезпечення.

6.1.7 Наведена функціонально-логічна структура АС може розглядатися як універсальна, в той час як фізична структура автоматизованої системи може мати значно більшу кількість модифікацій в залежності від цілей та завдань, які вона повинна вирішувати, способу розподілу функцій між окремими технічними засобами, видів та можливостей технічних засобів, що застосовуються, інших специфічних особливостей, які враховуються під час проектування конкретної обчислювальної мережі.

6.1.8 Типові адміністративні та організаційні вимоги до обчислювальної системи АС, умов її функціонування і забезпечення захисту інформації визначаються наступним.

6.1.8.1 Для АС в цілому та (або) для окремих (усіх) її компонентів у відповідності до вимог із захисту інформації від НСД повинен бути сформований перелік необхідних функціональних послуг захисту і визначено рівень гарантій їх реалізації.

6.1.8.2 Сервери, робочі станції, периферійні пристрої, інші технічні засоби обробки конфіденційної інформації повинні бути категорійовані згідно з вимогами нормативних документів із технічного захисту інформації, якщо це вимагається цими документами .

Засоби захисту інформації, інші технічні засоби та програмне забезпечення АС, що задіяні в КСЗІ, повинні мати підтвердження їхньої відповідності нормативним документам із захисту інформації (атестат, сертифікат відповідності, експертний висновок) і використовуватись згідно з вимогами, визначеними цими документами. Інших обмежень щодо типів технічних засобів обробки інформації та обладнання, видів програмного забезпечення не запроваджується.

6.1.8.3 Технічна та експлуатаційна документація на засоби захисту та обробки інформації, системне та функціональне програмне забезпечення належним чином класифіковані і для кожної категорії користувачів визначено перелік документації, до якої вони можуть отримати доступ. Доступ до документації фіксується у відповідних реєстрах. Порядок ведення реєстрів визначає СЗІ.

6.1.8.4 Сервери і робочі станції, що здійснюють зберігання та обробку конфіденційної інформації, повинні розташовуватися в приміщеннях, доступ до яких обслуговуючого персоналу та користувачів різних категорій здійснюється в порядку, що визначений СЗІ та затверджений керівником установи (організації).

6.1.8.5 Повинен здійснюватися контроль за доступом користувачів та обслуговуючого персоналу до робочих станцій, серверів АС і компонентів підсистеми обміну даними на всіх етапах життєвого циклу АС, а також періодичний контроль за цілісністю компонентів підсистеми обміну даними (з метою виявлення несанкціонованих відводів від компонентів підсистеми).

6.1.8.6 З метою забезпечення безперервного функціонування під час оброблення, зберігання та передачі конфіденційної інформації АС повинна мати можливість оперативного, без припинення її функціонування, проведення регламентного обслуговування, модернізації обчислювальної системи в цілому або окремих її компонентів. Порядок введення в експлуатацію нових компонентів, якщо це впливає на захист інформації в АС, визначається СЗІ.

6.1.8.7 Програмно-апаратні засоби захисту, що входять до складу КЗЗ, разом з організаційними заходами повинні забезпечувати СЗІ інформацією про користувачів, які працюють в системі, з локалізацією точки їхнього входу в систему і переліком технічних засобів і процесів, до яких вони отримали доступ.

6.1.8.8 Має бути визначено порядок організації та проведення СЗІ процедур періодичного та/або динамічного тестування комплексу засобів захисту інформації під час функціонування АС.

6.2 Характеристика фізичного середовища

6.2.1 У загальному випадку АС є територіально розосередженою системою, фізичне розташування компонентів якої можна представити як ієрархію, що включає:

- територію, на якій вона знаходиться;
- будівлю, яка знаходиться на території;
- окреме приміщення в межах будівлі.

6.2.2 АС комплектується необхідними засобами енергозабезпечення, сигналізації, зв'язку, допоміжними технічними засобами, іншими системами життєзабезпечення.

6.2.3 Типові адміністративні та організаційні вимоги щодо умов розміщення компонентів АС наступні.

6.2.3.1 Усі будівлі повинні бути розміщені в межах контрольованої території, що має пропускний та внутрішній режими, які відповідають режимним вимогам, що визначено чинними в організації нормативними та розпорядчими документами.

6.2.3.2 Контроль за доступом до приміщень, де знаходяться критичні з точки зору безпеки інформації компоненти АС, повинен забезпечуватись на всіх етапах її життєвого циклу. Порядок доступу до приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається СЗІ і затверджується керівником організації.

6.2.3.3 Для приміщень, в яких розташовані категорійовані компоненти АС, повинні бути вжиті відповідні заходи із захисту інформації від витоку технічними каналами, достатність і ефективність яких засвідчується актами атестації комплексів технічного захисту інформації для кожного такого приміщення.

6.3 Характеристика користувачів

6.3.1 За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування автоматизованих систем, особи, що мають доступ до АС, поділяються на наступні категорії:

- користувачі, яким надано повноваження розробляти й супроводжувати КСЗІ (адміністратор безпеки, співробітники СЗІ);
- користувачі, яким надано повноваження забезпечувати управління АС (адміністратори операційних систем, СКБД, мережевого обладнання, сервісів та ін.);
- користувачі, яким надано право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів;
- користувачі, яким надано право доступу тільки до відкритої інформації;
- технічний обслуговуючий персонал, що забезпечує належні умови функціонування АС;
- розробники та проектувальники апаратних засобів АС, що забезпечують її модернізацію та розвиток;
- розробники програмного забезпечення, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;
- постачальники обладнання і технічних засобів АС та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;
- технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища АС (електрики, технічний персонал з обслуговування будівель, ліній зв'язку тощо).

6.3.2 Усі користувачі та персонал АС повинні пройти підготовку щодо умов та правил використання технічних та програмних засобів, які застосовуються ними під час виконання своїх службових та функціональних обов'язків.

6.3.3 Доступ осіб всіх категорій, зазначених у п. 6.3.1, до конфіденційної інформації та її носіїв здійснюється на підставі дозволу, що надається наказом (розпорядженням) керівника організації. Дозвіл надається лише для виконання ними службових та функціональних обов'язків і на термін не більший, ніж той, що цими обов'язками передбачений.

Якщо в АС встановлено декілька класифікаційних рівнів конфіденційної інформації, кожній особі з допущених до роботи в АС мають бути визначені її повноваження щодо доступу до інформації певного класифікаційного рівня.

Дозвіл на доступ до конфіденційної інформації, що обробляється в АС, може надаватися лише користувачам. Як виключення, в окремих випадках (наприклад, аварії або інші непередбачені ситуації) дозвіл може надаватися іншим категоріям осіб на час ліквідації негативних наслідків і поновлення працездатності АС.

6.3.4 Персонал АС, розробники програмного забезпечення, розробники та проектувальники апаратних засобів, постачальники обладнання та фахівці, що здійснюють монтаж і обслуговування технічних засобів АС, і не мають дозволу на доступ до конфіденційної інформації, можуть мати доступ до програмних та апаратних засобів АС лише під час робіт із тестування й інсталяції програмного забезпечення, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їх доступу до даних конфіденційного характеру.

Зазначені категорії осіб повинні мати дозвіл на доступ тільки до конфіденційних відомостей, які містяться в програмній і технічній документації на АС або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

6.3.5 Порядок та механізми доступу до конфіденційної інформації та компонентів АС особами різних категорій розробляються СЗІ та затверджуються керівником організації.

6.3.6 Для організації управління доступом до конфіденційної інформації та компонентів АС необхідно:

- розробити та впровадити посадові інструкції користувачів та персоналу АС, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до АС;
- розробити та впровадити розпорядчі документи щодо правил перепусткового режиму на територію, в будівлі та приміщення, де розташована АС або її компоненти;
- визначити правила адміністрування окремих компонентів АС та процесів, використання ресурсів АС, а також забезпечити їх розмежування між різними категоріями адміністраторів;
- визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації;
- розробити та впровадити правила ідентифікації користувачів та осіб інших категорій, що мають доступ до АС.

6.4 Характеристика оброблюваної інформації

6.4.1 В АС обробляється конфіденційна інформація, володіти, користуватися чи розпоряджатися якою можуть окремі фізичні та/або юридичні особи, що мають доступ до неї у відповідності до правил, встановлених власником цієї інформації.

6.4.2 В АС може зберігатися і циркулювати відкрита інформація, яка не потребує захисту, або захист якої забезпечувати недоцільно, а також відкрита інформація, яка у відповідності до рішень її власника може потребувати захисту.

6.4.3 Конфіденційна й відкрита інформація можуть циркулювати та оброблятися в АС як різними процесами для кожної з категорій інформації, так і в межах одного процесу.

6.4.4 У загальному випадку в АС, безвідносно до ступеню обмеження доступу, інформація за рівнем інтеграції характеризується як:

- сукупність сильнозв'язаних об'єктів, що вимагають забезпечення своєї цілісності як сукупність;
- окремі слабозв'язані об'єкти, що мають широкий спектр способів свого подання, зберігання й передачі і вимагають забезпечення своєї цілісності кожний окремо.

Незалежно від способу подання об’єкти можуть бути структурованими або неструктурованими.

КСЗІ повинна реалізувати механізми, що забезпечують фізичну цілісність слабозв’язаних об’єктів, окремих складових сильнозв’язаних об’єктів, та підтримку логічної цілісності сильнозв’язаних об’єктів, що розосереджені в різних компонентах АС.

6.4.5 В АС присутня інформація, яка за часом існування та функціонування:

- є швидкозмінюваною з відносно коротким терміном її актуальності;
- має відносно тривалий час існування при високому ступені інтеграції і гарантуванні стану її незруйнованості за умови приналежності різним користувачам, в рамках сильно- або слабозв’язаних об’єктів.

КСЗІ повинна забезпечити доступність зазначених видів інформації у відповідності до особливостей процесів, що реалізують інформаційну модель конкретного фізичного об’єкта.

6.4.6 АС повинна забезпечувати підтримку окремих класів сукупностей сильнозв’язаних об’єктів стандартними для галузі системами керування базами даних, іншими функціональними чи системними процесами**,** які надають можливість здійснення паралельної обробки запитів і мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні таблиць, стовпців таблиці, записів таблиці.

АС повинна забезпечувати підтримку окремих класів сукупностей слабозв’язаних об’єктів стандартними для галузі операційними системами, які мають засоби, що в тій чи іншій мірі гарантують конфіденційність і цілісність інформації на рівні сукупності файлів, окремих файлів.

КСЗІ повинна гарантувати забезпечення цілісності, конфіденційності й доступності інформації, яка міститься в сильно- або слабозв’язаних об’єктах і має ступінь обмеження ДСК, згідно з визначеними у цьому документі вимогами до відповідного функціонального профілю захищеності.

6.5 Характеристика технологій оброблення інформації

6.5.1 Технологічні особливості функціонування АС класу 2 визначаються особливістю архітектури АС, способами застосування засобів обчислювальної техніки для виконання функцій збору, зберігання, оброблення, передавання та використання даних, вимогами до забезпечення властивостей інформації.

АС за структурою технічних та програмних засобів, що використовуються, може бути однорідною або гетерогенною структурою, мати різну топологію, що, відповідно, визначає різні підходи до забезпечення режимів циркулювання інформації в АС та способів доступу до неї.

6.5.2. КСЗІ повинна гарантувати користувачам стійкість автоматизованої системи до відмов та можливість проведення заміни окремих її компонентів з одночасним збереженням доступності до окремих компонентів АС або до АС в цілому.

6.5.3 В АС під час зберігання, оброблення та передавання конфіденційної інформації має забезпечуватися реєстрація дій користувачів способом, що дозволяє однозначно ідентифікувати користувача, адресу робочого місця, з якого здійснено доступ до об’єктів та час, протягом якого здійснювався доступ.

Засоби КЗЗ повинні забезпечити необхідний рівень цілісності та конфіденційності інформації в журналах реєстрації АС із можливим виділенням одного чи декількох серверів аудиту. Статистика роботи користувачів повинна бути спостереженою й доступною для адміністратора безпеки та/або співробітників СЗІ.

Журнали реєстрації системи повинні мати захист від несанкціонованого доступу, модифікації або руйнування.

6.5.4 У загальному випадку кожен користувач АС, що має дозвіл на роботу з конфіденційною інформацією, повинен мати можливість доступу до неї з будь-якої робочої станції автоматизованої системи.

У разі необхідності можуть вводитися обмеження щодо цього. За певних адміністративно-організаційних заходів та відповідних програмно-технічних рішень в АС, де одночасно циркулює інформація різних ступенів доступу, для роботи з інформацією, що має ступінь обмеження ДСК, можуть бути виділені окремі робочі станції. Робота інших робочих станцій, що не віднесені до переліку зазначених вище, повинна блокуватися за умови намагання користувачем будь-якої з категорій отримати доступ до конфіденційної інформації.

КСЗІ повинна забезпечити ідентифікацію користувача з визначенням точки його входу в АС, однозначно автентифікувати його і зареєструвати результат (успішний чи невдалий) цих подій у системному журналі. У випадку виявлення неавторизованого користувача повинна блокуватися можливість його роботи в АС.

6.5.5 КСЗІ повинна забезпечувати можливість двох режимів роботи користувача - із конфіденційною інформацією та з відкритою інформацією, гарантуючи в першому випадку доступ до відповідних об’єктів і процесів як з обмеженим доступом, так і до загальнодоступних, а в останньому - тільки до відкритої інформації й блокування будь-якого доступу до об’єктів і процесів з обмеженим доступу.

В обох режимах повинна забезпечуватися можливість визначення власниками об’єктів конкретних користувачів або їх групи, яким надається право мати доступ до цих об’єктів.

6.5.6 Конфіденційна інформація може зберігатися як на окремих виділених для цього (однорівневих) пристроях - серверах, робочих станціях, запам’ятовуючих пристроях та ін., так і на пристроях, що одночасно зберігають інформацію загального призначення (багаторівневих).

КСЗІ повинна забезпечити розмежування доступу користувачів різних категорій до інформації незалежно від способу її групування на однорівневих чи багаторівневих пристроях.

6.5.7 В АС повинна надаватись можливість формування робочих груп з використанням засобів адміністрування:

- за ознакою належності до того чи іншого компонента автоматизованої системи;
- відповідно до функцій, що необхідно виконувати конкретному користувачеві або групі користувачів.

Крайній випадок - вся АС призначена для забезпечення виконання усіх функцій усіма користувачами або групами користувачів.

Під час цього засоби адміністрування автоматизованої системи повинні забезпечувати контроль за можливостями встановлення, перегляду, модифікації стратегій управління (наприклад, реалізація управління віртуальними мережами), а засоби КЗЗ - гарантувати забезпечення контролю за цілісністю засобів адміністрування АС.

6.5.8 Копіювання об’єктів, що містять конфіденційну інформацію, із сервера на робочу станцію користувача дозволяється тільки у випадках, коли це передбачено технологічними процесами обробки інформації. КЗЗ повинен гарантувати, що зазначені процеси перед завершенням своєї роботи забезпечують копіювання цих об’єктів на сервер (якщо в цьому є потреба) і знищують їх на робочій станції способом, що унеможливлює відновлення або відтворення.

6.5.9 Під час обробки конфіденційної інформації повинна забезпечуватися можливість відміни окремої операції або певної їх послідовності до стану, що визначено користувачем або передбачено технологією реалізації певних процедур функціональним або системним програмним забезпеченням.

6.5.10 Виведення інформації у текстовому вигляді повинно здійснюватися на зареєстровані в установленому порядку паперові носії на спеціально виділених для цього

пристроях друку. КСЗІ повинна забезпечити контроль за процесом виконання роздруку інформації з фіксацією в системному журналі: імені користувача, об'єкта, робочої станції та часу, коли здійснюється роздрук. У разі необхідності можлива фіксація додаткової інформації, що характеризує процес роздруку і дозволяє його однозначно ідентифікувати.

6.5.11 Реалізація функцій копіювання інформації в електронному вигляді на зйомні носії інформації та створення резервних копій може здійснюватися тільки уповноваженими користувачами або за дозволом адміністратора безпеки.

КСЗІ повинна контролювати зазначені процеси шляхом реєстрації в журналі системи: імені користувача, об'єкта копіювання, робочої станції та часу, коли здійснюється процес копіювання або створення резервної копії. Допускається фіксація додаткової інформації, що характеризує ці процеси і дозволяє їх однозначно ідентифікувати.

6.5.12 Повинна бути реалізована можливість виявлення фактів несанкціонованого доступу до об'єктів та (або) процесів, що потенційно можуть призвести до виникнення загроз для інформації, і забезпечена фіксація в журналі системи: імені користувача, об'єкта та (або) процесу, до якого була спроба доступу, місця та часу, коли виникла загроза. Допускається фіксація додаткової інформації, яка дозволяє однозначно ідентифікувати процеси, що створили загрозу. КСЗІ повинна забезпечити блокування роботи робочих станцій, з яких була здійснена загроза інформації.

6.5.13 З урахуванням характеристик і особливостей подання оброблюваної інформації, особливостей процесів, що застосовуються для її оброблення, а також порядку роботи користувачів та вимог до забезпечення захисту інформації в АС класу 2 визначаються такі технології обробки інформації:

- обробка без активного діалогу зі сторони користувача слабозв'язаних об'єктів, що вимагають конфіденційності оброблюваної інформації, або конфіденційності й цілісності оброблюваної інформації;
- обробка без активного діалогу зі сторони користувача сильнозв'язаних об'єктів, що вимагають конфіденційності та цілісності оброблюваної інформації;
- обробка в активному діалоговому режимі зі сторони користувача слабозв'язаних об'єктів, що вимагають конфіденційності та доступності оброблюваної інформації, або конфіденційності та цілісності оброблюваної інформації;
- обробка в активному діалоговому режимі зі сторони користувача сильнозв'язаних об'єктів, що вимагають конфіденційності, цілісності та доступності оброблюваної інформації.

Визначені вище технології обробки інформації можуть бути застосовані як до АС в цілому, так і до окремих її компонентів або процесів, що використовуються в АС. Одночасно в АС можуть застосовуватись декілька технологій.

6.5.14 Обробка без активного діалогу зі сторони користувача слабозв'язаних об'єктів у загальному випадку представляє собою обробку окремого набору даних (або певної їх множини, але послідовно одне за одним) у фоновому режимі, який забезпечується операційними системами (за виключенням однокористувацьких однозадачних), що використовуються на робочих станціях та серверах автоматизованої системи.

Обробка без активного діалогу зі сторони користувача сильнозв'язаних об'єктів являє собою вирішення в фоновому режимі комплексів функціональних задач, які взаємодіють із базами даних, що підтримуються стандартними для галузі СКБД, а також реалізацію будь-яких інших процесів, які здійснюють одночасну обробку певної множини наборів даних, що мають між собою логічні зв'язки.

Обробка в активному діалоговому режимі зі сторони користувача слабозв'язаних об'єктів являє собою обробку окремого набору даних у режимі реального часу в діалозі між користувачем та прикладним процесом, що цю обробку здійснює (наприклад, створення та редагування текстів, і тому подібне).

Обробка в активному діалоговому режимі зі сторони користувача сильнозв'язаних об'єктів являє собою процеси реалізації в режимі реального часу взаємодії між користувачем та базою даних або сильнозв'язаними об'єктами (наприклад, будь-які інформаційні системи, що побудовані з використанням баз даних та СКБД і працюють у реальному часі; будь-які системи автоматизованого проектування тощо).

6.5.15 Перелік мінімально необхідних рівнів послуг безпеки, які реалізуються КЗЗ (функціональний профіль захищеності), вибирається в залежності від технологій обробки інформації, що застосовуються (відповідно до п. 6.5.13), та з урахуванням типових умов функціонування АС. Для АС класу 2 визначаються такі стандартні функціональні профілі захищеності оброблюваної інформації:

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності оброблюваної інформації:

2.К.3 = {КД-2, КА-2, КО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності та цілісності оброблюваної інформації:

2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності та доступності оброблюваної інформації:

2.КД.1а = {КД-2, КА-2, КО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації:

2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}.

Примітки: 1. У випадку, коли в АС класу 2 усі користувачі допущені до обробки конфіденційної інформації, реалізація послуги безпеки КО-1 необов'язкова.

У випадку, коли в АС класу 2 є користувачі, що допущені до обробки лише відкритої інформації, реалізація послуги безпеки КО-1 є обов'язковою.

2. Реалізація послуг безпеки, що базуються на довірчому принципі розмежування доступу (КД і ЦД), може здійснюватися у випадках:

- якщо політикою безпеки передбачено створення груп користувачів з однаковими повноваженнями щодо роботи з конфіденційною інформацією для розмежування доступу до об'єктів, що таку інформацію містять, у межах цих груп;
- для розмежування доступу до об'єктів, які потребують захисту, але не містять конфіденційної інформації.

У всіх інших випадках розмежування доступу здійснюється згідно з адміністративним принципом (послуги безпеки КА й ЦА).

3. Рівень ЦА-2 послуги безпеки "адміністративна цілісність" реалізується під час обробки конфіденційної інформації, що міститься в сильнозв'язаних об'єктах.

Для обробки конфіденційної інформації, що міститься в слабозв'язаних об'єктах, реалізується рівень послуги ЦА-1.

6.5.16 У разі необхідності для конкретної АС до визначених цим НД ТЗІ функціональних профілів захищеності можуть вводитися додаткові послуги безпеки, а також підвищуватись рівень будь-якої з наведених послуг.

За певних обставин в КСЗІ вимоги до політики реалізації окремих послуг безпеки можуть частково забезпечуватися організаційними або іншими заходами захисту. Якщо ці заходи у повному обсязі відповідають встановленим НД ТЗІ 2.5-004 специфікаціям для певного рівня послуги безпеки, то рівень такої послуги, що входить до визначених у п. 6.5.15 профілів захищеності, може бути знижений на відповідну величину.

Як виняток, послуга безпеки, що входить до визначених у п. 6.5.15 профілів захищеності, може не реалізовуватись, якщо її політика у повному обсязі відповідно до моделі захисту інформації спрямована на нейтралізацію лише несуттєвих загроз, визначених моделлю загроз для інформації в АС.

6.5.17 У випадках, коли в АС для окремих компонентів існують відмінності у характеристиках фізичного та інформаційного середовищ, середовища користувачів, технологій оброблення інформації, рекомендується визначати перелік мінімально необхідних рівнів послуг для кожного компонента окремо.

7 Політика реалізації послуг безпеки інформації в АС класу 2

Політика безпеки інформації в АС повинна поширюватися на об’єкти комп’ютерної системи, які безпосередньо чи опосередковано впливають на безпеку конфіденційної інформації.

До таких об’єктів належать:

- адміністратор безпеки та співробітники СЗІ;
- користувачі, яким надано повноваження інших адміністраторів;
- користувачі, яким надано право доступу до конфіденційної інформації або до інших видів інформації;
- слабо- та сильнозв’язані об’єкти, які містять конфіденційну інформацію або інші види інформації, що підлягають захисту;
- системне та функціональне програмне забезпечення, яке використовується в АС для оброблення інформації або для забезпечення КЗЗ;
- технологічна інформація КСЗІ (дані щодо персональних ідентифікаторів та паролів користувачів, їхніх повноважень та прав доступу до об’єктів, встановлених робочих параметрів окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);
- засоби адміністрування та управління обчислювальною системою АС та технологічна інформація, яка при цьому використовується;
- окремі периферійні пристрої, які задіяні у технологічному процесі обробки конфіденційної інформації;
- обчислювальні ресурси АС (наприклад, дисковий простір, тривалість сеансу користувача із засобами АС, час використання центрального процесора і т. ін.), безконтрольне використання яких або захоплення окремим користувачем може призвести до блокування роботи інших користувачів, компонентів АС або АС в цілому.

7.1 Вимоги до забезпечення конфіденційності оброблюваної інформації

7.1.1 Довірча конфіденційність

КЗЗ повинен реалізувати рівень КД-2.

Ця послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів.

Політика довірчої конфіденційності поширюється на: користувачів усіх категорій; об’єкти, які

містять конфіденційну інформацію, за умови визначення в АС груп користувачів з однаковими повноваженнями стосовно такої інформації і тільки в межах цих груп; об’єкти, які містять технологічну інформацію КСЗІ або управління АС і можуть використовуватися тільки користувачами, яким надано однакові повноваження відповідних адміністраторів, в межах свого домену; всі інші об’єкти, які підлягають захисту, але не належать до зазначених вище видів, - і забезпечує взаємодію зазначених об’єктів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується слабо- та сильнозв’язаних об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від цього об'єкта.

КЗЗ повинен реалізувати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу як власнику процесу, можливість визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

Ця послуга може реалізовуватися лише у разі необхідності та у доповнення до послуги КА-2, яка визначає основний механізм розмежування доступу до конфіденційної інформації в АС класу 2.

7.1.2 Адміністративна конфіденційність

КЗЗ повинен реалізувати рівень КА-2.

Ця послуга дозволяє адміністраторові безпеки (уповноваженим співробітникам СЗІ) та/або користувачам, яким надано повноваження інших адміністраторів, керувати потоками інформації від захищених об'єктів, що зберігаються й циркулюють в АС, до користувачів.

Політика адміністративної конфіденційності поширюється на: користувачів усіх категорій; сильно- та слабозв'язані об'єкти, що містять конфіденційну інформацію; системне та функціональне програмне забезпечення, що використовується для оброблення конфіденційної інформації; технологічну інформацію КСЗІ; технологічну інформацію щодо управління АС; доступ користувачів до окремих видів периферійних пристроїв (принтерів, накопичувачів на змінних машинних носіях інформації тощо), задіяних в обробці конфіденційної інформації, - і забезпечує взаємодію зазначених об’єктів. Стосовно об’єктів, для яких додатково в межах визначених доменів реалізується послуга КД-2, ця послуга застосовується для розмежування доступу до інформації користувачів на рівні доменів та для розмежування доступу до інформації користувачів різних доменів. Якщо послуга КД-2 не використовується, то політика адміністративної конфіденційності повинна поширюватися, крім зазначених вище, і на інші об’єкти, яких стосувалася послуга КД-2.

Розмежування доступу користувачів усіх категорій до захищеного об'єкта здійснюється засобами КЗЗ на підставі атрибутів доступу користувача й захищеного об’єкта. Призначення атрибутів доступу користувачам і процесам здійснюється адміністратором безпеки та/або уповноваженим на це співробітником СЗІ, на основі аналізу функціональних обов'язків окремих користувачів або груп користувачів та процесів і об'єктів, що відносяться до їх компетенції.

КЗЗ повинен надавати можливість користувачам, що мають відповідні повноваження - адміністраторам операційних систем, адміністраторам СКБД, адміністраторам мережевого обладнання, адміністраторам сервісів, - права доступу до

процесів, що забезпечують ведення системних процесів щодо адміністративного супроводження функціонування АС в цілому, окремих її компонентів та сервісів.

КЗЗ повинен надавати тільки адміністратору безпеки та/або уповноваженим співробітникам СЗІ права доступу до процесів, що забезпечують актуалізацію, супроводження та аналіз технологічної інформації КСЗІ.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки (уповноваженого співробітника СЗІ) або користувачів, яким надані повноваження інших адміністраторів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу визначати конкретних користувачів і/або групи користувачів, що мають право ініціювати процес, через керування належністю користувачів і процесів до відповідних доменів.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

7.1.3 Повторне використання об'єктів

КЗЗ повинен реалізувати рівень КО-1.

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

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів АС, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами АС та прикладними процесами, що виконуються в АС.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках, якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту (імпорту) конфіденційної інформації з (в) АС та створенні “твердих” копій тощо.

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, інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Вимога цієї послуги в повному обсязі поширюється і на розділювані одночасно декількома користувачами процеси.

7.2 Вимоги до забезпечення цілісності оброблюваної інформації

7.2.1 Довірча цілісність

КЗЗ повинен реалізувати рівень ЦД-1.

Ця послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь-якої категорії керувати потоками інформації в АС від інших користувачів до захищених об'єктів, що належать його домену.

Умови реалізації в АС послуги ЦД-1 повністю співпадають з умовами реалізації послуги КД-2, а політика довірчої цілісності стосується тих самих об’єктів, що і політика довірчої конфіденційності.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильнозв’язані об’єкти, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити

конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Ця послуга може реалізовуватися лише у разі необхідності та у доповнення до послуги ЦА-2 (ЦА-1), яка визначає в АС класу 2 основний механізм захисту від несанкціонованої модифікації об’єктів, які містять конфіденційну інформацію.

7.2.2 Адміністративна цілісність

Послуги адміністративної цілісності застосовуються для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяють адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, керувати потоками інформації в АС від користувачів до захищених об'єктів.

У залежності від технологій обробки інформації, які застосовуються в АС, КЗЗ повинен реалізувати рівень ЦА-1 або ЦА-2.

Якщо послуга ЦД-1 не використовується, то політика адміністративної цілісності повинна поширюватися також на всі об’єкти, яких стосувалася послуга ЦД-1, а не тільки на зазначені нижче у послугах ЦА-1 або ЦА-2.

7.2.2.1 Мінімальна адміністративна цілісність

Політика мінімальної адміністративної цілісності поширюється на: користувачів усіх категорій; слабозв'язані об'єкти, що містять конфіденційну інформацію; файлову систему (логічні диски, каталоги, підкаталоги, файли); функціональне програмне забезпечення, що використовується для оброблення конфіденційної інформації; технологічну інформацію КСЗІ; технологічну інформацію щодо управління АС - і забезпечує взаємодію зазначених об’єктів.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, а також визначати атрибути доступу користувача і захищеного об'єкта, на підставі яких КЗЗ буде здійснювати розмежування доступу користувачів різних категорій, надається тільки адміністратору безпеки та/або уповноваженому співробітнику СЗІ.

Розмежування доступу здійснюється на рівні надання (встановлення заборони) доступу користувачів до процесів, за допомогою яких можна модифікувати об’єкт.

КЗЗ повинен обробляти запити на зміну атрибутів доступу різних категорій користувачів тільки в тому випадку, якщо вони надходять від адміністратора безпеки або від уповноваженого співробітника СЗІ.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного захищеного об’єкта визначити домен, якому повинні належати ті користувачі і/або групи користувачів, що мають право модифікувати об’єкт. Тільки їм надається право включати й вилучати користувачів та об'єкти до/з конкретних доменів.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

7.2.2.2 Базова адміністративна цілісність

Політика базової адміністративної цілісності поширюється на: користувачів усіх категорій; сильнозв'язані об'єкти, що містять конфіденційну інформацію; призначене для оброблення цих об'єктів системне та функціональне програмне забезпечення, а також

створену в процесі обробки сильнозв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, - і забезпечують взаємодію зазначених об’єктів.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, а також визначати атрибути доступу процесу й захищеного об'єкта, на підставі яких КЗЗ буде здійснювати розмежування доступу, надається тільки адміністратору безпеки (уповноваженому співробітнику СЗІ).

Розмежування доступу здійснюється в межах певного процесу наданням користувачу права (встановленням заборони) за допомогою функціональних можливостей цього процесу модифікувати об’єкт.

КЗЗ повинен обробляти запити на зміну атрибутів доступу процесів і захищених об'єктів тільки в тому випадку, якщо вони надходять від адміністратора безпеки або від уповноваженого співробітника СЗІ.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного захищеного об'єкта (сукупності сильнозв'язаних об'єктів або певним чином виділеної підмножини їх, об'єкта, окремого стовпчика або окремого поля запису структурованого об'єкта) визначити домен, якому повинні належати ті процеси і/або групи процесів, що мають право модифікувати об’єкт. Тільки їм надається право включати й вилучати процеси та об'єкти до/з конкретних доменів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

7.2.3 Відкат

КЗЗ повинен реалізувати рівень ЦО-1.

Ця послуга забезпечує можливість відмінити окрему операцію або послідовність операцій й повернути захищений об'єкт, з яким маніпулював користувач, до попереднього наперед визначеного стану.

Політика обмеженого відкату поширюється на: користувачів усіх категорій; сильно- та слабозв’язані об’єкти, які містять конфіденційну інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об’єктів.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

Факт використання користувачем послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки НР-2.

7.3 Вимоги до забезпечення доступності оброблюваної інформації

7.3.1 Використання ресурсів

КЗЗ повинен реалізувати рівень ДР-1.

Ця послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, поширюється на: сильно- та слабозв'язані об'єкти, що містять інформацію будь-яких категорій; файлову систему (логічні диски, каталоги, підкаталоги тощо); системне та функціональне програмне забезпечення; технологічну інформацію щодо управління АС; окремі периферійні

пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.п.); обчислювальні ресурси АС - і забезпечує взаємодію зазначених об’єктів, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об’єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

7.3.2 Стійкість до відмов

КЗЗ повинен реалізувати рівень ДС-1.

Політика стійкості до відмов, що реалізується КЗЗ, поширюється на: сильно- та слабозв'язані об'єкти, що містять конфіденційну інформацію; файлову систему (логічні диски, каталоги, підкаталоги тощо); системне та функціональне програмне забезпечення; технологічну інформацію КСЗІ; технологічну інформацію щодо управління АС; окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.ін.) - і забезпечує взаємодію зазначених об’єктів. Послуга гарантує доступність АС в цілому або окремих її об'єктів і процесів після відмови якогось компонента АС.

Розробниками АС повинен бути виконаний аналіз можливих відмов компонентів АС. Адміністратор безпеки (служба захисту інформації) спільно з користувачами, яким надано повноваження інших адміністраторів, повинен проаналізувати стійкість окремих компонентів АС до відмов та визначити:

- множину компонентів АС, що є критичними стосовно забезпечення стійкого функціонування, та типи відмов цих компонентів, після яких АС здатна продовжувати функціонування;
- рівні відмов, у разі перевищення яких відмови призводять до погіршення характеристик обслуговування або недоступності послуг.

Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг і, в гіршому випадку, має виявлятися в погіршенні характеристик обслуговування користувачів.

КЗЗ повинен мати можливість реєстрації факту відмови будь-якого захищеного компонента АС та повідомлення щодо цієї події адміністратора безпеки та/або іншого адміністратора.

7.3.3 Гаряча заміна

КЗЗ повинен реалізувати рівень ДЗ-1.

Ця послуга дозволяє гарантувати доступність АС в цілому, окремих процесів й об'єктів, можливість використання інформації в процесі заміни окремих компонентів.

Політика модернізації, що реалізується КЗЗ, поширюється на: системне та функціональне програмне забезпечення; засоби захисту інформації та засоби управління КСЗІ; засоби адміністрування та управління обчислювальною системою АС; окремі периферійні пристрої (принтери, накопичувачі та змінні носії інформації і т.ін.), які задіяні для обробки конфіденційної інформації, - і забезпечує взаємодію зазначених об’єктів. Послуга гарантує, що модернізація АС (встановлення нової версії програмного або апаратного забезпечення, заміна захищеного компонента та ін.) не призведе до компрометації політики безпеки інформації в АС.

Політика проведення модернізації АС повинна надавати можливість провести модернізацію АС адміністратору безпеки, уповноваженим співробітникам СЗІ, іншим адміністраторам (адмністратору операційної системи, адміністратору баз даних,

адміністраторам сервісів та ін.), а також визначати для кожного з них повноваження та множину виконуваних ними допустимих операцій з метою модернізації АС.

Модернізація окремих компонентів АС не повинна призводити до необхідності проведення повторної інсталяції програмного забезпечення цих компонентів або до переривання виконання КЗЗ функцій захисту.

7.3.4 Відновлення після збоїв

КЗЗ повинен реалізувати рівень ДВ-1.

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на: системне та функціональне програмне забезпечення; засоби захисту інформації та засоби управління КСЗІ; засоби адміністрування та управління обчислювальною системою АС; окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації, - і забезпечує взаємодію зазначених об’єктів. Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування АС або окремих її компонентів, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція АС.

Після відмови АС або окремих її компонентів, або переривання обслуговування КЗЗ повинен перевести АС або окремі її компоненти до стану, із якого повернути до нормального функціонування може тільки адміністратор безпеки, інші адміністратори або співробітники СЗІ. Повинні бути визначені повноваження адміністратора безпеки, уповноважених співробітників СЗІ, інших адміністраторів (адміністратора операційної системи, адміністратора баз даних, адміністраторів сервісів та ін.) та множина виконуваних ними допустимих операцій з метою повернення АС у відомий захищений стан.

Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

7.4 Вимоги до забезпечення спостереженості оброблюваної інформації

7.4.1 Реєстрація

КЗЗ повинен реалізувати рівень НР-2.

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів, що існують в АС і стосуються захищених об’єктів.

Політика реєстрації поширюється на: користувачів усіх категорій; сильно- та слабозв'язані об'єкти, що містять конфіденційну інформацію; системне та функціональне програмне забезпечення, призначене для оброблення цих об'єктів; використання периферійного обладнання, задіяного для оброблення конфіденційної інформації; використання обчислювальних ресурсів АС, а також створену в процесі обробки сильно- та слабозв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, - і забезпечує взаємодію зазначених об’єктів.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

- вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;

- реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії із системи;

- зміна паролю користувачем будь-якої категорії;

- отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні конфіденційної інформації;

- виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку, що для роботи з інформацією із грифом ДСК не призначений;

- копіювання наборів даних із інформацією конфіденційного характеру на запам'ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання інформації конфіденційного характеру на запам'ятовуючих пристроях, які згідно з політикою безпеки для цього не призначені;

- виявлення і реєстрація фактів порушення цілісності КЗЗ;

- інші події, обов'язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

7.4.2 Достовірний канал

КЗЗ повинен реалізувати рівень НК-1.

Ця послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з АС не може бути модифікованою іншим користувачем або процесом. Послуга повинна визначати вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об'єктів.

Достовірний канал повинен використовуватися для початкової ідентифікації та автентифікації. Зв'язок із використанням даного каналу повинен ініціюватися виключно користувачем.

7.4.3 Цілісність комплексу засобів захисту

КЗЗ повинен реалізувати рівень НЦ-2.

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

Політика цілісності КЗЗ поширюється на: адміністратора безпеки та/або уповноважених співробітників СЗІ; окремі компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ; засоби захисту інформації, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об'єктів.

Політика реалізації послуги повинна гарантувати, що усі послуги безпеки доступні тільки через інтерфейс КЗЗ й усі запити в АС на доступ до захищених об'єктів контролюються КЗЗ. Якщо існують якісь обмеження, недотримання яких може призвести до надання послуг в обхід інтерфейсу КЗЗ і порушення політики безпеки, то такі обмеження повинні бути описані і задокументовані. Порядок дотримання користувачами цих обмежень визначається і контролюється адміністратором безпеки або уповноваженим співробітником СЗІ.

З метою захисту від зовнішніх впливів КЗЗ повинен визначати й підтримувати власний домен виконання, який є відмінним від доменів виконання усіх інших процесів, а також повинен мати механізми, що використовуються для реалізації розмежування доменів.

У власному домені повинен забезпечуватися захист від несанкціонованої модифікації механізмів КЗЗ і/або втрати керування КЗЗ.

Повинен бути визначений механізм контролю цілісності компонентів, що входять до складу КЗЗ. У разі виявлення порушення цілісності будь-якого зі своїх компонентів КЗЗ повинен повідомити щодо цього адміністратора безпеки або уповноваженого співробітника СЗІ і перевести АС до стану, в якому забороняється обробка конфіденційної інформації. Повернути АС до нормального функціонування може тільки адміністратор безпеки або уповноважений співробітник СЗІ після відновлення відповідності цього компонента КЗЗ еталону.

7.4.4 Самотестування

КЗЗ повинен реалізувати рівень НТ-2.

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій АС, що забезпечуються захистом.

Політика самотестування поширюється на: адміністратора безпеки та/або уповноважених співробітників СЗІ; компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ; засоби захисту інформації, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об’єктів.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в АС всіх критичних для безпеки конфіденційної інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки або уповноважених співробітників СЗІ.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, в якому забороняється обробка конфіденційної інформації взагалі, або до стану, в якому забороняється обробка конфіденційної інформації з використанням послуг безпеки, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки або уповноважений співробітник СЗІ після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

7.4.5 Ідентифікація та автентифікація

КЗЗ повинен реалізувати рівень НИ-2.

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до захищених об’єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на: усіх осіб, які намагаються одержати доступ до АС; користувачів усіх категорій, які намагаються одержати доступ до сильно- та слабозв'язаних об'єктів, що містять конфіденційну інформацію, призначену для оброблення цих об'єктів системного та функціонального програмного забезпечення, периферійного обладнання, задіяного для обробки конфіденційної інформації, створеної у процесі обробки сильно- та слабозв'язаних об'єктів, технологічної інформації КСЗІ та технологічної інформації щодо управління АС, - і забезпечує взаємодію зазначених об’єктів.

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені.

Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

7.4.6 Розподіл обов'язків

КЗЗ повинен реалізувати рівень НО-2.

Ця послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів із певними й притаманними для кожної з категорій функціями (ролі). Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів й обмеження авторитарності керування АС.

Політика розподілу обов’язків, що реалізується КЗЗ, поширюється на користувачів усіх категорій і повинна визначати щонайменше такі ролі:

- адміністратора безпеки;
- не менше, ніж одного іншого адміністратора (адміністратора баз даних, адміністратора мережевого обладнання, адміністратора сервісів та ін.);
- користувачів, яким надано право доступу до конфіденційної інформації.

Ролі адміністраторів можуть дублюватися уповноваженими на це користувачами. Кількість таких користувачів повинна бути мінімальною.

Функції, що притаманні кожній із зазначених категорій адміністраторів, повинні бути максимально розмежовані й мінімізовані таким чином, щоб обмежити їх коло тільки тими, що необхідні для виконання ними функціональних обов'язків, що передбачаються експлуатаційною документацією на відповідні компоненти АС.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального програмного забезпечення, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління АС та системного й функціонального програмного забезпечення, яке реалізує ці функції. Усім іншим користувачам доступ до цих об’єктів повинен бути заборонений.

Повинен заборонятися доступ адміністраторів до сильно- та слабозв'язаних об'єктів, що містять конфіденційну інформацію, за виключенням випадків, коли їхніми функціональними обов’язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки конфіденційної інформації.

КЗЗ повинен присвоїти користувачу атрибути, якими однозначно характеризується надана йому роль. Користувач може виступати в певній ролі тільки після того, як він виконає дії, що підтверджують прийняття ним цієї ролі.

8 Критерії гарантій

У відповідності до НД ТЗІ 2.5-004 критерії гарантій встановлюють вимоги до коректності реалізації послуг безпеки інформації, які забезпечуються КЗЗ, як складовою частиною КСЗІ в АС класу 2. Рівень реалізації послуг безпеки повинен бути не нижчий, ніж Г2.

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації, випробувань КЗЗ.

8.1 Архітектура

Програмне забезпечення, призначене для реалізації КЗЗ, повинне максимальним чином будуватися за модульним принципом.

Склад послуг безпеки, а також механізмів захисту, що реалізують кожну з послуг, визначається політикою безпеки інформації в АС і повинен відповідати її вимогам. Якщо не всі вимоги політики безпеки реалізуються КЗЗ, то вони повинні підтримуватися організаційними та іншими заходами захисту КСЗІ. У складі КЗЗ не повинні міститися послуги та використовуватися засоби, які мають не передбачені політикою безпеки функції. Використання таких засобів можливе за умови вилучення цих функцій або гарантування неможливості їх активізації.

Мають бути описані особливості архітектури компонентів КСЗІ та їх призначення. Стиль опису – неформалізований, вимоги щодо детального опису не висуваються.

8.2 Середовище розробки

Мають бути визначені всі стадії та етапи життєвого циклу АС, а для кожної стадії та етапу – перелік і обсяги необхідних робіт та порядок їх виконання. Якщо для якихось робіт вимагається створення особливих умов – це повинно бути визначено окремо. Всі стадії та етапи робіт повинні бути задокументовані. Види та зміст документів встановлено державними стандартами.

На всіх стадіях життєвого циклу повинні існувати процедури керування конфігурацією АС. Ці процедури повинні визначати технологію відслідковування та внесення змін в апаратне та програмне забезпечення КСЗІ, тестове покриття і документацію та гарантувати, що без дотримання цієї технології ніякі зміни не можуть бути внесені. Технологія відслідковування та внесення змін повинна гарантувати постійну відповідність між документацією й реалізацією поточної версії КЗЗ (інших компонентів КСЗІ).

8.3 Послідовність розробки

Для всіх стадій життєвого циклу АС повинні бути розроблені функціональні специфікації КСЗІ.

На підготовчому етапі створення КСЗІ має бути виконане обстеження середовищ функціонування АС, в результаті якого визначаються об’єкти захисту, здійснюється класифікація інформації та розробляється модель загроз для інформації й концепція політики безпеки інформації в АС. На підставі цих даних мають бути сформульовані функціональні специфікації вимог із захисту інформації в АС. Ці специфікації мають бути викладені в окремому розділі технічного завдання на створення АС або в окремому технічному завданні на створення КСЗІ.

Функціональні специфікації політики безпеки й моделі політики безпеки повинні, як мінімум, містити перелік й опис послуг безпеки, що надаються КЗЗ, а також правила розмежування доступу до захищених об’єктів АС.

Функціональні специфікації проекту архітектури КСЗІ повинні містити модель захисту (ескізний проект), де враховані всі суттєві загрози і для кожної з них визначено можливі варіанти її блокування (попередження) за допомогою КЗЗ або організаційними чи іншими заходами захисту. Якщо існує неоднозначність, повинні надаватися додаткові аргументи на користь вибору того чи іншого варіанту.

Функціональні специфікації детального проекту КСЗІ повинні містити принципи побудови, функціональні можливості, опис функціонування кожного механізму захисту та

взаємодії механізмів між собою у складі КЗЗ. Повинні бути розроблені документи, що регламентують використання засобів КЗЗ, а також організаційних та інших заходів захисту, які входять до КСЗІ. Як реалізація детального проекту може розглядатися технічний, робочий або техно-робочий проекти.

Функціональні специфікації всіх рівнів надаються в описовому (неформалізованому) виді.

Має бути підтверджена (показана) відповідність специфікацій КСЗІ всіх рівнів. Формальних доказів відповідності не вимагається. Таким підтвердженням може бути дотримання власником АС і суб'єктами господарювання, які беруть участь у створенні АС і КСЗІ, встановленого нормативними документами із захисту інформації порядку. Наприклад, підтвердженням відповідності між специфікаціями КСЗІ різних рівнів деталізації може бути узгодження в установленому порядку відповідних документів (моделі загроз, технічного завдання, технічного проекту тощо), висновок приймальної комісії щодо цього під час випробувань КСЗІ або окремих її компонентів, результати контролю за виконаними роботами на етапах створення АС з боку системи управління якістю виробництва, якщо у власника та розробників АС така система впроваджена та ін.

Окремі етапи робіт повинні бути задокументовані відповідно до вимог НД ТЗІ 1.4-001 у вигляді окремих розділів плану захисту інформації в АС або вимог інших нормативно-правових актів і нормативних документів із ТЗІ.

8.4 Середовище функціонування

Повинні існувати засоби інсталяції, генерації й запуску КЗЗ, які гарантують, що експлуатація АС починається з безпечного стану, а також, існувати документи (інструкції), які регламентують порядок керування цими процедурами. Якщо можливі різні варіанти конфігурації КЗЗ, то всі вони повинні бути описані в інструкціях.

Розробник апаратного, програмного, програмно-апаратного забезпечення КСЗІ повинен шляхом впровадження технічних, організаційних або фізичних заходів безпеки гарантувати, що забезпечення, яке ним поставляється, відповідає еталону.

8.5 Документація

Документація на КЗЗ у вигляді окремих документів або розділів інших документів повинна містити опис послуг безпеки, що реалізуються КЗЗ, а також настанови для різних категорій користувачів (адміністратора безпеки, адміністратора баз даних, адміністратора сервісів, звичайного користувача тощо) стосовно використання послуг безпеки.

Вимоги до складу й змісту документації на інші компоненти КСЗІ, організаційні або інші заходи захисту визначаються технічним завданням на створення КСЗІ.

8.6 Випробування

Випробування КЗЗ можуть проводитись як самостійно, так і у складі КСЗІ.

Для проведення випробувань розробник КЗЗ повинен підготувати програму й методику випробувань, розробити процедури (тести) випробувань усіх механізмів, що реалізують послуги безпеки.

Розробник КЗЗ повинен надати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування

Розробник КЗЗ 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 " .

Програма й методика випробувань КЗЗ, тестове покриття, результати випробувань КЗЗ входять до складу обов'язкового комплекту документації, яка надається організатору експертизи під час проведення державної експертизи КСЗІ в АС.