Загальні вимоги із захисту службової інформації

Засади щодо захисту службової інформації визначаються Законами України “Про інформацію” і “Про захист інформації в інформаційно-телекомунікаційних 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”.

Визначення

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.

Визначення

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.

Загальні вимоги із захисту службової інформації

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:

Загальні вимоги із захисту службової інформації

Загальні вимоги передбачають:

- наявність переліку службової 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 службової інформації;
- можливість надання користувачам тільки за умови службової необхідності санкціонованого та контрольованого доступу до службової інформації, що обробляється в АС;
- заборону несанкціонованої та неконтрольованої модифікації службової інформації в АС;

- здійснення СЗІ обліку вихідних даних, отриманих під час вирішення функціональних задач у формі віддрукованих документів, що містять службову інформацію, у відповідності з “Інструкцією про порядок обліку, зберігання й використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, що є власністю держави”;
- - заборону несанкціонованого копіювання, розмноження, розповсюдження службової інформації в електронному вигляді;
- - забезпечення СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням службову інформації в електронному вигляді;

- можливість здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;
- забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до службової інформації.

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

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.

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.

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.

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.

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.

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

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.

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 .

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.

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).

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. З метою забезпечення безперервного функціонування під час оброблення, зберігання та передачі службової 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.

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.

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

Характеристика фізичного середовища

У загальному випадку АС є територіально розсередженою 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.

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

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

- 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.
- 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.

Характеристика користувачів

- 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).

Для організації управління доступом до службової 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.

Характеристика оброблюваної інформації

- В АС обробляється службова 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.
- 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.
- Службова й відкрита інформація можуть циркулювати та оброблятися в АС як різними процесами для кожної з категорій інформації, так і в межах одного процесу.

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.

Характеристика технологій оброблення інформації

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.

Характеристика технологій оброблення інформації

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.

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.

Характеристика технологій оброблення 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.

КСЗІ повинна забезпечувати можливість двох режимів роботи користувача - із службовою 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.

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

  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.

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.

Перелік мінімально необхідних рівнів послуг безпеки, які реалізуються КЗЗ (функціональний профіль захищеності), вибирається в залежності від технологій обробки інформації, що застосовуються, 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}.

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 службової інформації.

До таких об’єктів належать:

- - адміністратор безпеки та співробітники СЗІ;
- - користувачі, яким надано повноваження інших адміністраторів;
- - користувачі, яким надано право доступу до службової інформації або до інших видів інформації;
- - слабо- та сильнозв’язані об’єкти, які містять службову 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 службової 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.

Вимоги до забезпечення конфіденційності оброблюваної інформації 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, 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.

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.

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 службову інформацію і ресурси яких поділяються між користувачами АС та прикладними процесами, що виконуються в АС.

Вимоги до забезпечення цілісності оброблюваної інформації

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.

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.

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 службову інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об’єктів.

Вимоги до забезпечення доступності оброблюваної інформації

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

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.

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 службової 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.

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 службової інформації.

Вимоги до забезпечення спостереженості оброблюваної інформації 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.

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 службової інформації;
- - виведення користувачем будь-якої категорії документа або службової інформації на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або службової інформації на пристрій друку, що для роботи зі службовою інформацією не призначений;
- - копіювання наборів даних із службової інформацією на запам'ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання службової інформації 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

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.

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.

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.

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.

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.