**Лекція 9. Послуги щодо забезпечення безпеки інформації.**

**Вступ.**

**Питання 1. Складові політики конфіденційності.**

**Питання 2. Складові політики цілісності.**

**Питання 3. Послуги доступності.**

**Питання 4. Послуги спостереженості.**

**Вступ.**

**Питання 1.**

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».

Послуги конфіденційності та цілісності, а також деякою мірою - використання ресурсів, є класичними послугами, що безпосередньо реалізують ту частину політики безпеки, яка складає ПРД.

Послуги конфіденційності забезпечують можливість керування потоками інформації від захищених пасивних об'єктів до об'єктів-користувачів з метою захисту пасивних об'єктів від несанкціонованого ознайомлення з їх умістом (компрометації).

Механізмами, що забезпечують реалізацію послуг конфіденційності, є механізми керування доступом, тобто надання можливості доступу до ресурсу згідно зі спеціально визначеними правилами.

Як основні схеми, на підставі яких може здійснюватися керування доступом, можуть використовуватися:

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

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

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

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

- ідентифікатори відповідних об'єктів;

- ідентифікатори груп відповідних об'єктів;

- інформацію про права доступу до пасивних об'єктів у вигляді міток доступу, списків керування доступом або списків повноважень;

- інформацію про права володіння пасивним об'єктом;

- інформацію про час спроби доступу;

- інформацію про маршрут запиту доступу в розподілених системах;

- інформацію про тривалість сеансу доступу до ресурсу.

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

**1.1. Довірча конфіденційність (КД)**

Послуга КД дозволяє звичайному користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Як правило, під об'єктами, що належать домену користувача, маються на увазі об'єкти, створені користувачем. Рівні послуги КД ранжируются на підставі повноти захисту і вибірковості керування.

Мінімальна довірча конфіденційність (КД-1).

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

Базова довірча конфіденційність (КД-2).

Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів.

Повна довірча конфіденційність (КД-3).

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

Абсолютна довірча конфіденційність (КД-4).

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

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

**1.2. Адміністративна конфіденційність (КА)**

Послуга КА дозволяє адміністратору керувати потоками інформації від захищених об'єктів до користувачів.

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

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

Мінімальна адміністративна конфіденційність (КА-1).

Політика адміністративної конфіденційності повинна визначати множину об'єктів ІТС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта.

Абсолютна адміністративна конфіденційність (КА-4).

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ІТС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача, процесу і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта.

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

**1.3. Повторне використання об'єктів (КО-1)**

Послуга КО-1 дозволяє забезпечити коректність повторного використання одних і тих же ресурсів. Послуга гарантує, що у випадку, якщо один і той же ресурс виділяється новому користувачу або процесу, він не містить інформації, що залишилася від попереднього користувача або процесу. Реалізація даної послуги дозволяє забезпечити захист від атак типу «збирання сміття».

Механізмами, що забезпечують реалізацію послуги, є механізми:

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

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

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

Залежно від реалізованих механізмів можна виконувати очищення об'єкта після його звільнення користувачем або безпосередньо перед його наданням наступному користувачу.

Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

**1.4. Аналіз прихованих каналів (КК)**

Послуга КК дозволяє виявити та вилучити потоки інформації, які не контролюються іншими послугами безпеки. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Виявлення прихованих каналів (КК-1)

Всі приховані канали, які існують в апаратному і програмному забезпеченні повинні бути документовані. Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів. Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність.

Контроль прихованих каналів (КК-2)

КЗЗ, крім вище вказаних, повинен забезпечувати реєстрацію використання знайдених прихованих каналів.

Перекриття прихованих каналів (КК-3)

Всі знайдені під час аналізу приховані канали повинні бути усунені.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня КО-1 послуги «повторне використання об'єктів», оскільки можливість одержання інформації, що залишилась в об'єкті від попереднього користувача, сама собою може розглядатися як прихований канал.

**1.5. Конфіденційність при обміні (КВ)**

Послуга КВ забезпечує захист даних від несанкціонованого ознайомлення під час їх обміну через незахищене середовище.

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

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

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

Функціонування механізмів, що забезпечують реалізацію послуги, може ґрунтуватися на одному з принципів забезпечення конфіденційності таких шляхом:

- керування маршрутом передачі пасивних об'єктів з метою унеможливлення несанкціонованого ознайомлення з їх умістом;

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

- заповнення трафіка методом доповнення хибних даних;

- заповнення трафіка методом генерації хибних повідомлень;

- використання змінного надання даних;

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

- організації прихованого каналу передачі усередині іншого відкритого каналу (принцип стеганографії).

Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Мінімальна конфіденційність при обміні (КВ-1).

КЗЗ забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Базова конфіденційність при обміні (КВ-2).

КЗЗ дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Повна конфіденційність при обміні (КВ-3).

КЗЗ дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

Абсолютна конфіденційність при обміні (КВ-4).

КЗЗ дозволяє забезпечити захист від компрометації за рахунок аналізу трафіку і від витоку інформації прихованими каналах обміну, що існують. Для реалізації даного рівня від розробника вимагається виконання аналізу прихованих каналів.

**Питання 2**.

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

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

**2.1. Довірча цілісність (ЦД)**

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

Мінімальна довірча цілісність (ЦД-1)

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

Базова довірча цілісність (ЦД-2)

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

Повна довірча цілісність (ЦД-3)

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

Абсолютна довірча цілісність (ЦД-4)

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

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

**2.2. Адміністративна цілісність (ЦА)**

Послуга ЦА дозволяє адміністратору керувати потоками інформації від користувачів і процесів до захищених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт.

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

Мінімальна адміністративна цілісність (ЦА-1)

Реалізація послуги на даному рівні повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Абсолютна адміністративна цілісність (ЦА-4)

Реалізація послуги на даному рівні повинна відноситись до всіх об'єктів КС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів, які мають, а також тих, які не мають права ініціювати процес.

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

**2.3. Відкат (ЦО)**

Послуга ЦО забезпечує можливість відмінити декілька операцій і повернути захищений об’єкт до попереднього стану. Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури та підтримувати цілісність баз даних, додатків, побудованих на транзакціях тощо.

Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі. Відміна операції не повинна приводити до видалення з журналу запису про операцію, яка пізніше була відмінена. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Обмежений відкат ЦО-1

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Повний відкат ЦО-2

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.

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

**2.4. Цілісність при обміні (ЦВ)**

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

Мінімальна цілісність при обміні (ЦВ-1)

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

Базова цілісність при обміні (ЦВ-2)

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

Повна цілісність при обміні (ЦВ-3)

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

**Питання 3.**

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

**3.1. Використання ресурсів (ДР)**

Послуга ДР забезпечує доступність ресурсів ІТС шляхом керування ресурсами, що виділяються користувачам.

Як приклади ресурсів, що спільно використовуються для збереження, оброблення або передачі пасивних об'єктів різних типів, можна навести:

- дисковий простір (для збереження об'єктів у вигляді файлів);

- табличний простір системи керування базами даних (для збереження об'єктів у вигляді записів таблиць системи керування базами даних);

- мережеві з'єднання (для передачі пасивних об'єктів);

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

Рівні даної послуги ранжируються на підставі повноти захисту і вибiрковості керування доступністю послуг ІТС.

Квоти (ДР-1)

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

Недопущення захоплення ресурсів (ДР-2)

Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

Пріоритетність використання ресурсів (ДР-3)

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

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

**3.2. Стійкість до відмов (ДС)**

Послуга ДС забезпечує доступність послуг і ресурсів ІТС після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість ІТС продовжувати функціонування залежно від кількості відмов і послуг, доступних після відмови.

Стійкість при обмежених відмовах (ДС-1)

КЗЗ повинний визначати множину компонентів ІТС, до яких вона відноситься, і типи їх відмов, після яких ІТС в змозі продовжувати функціонування. Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування.

Стійкість без погіршення характеристик обслуговування (ДС-3)

Політика стійкості до відмов повинна відноситися до всіх компонентів ІТС. Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування.

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

**3.3. Гаряча заміна (ДЗ)**

Послуга ДЗ гарантує доступність послуг і ресурсів ІТС в процесі заміни окремих компонентів. Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

Рівні даної послуги ранжируються на підставі повноти захисту.

Модернізація (ДЗ-1)

Політика КЗЗ повинна визначати політику проведення модернізації ІТС. Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію ІТС. Модернізація не повинна призводити до необхідності ще раз проводити інсталяцію ІТС або до переривання виконання КЗЗ функцій захисту

Гаряча заміна будь-якого компонента (ДЗ-3)

Політика КЗЗ повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування. Адміністратор повинен мати можливість замінити будь-який захищений компонент.

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

**3.4. Відновлення після збоїв (ДВ)**

Послуга ДВ забезпечує доступність послуг і ресурсів ІТС шляхом переведення у захищений стан після її відмови. Відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації КЗЗ може продукувати відновлення працездатності автоматично. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Ручне відновлення (ДВ-1)

Після відмови ІТС або переривання обслуговування КЗЗ повинен перевести її до стану, із якого повернути її до нормального функціонування може тільки адміністратор.

Вибіркове відновлення (ДВ-3)

Після будь-якої відмови ІТС або переривання обслуговування, що не призводить до необхідності заново інсталювати ІТС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути її до нормального функціонування. Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести ІТС до стану, з якого повернути її до нормального функціонування може тільки адміністратор.

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

**Питання 4.**

Для того, щоб ІТС могла бути оцінена на відповідність критеріям спостереженості, КЗЗ повинен забезпечити відповідальність користувача за свої дії та підтримку спроможності КЗЗ виконувати свої функції. Спостережність забезпечується в ІТС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

**4.1. Реєстрація (НР)**

Послуга НР забезпечує розпізнавання, фіксування та аналіз подій, пов'язаних з дотриманням політики безпеки інформації. Використання засобів перегляду та аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою адміністраторів.

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

- виявляти (реєструвати) факти виникнення подій;

- генерувати записи в журналі реєстрації;

- накопичувати і зберігати дані журналів реєстрації або передавати їх в інші системи.

Під подіями, що мають відношення до безпеки, слід розуміти події, пов'язані зі спробами або фактами певних дій, які стосуються виконання функціональними модулями, що входять до складу КЗЗ, операцій згідно з вимогами політики різних послуг безпеки.

Чіткого визначення поняття події, що має безпосереднє відношення до безпеки, не існує. Однак під такою подією слід розуміти факт звертання до КЗЗ, що реалізує будь-яку послугу безпеки, наприклад:

- надання доступу;

- відмова в доступі;

- виконання автентифікації;

- зміна атрибутів доступу;

- створення об'єкта;

- модифікація об'єкта;

- видалення об'єкта;

- використання привілеїв тощо.

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

Для забезпечення контролю реєстраційних подій використовуються такі підходи:

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

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

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

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

Для реалізації найбільш високих рівнів даної послуги необхідна наявність засобів аналізу журналу реєстрації. Засоби аналізу - це засоби, що виконують більш складну, ніж перегляд, оцінку журналу реєстрації з метою виявлення можливих порушень політики безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування, фільтрації за певними критеріями та інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати події, що реєструються.

Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності виявлення потенційних порушень.

Зовнішній аналіз (НР-1)

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Захищений журнал (НР-2)

КЗЗ повинен додатково забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Сигналізація про небезпеку (НР-3)

КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ІТС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

Детальна реєстрація (НР-4)

КЗЗ повинен додатково здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки.

Аналіз у реальному часі (НР-5)

КЗЗ повинен додатково здійснювати аналіз даних реєстрації у реальному часі.

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

**4.2. Ідентифікація і автентифікація (НИ)**

Послуга НИ дозволяє визначити та перевірити користувача, який намагається одержати доступ до ІТС. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем.

За результатами ідентифікації і автентифікації користувача КЗЗ, по-перше, приймає рішення про те, чи дозволено даному користувачу увійти в систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Функціонування механізмів автентифікації ґрунтується на одному з таких принципів:

1) «знання чогось» (наприклад, паролів або криптографічних ключів);

2) «володіння чимось» (карткою з магнітною смугою, смарт-карткою, переносним ідентифікатором тощо);

3) «притаманність невід'ємних характеристик» (рукописний підпис, відбиток пальця, голосові параметри, характеристики сітківки ока, динамічні характеристики при роботі з клавіатурою тощо).

Перший тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена простотою його повторення: достатньо просто обчислити або вгадати інформацію автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Основною перевагою другого типу автентифікації є складність або висока вартість дублювання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Реалізація третього типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для використання даного механізму є висока вартість пристроїв автентифікації. Крім того, використання цих достатньо дорогих засобів автентифікації не гарантує безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може стати непридатним для деяких застосувань.

Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Зовнішня ідентифікація і автентифікація (НИ-1)

Перш ніж дозволити будь-якому користувачу виконувати будь-які дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Одиночна ідентифікація і автентифікація (НИ-2)

КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Множинна ідентифікація і автентифікація (НИ-3)

КЗЗ повинен автентифікувати цього користувача з використанням захищених механізмів двох або більше типів різних типів автентифікації, наприклад, введеного з клавіатури пароля і зовнішнього ідентифікатора.

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

**4.3. Достовірний канал (НК)**

Послуга НК забезпечує гарантію взаємодії КЗЗ безпосередньо з користувачем, що унеможливлює будь-яке стороннє втручання в цю взаємодію. Зазначена можливість, ініційована користувачем, повинна забезпечувати захист від шкідливих програмних засобів типу «троянський кінь». Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Однонаправлений достовірний канал (НК-1)

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

Двонаправлений достовірний канал (НК-2)

Достовірний канал повинен використовуватися також у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ. Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача.

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

**4.4. Розподіл обов'язків (НО)**

Послуга НО дозволяє зменшити ймовірність неправильних дій користувачів і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Виділення адміністратора (НО-1)

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача та притаманні їм функції.

Розподіл обов'язків адміністраторів (НО-2)

Політика повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора (наприклад, системи). Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Ролі не обов’язково мають бути абсолютно взаємовиключними, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам тощо.

Розподіл обов'язків на підставі привілеїв (НО-3)

Політика додатково повинна визначати множину ролей користувачів.

**4.5. Цілісність КЗЗ (НЦ)**

Послуга НЦ визначає міру здатності КЗЗ захищати себе та керувати захищеними об'єктами. Жодна ІТС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу.

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

- порівняння із заздалегідь створеною еталонною копією;

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

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

- вироблення/перевірки електронного цифрового підпису.

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

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

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

КЗЗ з контролем цілісності (НЦ-1)

Рівень даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг. КЗЗ повинен мати можливість перевіряти свою цілісність і у разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

КЗЗ з гарантованою цілісністю (НЦ-2)

КЗЗ повинен підтримувати власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

КЗЗ з функціями диспетчера доступу (НЦ-3)

КЗЗ повинен забезпечити керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ. Дана вимога є другою функціональною вимогою до реалізації диспетчера доступу.

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

**4.6. Самотестування (НТ)**

Послуга НТ дозволяє КЗЗ перевірити та гарантувати правильність функціонування певної множини функцій ІТС. Рівні даної послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача, в процесі запуску або штатної роботи.

Самотестування за запитом (НТ-1)

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій за запитом користувача, що має відповідні повноваження.

Самотестування в реальному часі (НТ-3)

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій за запитом користувача, що має відповідні повноваження, а також при ініціалізації КЗЗ і в процесі штатного функціонування.

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

**4.7. Ідентифікація і автентифікація при обміні (НВ)**

Послуга НВ дозволяє встановити та перевірити ідентичність іншого КЗЗ у процесі взаємодії. Функціонування засобів, що забезпечують реалізацію послуги, повинно обов'язково передбачати виконання таких дій:

- одержання інформації автентифікації, необхідної для генерації/перевірки запитів автентифікації сторонами взаємодії (ініціатором і верифікатором);

- генерація і передача запитів автентифікації стороною-ініціатором;

- перевірка та оброблення запитів автентифікації стороною-верифікатором.

При цьому функціонування механізмів, що реалізують послугу, може ґрунтуватися на одному з таких принципів:

- знання загального секрету;

- підтвердження довіреною третьою стороною;

- контекст запиту автентифікації.

Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла (НВ-1)

КЗЗ дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

Автентифікація джерела даних (НВ-2)

КЗЗ дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення.

Автентифікація з підтвердженням (НВ-3)

КЗЗ дозволяє виключити можливість деяких видів внутрішнього шахрайства.

**4.8. Автентифікація відправника (НА)**

Послуга НА дозволяє однозначно встановити приналежність певного об'єкта певному користувачу. Функціонування засобів, що забезпечують реалізацію послуги, повинно обов'язково передбачати виконання таких дій:

- генерація підтверджень авторства (маркерів причетності), однозначно пов'язаних з переданими об'єктами (повідомленнями);

- передача і збереження підтверджень авторства (маркерів причетності);

- перевірка підтверджень авторства (маркерів причетності).

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

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

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

Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Базова автентифікація відправника (НА-1)

Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

Автентифікація відправника з підтвердженням (НА-2)

Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною.

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

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

**4.9. Автентифікація одержувача (НП)**

Послуга НП дозволяє однозначно установити факт одержання певного об'єкта певним користувачем. Функціонування засобів, що забезпечують реалізацію послуги, повинно обов'язково передбачати виконання таких дій:

- генерація підтверджень одержання (маркерів причетності), однозначно пов'язаних з отриманими об'єктами (повідомленнями);

- передача і збереження підтверджень одержання (маркерів причетності);

- перевірка підтверджень одержання (маркерів причетності).

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

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

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

Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Базова автентифікація отримувача (НП-1)

Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації.

Автентифікація отримувача з підтвердженням (НП-2)

Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта.

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

**Контрольні питання**

Які механізмами забезпечують реалізацію послуг конфіденційності?

На підставі чого може здійснюватися керування доступом?

Які є послуги конфіденційності без обміну даними?

Що дозволяє послуга «Довірча конфіденційність»?

Що дозволяє послуга «Адміністративна конфіденційність»?

Що дозволяє послуга «Повторне використання об'єктів»?

Що дозволяє послуга «Аналіз прихованих каналів»?

Що забезпечує послуга «Конфіденційність при обміні»?

Які є послуги цілісності?

Що дозволяє послуга «Довірча цілісність»?

Що дозволяє послуга «Адміністративна цілісність»?

Яку можливість забезпечує послуга «Відкат»?

Що забезпечує послуга «Цілісність при обміні»?

Які є послуги доступності?

Що забезпечує послуга «Використання ресурсів»?

Що забезпечує послуга «Стійкість до відмов»?

Що забезпечує послуга «Гаряча заміна»?

Що забезпечує послуга «Відновлення після збоїв»?

Які є послуги спостереженості без обміну даними?

Що забезпечує послуга «Реєстрація»?

Що дозволяє послуга «Ідентифікація і автентифікація»?

Що забезпечує послуга «Достовірний канал»?

Що дозволяє послуга «Розподіл обов'язків»?

Що визначає послуга «Цілісність КЗЗ»?

Що дозволяє КЗЗ послуга «Самотестування»?

Що дозволяє послуга «Ідентифікація і автентифікація при обміні»?

Що дозволяє послуга «Автентифікація відправника»?

Що дозволяє послуга «Автентифікація одержувача»?