Безпека операційних систем і комп'ютерних мереж

Лекція 5

Нормативні документи системи ТЗІ в Україні

НД ТЗІ з питань захисту інформації в КС від НСД

- Загальні положення із захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99)
- Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-003-99)
- Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99)
- Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5-005-99)
- Методичні вказівки по розробці технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (НД ТЗІ 3.7-001-99)
- Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000)

НД ТЗІ з питань захисту інформації в КС від НСД

- Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження і модернізації засобів технічного захисту інформації від несанкціонованого доступу. (НД ТЗІ 3.6-001-2000)
- Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 (НД ТЗІ 2.5-008-02)
- Вимоги до захисту інформації WEB–сторінки від несанкціонованого доступу (НД ТЗІ 2.5-010-03)
- Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003-05)
- Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу (НД ТЗІ 2.7-009-09)
- Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу (НД ТЗІ 2.7-010-09)

Термінологія в галузі захисту інформації в КС від НСД

~~Суб'єкт~~ → Об'єкт-користувач
Об'єкт-процес

Доступ:
користувач → процес → пасивний об'єкт

Керування доступом:

~~Дискреційне~~ - - - - → Довірче

~~Мандатне~~ - - - - → Адміністративне

Термінологія в галузі захисту інформації в КС від НСД

- Довірче керування доступом
  - користувачам дозволено керувати доступом до об’єктів свого домену (наприклад, на підставі права володіння об’єктами)
- Адміністративне керування доступом
  - керувати доступом до об’єктів дозволено лише спеціально уповноваженим користувачам (адміністраторам)

Критерії оцінки захищеності інформації в КС від НСД

- Критерії конфіденційності
- Критерії цілісності
- Критерії доступності
- Критерії спостережності
- Критерії гарантій

Функціональні критерії

Концепція функціонального профілю в НД ТЗІ

- Послуга (сервіс) безпеки
  - *Сукупність функцій, що забезпечують захист від певної загрози або від множини загроз*
  - Для кожної послуги запропонована окрема шкала оцінок, яка визначає рівень реалізації цієї послуги
- Функціональний профіль
  - *Перелік рівнів функціональних послуг, які реалізуються комп'ютерною системою*
  - Функціональний профіль оформлюється певним чином
    - зокрема, специфіковано порядок, у якому повинні бути названі послуги

Критерії конфіденційності

- Довірча конфіденційність (КД-1…4)
  - дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів
- Адміністративна конфіденційність (КА-1…4)
  - дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів
- Повторне використання об'єктів (КО-1)
  - дозволяє забезпечити коректність повторного використання розділюваних об'єктів, тобто таких, які почергово виділяються різним користувачам та/або процесам
  - гарантує, що коли розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від попереднього користувача або процесу
- Аналіз прихованих каналів (КК-1…3)
  - забезпечує виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами
- Конфіденційність при обміні (КВ-1…4)
  - забезпечує захист об'єктів від несанкціонованого ознайомлення з інформацією, яку вони містять, під час їх передавання через незахищене середовище

Критерії цілісності

- Довірча цілісність (ЦД-1…4)
  - дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену
- Адміністративна цілісність (ЦА-1…4)
  - дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів
- Відкат (ЦО-1...2)
  - забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього стану
- Цілісність при обміні (ЦВ-1…3)
  - забезпечує захист об'єктів від несанкціонованої модифікації інформації, яку вони містять, під час їх передавання через незахищене середовище

Критерії доступності

- Використання ресурсів (ДР-1…3)
  - забезпечує керування використанням користувачами послуг і ресурсів
- Стійкість до відмов (ДС-1…3)
  - гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента
- Гаряча заміна (ДЗ-1…3)
  - дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів
- Відновлення після збоїв (ДВ-1…3)
  - забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування

Критерії спостережності (1/2)

- Реєстрація (НР-1…5)
  - дозволяє контролювати небезпечні для КС дії шляхом реєстрації і аналізу подій, що мають відношення до безпеки
- Ідентифікація й автентифікація (НИ-1…3)
  - дозволяє КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС
- Достовірний канал (НК-1…2)
  - дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ
- Розподіл обов'язків (НО-1…3)
  - дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування
- Цілісність комплексу засобів захисту (НЦ-1…3)
  - визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами

Критерії спостережності (2/2)

- Самотестування (НТ-1…3)
  - дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС
- Ідентифікація й автентифікація при обміні (НВ-1…3)
  - дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію
- Автентифікація відправника (НА-1…2)
  - дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем
- Автентифікація одержувача (НП-1…2)
  - дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем

Критерії гарантій

- Архітектура
- Середовище розроблення:
  - процес розроблення
  - керування конфігурацією
- Послідовність розроблення:
  - функціональні специфікації (політика безпеки)
  - функціональні специфікації (модель політики безпеки)
  - проект архітектури
  - детальний проект
  - реалізація
- Середовище функціонування
- Документація
- Випробування комплексу засобів захисту

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

Обмеження на функціональний профіль

- Обов’язково має виконуватись послуга “Цілісність комплексу засобів захисту” (щонайменше, рівень НЦ-1)
- Мають бути задоволені усі вимоги специфікацій послуг щодо виконання інших послуг
  - КД, КА, ЦД, ЦА, ЦО, НР, НО, НА, НП → НИ-1 (ідентифікація, автентифікація)
  - КА, ЦА, КВ-2-4, ЦВ-2,3, ДР, ДС, ДЗ, ДВ, НР-2,5, НЦ-1, НТ-2 → НО-1 (виділення адміністратора)
  - КД-3,4, КА-3,4, ЦД-3,4, ЦА-3,4, КК → КО-1 (повторне використання об’єктів)
  - КК-2, КВ-4, НЦ-1 → НР-1 (реєстрація)
  - КВ-3,4, ЦВ-3 → НВ-1 (ідентифікація й автентифікація при обміні)
  - ДЗ-2,3 → ДС-1 (стійкість до відмов)
  - НИ-2,3 → НК-1 (достовірний канал)
  - КК, КВ-4 → Г-3

Класифікація АС і стандартні функціональні профілі ЗІ в КС

- Клас 1: одномашинний однокористувачевий комплекс
  - Окрема робоча станція, що не підключена до мережі
- Клас 2: локалізований багатомашинний багатокористувачевий комплекс
  - Локальна мережа
  - Багатотермінальний сервер
  - Кілька комп'ютерів, що не поєднані у мережу, але знаходяться у спільному приміщенні і виконують спільні завдання
- Клас 3: розподілений багатомашинний багатокористувачевий комплекс
  - Головна ознака – принципова неможливість повного контролю території, на якій знаходиться АС

Семантика профілю

- Опис профілю складається з трьох частин:
  - буквено-числового ідентифікатора
  - знака рівності
  - переліку рівнів послуг, взятого в фігурні дужки
- Ідентифікатор у свою чергу включає:
  - позначення класу АС (1, 2 або 3)
  - буквену частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д)
  - номер профілю і необов'язкове буквене позначення версії
- Всі частини ідентифікатора відділяються один від одного крапкою
  - Наприклад, 2.К.4 — функціональний профіль номер чотири, що визначає вимоги до АС класу 2, призначених для обробки інформації, основною вимогою щодо захисту якої є забезпечення конфіденційності
- Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю
  - Наприклад, нарощування можливостей реєстрації приведе до появи нової версії
- Внесення деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого класу чи підкласу АС

Приклади стандартних функціональних профілів захищеності

1.Ц.2 = { ЦА-2, ЦО-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
1.Д.2 = { ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }
1.Д.3 = { ДР-2, ДС-2, ДЗ-2, ДВ-2,
НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }
1.КЦ.2 = { КА-1, КО-1,
ЦА-2, ЦО-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
2.КЦ.2 = { КД-2, КО-1,
ЦД-1, ЦО-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1 }
2.КЦД.2 = { КД-2, КА-2, КО-1,
ЦД-1, ЦА-2, ЦО-1,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }
3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,
ЦД-1, ЦА-2, ЦО-1, ЦВ-2,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

НД ТЗІ 2.5-008-02

- Повна назва документа - Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
- Мета документа – надання нормативно-методологічної бази під час розроблення комплексів засобів захисту від НСД до конфіденційної інформації, яка обробляється в АС класу 2, створення КСЗІ, 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
- В документі наведені:
  - загальні вимоги до захисту конфіденційної інформації, які випливають з вимог чинного законодавства
  - характеристики типових умов функціонування АС класу 2. Розглянуті обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, користувачі АС та оброблювана інформація, у тому числі й технологія її оброблення.
  - детальні вимоги щодо захисту інформації в АС класу 2
  - докладно розібрана політика реалізації послуг безпеки інформації в АС класу 2
- Фактично, документ є детальною настановою з розроблення технічного завдання на створення КСЗІ в АС класу 2

Політика безпеки згідно НД ТЗІ 2.5-008-02

- Як основний принцип політики безпеки визначено адміністративний принцип розмежування доступу, який забезпечується послугами безпеки КА і ЦА
- Реалізація послуг безпеки, що базуються на довірчому принципі розмежування доступу (КД і ЦД), може здійснюватися у випадках:
  - коли 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
- Визначені такі стандартні функціональні профілі захищеності оброблюваної інформації:
  - 2.К.3 = {КД-2, КА-2, КО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}
  - 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}
  - 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}
  - 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}
- Мінімальним достатнім рівнем гарантій реалізації КЗЗ АС класу 2 є рівень Г–2
- Реалізація послуги безпеки КО-1 є необов'язковою у тому випадку, коли в АС класу 2 усі користувачі допущені до обробки конфіденційної інформації одного рівня

НД ТЗІ 2.5-010-03

- Повна назва документа – Вимоги до захисту інформації WEB–сторінки від несанкціонованого доступу
- Документ встановлює вимоги до технічних та організаційних заходів захисту інформації Web-сторінки (Web-сайту) в мережі Інтернет
  - Зокрема, мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації Web-сторінки від несанкціонованого доступу згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями
- Мета документа – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації Web-сторінки під час створення КСЗІ
- В документі наведені:
  - загальні вимоги до захисту інформації Web-сторінки, які випливають з вимог чинного законодавства
    - актуалізація розміщених на Web-сторінці інформаційних ресурсів та керування доступом до них здійснюється за допомогою АС, в якій повинна бути створена КСЗІ
  - характеристики типових умов функціонування такої АС
  - детальні вимоги щодо захисту інформації Web-сторінки
  - докладно розібрана політика реалізації послуг безпеки інформації в АС, що забезпечує функціонування Web-сторінки

Категорії інформації Web-сторінок згідно НД ТЗІ 2.5-010-03

- Інформація Web-сторінки поділяється на дві категорії: загальнодоступна і технологічна
  - Загальнодоступна – інформація, що розміщується на Web-сторінці з метою надання можливості користування нею будь-яким фізичним або юридичним особам, які мають доступ до мережі Інтернет
  - Технологічна інформація Web-сторінки – технологічна інформація КСЗІ та технологічна інформація щодо адміністрування та управління обчислювальною системою АС і засобами обробки інформації
    - дані про мережні адреси,
    - імена, персональні ідентифікатори та паролі користувачів,
    - їхні повноваження та права доступу до об’єктів,
    - інформація журналів реєстрації дій користувачів,
    - інша інформація баз даних захисту,
    - встановлені робочі параметри окремих механізмів або засобів захисту,
    - інформація про профілі обладнання та режими його функціонування,
    - робочі параметри функціонального ПЗ тощо.
- Розміщення на Web-сторінці конфіденційної інформації діючим законодавством не припускається
  - Якщо інформація не є власністю держави або інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом, то власник інформації може запроваджувати правила доступу до неї на свій розсуд, але при цьому вимоги НД ТЗІ 2.5-010-03 не дотримуються

Технології доступу до інформації згідно НД ТЗІ 2.5-010-03

- Web-сторінка може бути розміщена
  - на території власника інформації
  - на території сторонньої організації (наприклад, оператора мережі доступу до Інтернет)
    - Власник інформації, виходячи з чинного законодавства, визначає правила доступу до інформації
    - Власник системи здійснює захист інформації, зокрема, забезпечуючи відповідне розмежування доступу до інформації
- Доступ до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації може здійснюватись у два способи:
  - **Технологія Т1**: з робочої станції, розміщеної на тій самій території, що і Web-сервер (установи-власника Web-сторінки або оператора) або з консолі Web-сервера
  - **Технологія Т2**: з робочої станції, яка розміщена на території установи-власника Web-сторінки, до Web-сервера, що розміщений на території оператора, з використанням мереж передачі даних
- Технологія Т2 відрізняється від технології Т1:
  - наявністю незахищеного середовища, яке не контролюється
  - додатковими вимогами щодо ідентифікації та автентифікації між КЗЗ робочої станції й КЗЗ Web-сервера під час спроби розпочати обмін інформацією
  - додатковими вимогами щодо забезпечення цілісності інформації при обміні

Функціональні профілі захищеності згідно НД ТЗІ 2.5-010-03

- Коли доступ до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації здійснюється за технологією Т1, мінімально необхідний функціональний профіль визначається:

  {КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}
- Коли передбачається можливість доступу до технологічної інформації та/або передавання даних для актуалізації загальнодоступної інформації за технологією Т2, мінімально необхідний функціональний профіль визначається:

  {КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1}
- Мінімальним достатнім рівнем гарантій реалізації КЗЗ Web-сторінки є рівень Г–2

Оцінювання за критеріями

- Передбачено дві процедури:
  - Сертифікація засобів захисту
    - Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення
      - Наказ Держстандарту України та Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 9.07.2001 № 329/32
  - Державна експертиза КСЗІ
    - Положення про державну експертизу в сфері технічного захисту інформації
      - Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93
- Реально побудована система проведення державної експертизи, як для КСЗІ, так і для засобів захисту