УДК 519.6
Снопик В. – ст.гр. ІПЗзмсм-51
Тернопільський національний економічний університет

АНАЛІЗ ЗАХИЩЕНОСТІ ВІДДАЛЕНОГО ДОСТУПУ

Науковий керівник: к.т.н., доцент Співак І.Я.

Snopik V.
Ternopil National Economic University

ANALYSIS OF THE SECURITY OF REMOTE ACCESS

Supervisor: Ph.D. Spivak I.

Ключові слова: аналіз. захист, віддалений доступ.
Keywords: analysis, protection, remote access.

Розподілена мережа є принадливою для багатьох загроз як ненавмисних, так і зловмисних (у першу чергу, несанкціонованих) дій, і в певних випадках ці загрози можуть бути реалізованими успішно. Це пов'язано як із можливою високою професійністю порушників, так і з вразливістю всіх комп'ютеризованих систем. Дослідження й аналіз інформаційної безпеки різних розподілених обчислювальних систем підтверджують той факт, що, незалежно від використовуваних мережних протоколів, топології, інфраструктури розподілених обчислювальних систем, механізми реалізації загроз у РОМ є інваріантними стосовно особливостей конкретної системи. Це пояснюється тим, що розподілені обчислювальні системи проектуються на основі однакових принципів, отже мають практично однакові проблеми безпеки. Тому виявляється, що причини успіху атак на різні РОМ однакові. Таким чином, з'являється можливість увести поняття типової віддаленої загрози — це віддалений інформаційний вплив, що програмно здійснюється каналами телекомунікаційної мережі з метою порушення тієї чи іншої функціональної властивості захищеності (конфіденційності, доступності, цілісності) інформаційних об'єктів, їхніх потоків чи елементів мережі та є характерним для будь-якої розподіленої обчислювальної системи.

Уся множина загроз, що реалізуються навмисними чи випадковими порушниками в будь-якій системі, у тому числі й у РОМ, може буди розглянута як сукупність атак на основні функціональні властивості захищеності інформаційних об'єктів та їхніх потоків — конфіденційність, цілісність, доступність інформаційних об'єктів, системи чи її елементів.

Шляхами реалізації таких загроз щодо *конфіденційності інформаційних ресурсів* є:

1) несанкціонований доступ до інформаційних ресурсів із подоланням засобів захисту в локальній мережі чи в елементах розподіленої мережі;

2) використання витоків інформації технічними каналами в локальній мережі чи в елементах розподіленої мережі;

3) подолання неавторизованим користувачем криптографічної захищеності інформаційних об'єктів (у разі її наявності) у локальній мережі чи в елементах розподіленої мережі;

4) використання спеціальних типів вірусних атак, що переводять захищений інформаційний ресурс із розряду конфіденційного до розряду відкритого.