

Міжнародна студентська науково - технічна конференція
"ПРИРОДНИЧІ ТА ГУМАНІТАРНІ НАУКИ. АКТУАЛЬНІ ПИТАННЯ"

УДК 004.75

Чиж О. – ст. гр. СІм-62

Тернопільський національний технічний університет імені Івана Пулюя

**ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
У КОМП'ЮТЕРНИХ МЕРЕЖАХ**

Науковий керівник: доктор технічних наук, професор Лупенко С.А.

Chyzh O.

Ternopil Ivan Pul'uj National Technical University

**THREATS TO INFORMATION SECURITY
IN COMPUTER NETWORKS**

Supervisor: doctor of technical sciences, professor Lupenko S.A.

Ключові слова: атака, зловмисник, інформаційна безпека.

Keywords: attack, malice, information security

Комп'ютерні мережі через притаманні їм особливості створюють умови для виникнення численних загроз безпеці інформації. Розподіл ресурсів та інформації у просторі робить можливою наявність специфічного виду атак – так званих мережевих, або віддалених атак.

Однією з основних причин потенційної вразливості комп'ютерних мереж є принципи їх функціонування. Інформаційний обмін у мережі здійснюється за допомогою механізму повідомлень. У вузлах мережі присутні апаратні та програмні засоби, які діють автоматизовано, без втручання оператора. Такі засоби призначення для передавання і приймання даних через мережу.

Мережа Інтернет становить особливу небезпеку через свою доступність і глобальний масштаб. У мережі присутні та активно діють численні зловмисники – професіонали та просто допитливі користувачі, які знайшли інструменти зламу – доступне в мережі відповідне програмне забезпечення і тепер намагаються його випробувати на різних ресурсах. Атака на підключену до мережі автономну систему може бути матеріально чи політично вмотивованою. Зловмисники, навіть якщо будуть вистеженими, можуть знаходитися в іншому правовому полі (іншій державі) і бути недосяжними для покарання.

Типові атаки, що можуть бути застосовані для нападу на розподілені системи та які слід моделювати під час випробувань стійкості до них систем:

- вгадування паролів, або атаки за словником;
- реєстрація та маніпуляції з мережевим трафіком;
- імпорт фальшивих пакетів даних;
- експлуатація відомих вразливостей програмного забезпечення (мови макросів, помилок в ОС, служби віддаленого доступу тощо).

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – Київ: Видавнича група ВНУ, 2009. – 610 с.