$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv$ xp-1 $\equiv$1 mod p, тобто $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ або $a^{\frac{p-1}{2}}$ - 1 ділиться на p. Якщо a є квадратичним нелишком, то $a^{\frac{p-1}{2}}$ - 1 не ділиться на p, звідки $a^{\frac{p-1}{2}}$ + 1 повинно ділитися на p, або $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

**Висновок**

Співвідношення обчислювальних складностей розробленого алгоритму відносно класичного визначає виграш в ефективності:

$$E(п) = \frac{n\left(\log_2 n\right)^2}{n\left(\log_2 n\right)} = \log 2n.$$

Отже, виграш в ефективності удосконаленого методу при зростанні розрядності чисел зростає в log2n разів.

Застосування на практиці різних методів розкладання чисел показало, що час виконання алгоритму безпосередньо залежить від його типу та обчислювальної складності.

**Список використаних джерел**


1. Акушский И.Я. Машинная арифметика в остаточных классах. // Акушский И.Я., Юдицкий Д.И – М: Сов.радио, 1968. – 440 с.
2. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ„Терно–граф”, 2010. – 536 с.



УДК 683.1


# ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ


**Якименко І.З.[1)], Сіверський М.І.[2)]**

*Тернопільський національний економічний університет*

*[1)] к.т.н., доцент; [2)] магістрант*


## І. Постановка проблеми

Швидкий ріст структур інформаційних зв'язків спричинив багаторазовий ріст швидкості інформаційних потоків в комп’ютерних мережах. Величезний потенціал розвитку цих технологій породив загрозу інформаційній безпеці - складну науково-практичну проблему із соціальними наслідками. У цій ситуації найважливішим завданням є організація швидкого, надійного та захищеного зв'язку в мережах загального користування (МЗК).

Захист інформаційних потоків на сьогоднішній день стає усе більш складною проблемою, яка зумовлена певними обставинами, а саме: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державних і військових секретів, але й промислової, комерційної та фінансової таємниць; можливості несанкціонованих дій з інформацією, що розширюються [1]. Однак наразі приділяється мало уваги факту екстенсивного росту мереж загального користування, а також тому, що більша частина інформації передається саме за їхньою допомогою.

## ІІ. Мета роботи.

Проведення аналізу моделей захисту інформації в мережах загального користування на основі класифікації показників безпеки.

## ІІІ. Захист інформації в мережах загального користування

Відомо, що основними каналами передачі інформації в МЗК є лінії зв'язку (телефонні). Захист ліній зв'язку являє собою дуже серйозну проблему, тому що ці лини найчастіше бувають безконтрольними і з них можуть несанкціоновано отримуватися інформація [2].

Розробка технічних методів і засобів захисту інформації заснована на використанні методів математичного моделювання [3].

До основних задач моделювання систем захисту інформаційних потоків в комп’ютерних мережах, які найчастіше зустрічають в літературних джерелах, можна поділити на [4]: оцінка якості

функціонування систем захисту інформації (ЗІ); проведення аналізу надійності систем ЗІ; класифікація показників безпеки інформації; обґрунтування та вибір критерію для оптимізації технічної системи ЗІ; проведення аналізу ризиків інформаційної безпеки і виділити їхні наслідки; огляд методів впливу дестабілізуючих факторів на завадостійкість передачі інформації; визначити критерії невидимості для схованих каналів; проведення досліджень і аналізу захищеності бездротових корпоративних мереж; практична реалізація криптографічних методів ЗІ; методи вилученого адміністрування для несанкціонованого доступу до інформаційних ресурсів.

В особливий клас можна виділити завдання ведення інформаційних війн, системи керування вмістом і безпека веб-сайтів, застосування штучних нейронних мереж систем ЗІ, економічної безпеки держави.

Що стосується математичного моделювання інформаційної безпеки (ІБ) багатьма науковцями ведеться робота щодо розробки моделей аналізу загроз ІБ у комп'ютерній мережі.

Для розв'язання задачі захисту конфіденційної інформації, яка передається на великі відстані, існує фактично два методи: прокладати власні лінії зв'язку; використовувати існуючі лінії зв'язку МЗК (телефонні мережі, Інтернет і т.д.).

Перший метод має кілька очевидних недоліків: витрати фінансів та часу, не гарантує надійного захисту комунікацій, обмежений у застосуванні.

Другий метод – застосування відкритих комунікаційних каналів має лише один, але дуже істотний недолік: повна відсутність захищеності даних, що передаються. Усунути цей недолік покликані системи захисту інформації, які створюють захищений закритий канал усередині відкритого каналу МЗК, запобігаючи, таким чином, несанкціонованому зніманню інформації при передачі від абонента до абонента за принципом точка-точка.

### IV. Висновок

Отже, проведений аналіз задач захисту інформаційних потоків в мережах загального користування дозволив виділити основні переваги та недоліки основних методів збереження конфіденційності інформації, яка передається на великі відстані.

### Список використаних джерел


1. Ленков СВ. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий— Т.2: Информационная безопасность. — 2008. — 344 с.
2. Хома В.В. Методи та засоби забезпечення конфіденційності телефоних повідомлень. / Хома В.В. // Сучасна спеціальная техніка, №3(18), 2009. – С. 50-59.
3. 3 Петров А.А. Особенности проектирования математических моделей защиты информации // Вісник СНУ ім. В.Даля. – 2009. - №131.– С. 122-127.
4. Живко З.Б. Ризики інформаційної безпеки та їх наслідки. / С.В. Малкуш, М.О. Живко // Сучасна спеціальна техніка. – 2010. – №1(20). – С. 21-29.



УДК 683.1


## МЕТОД МОДЕЛЮВАННЯ ЗАХИСТУ СИСТЕМИ ВІД ЗАГРОЗ ЛІНІЙНОГО ВИДУ


**Яциковська У.О.[1)], Якименко І.З.[2)], Маланчук М.В. .[3)]**

*[1)]Тернопільський національний технічний університет ім.І. Пулюя, к.т.н.;*
*Тернопільський національний економічний університет*
*[2)] к.т.н.; [3)] магістрант*


### І. Постановка проблеми

Останнім часом несанкціонований доступ до інформації сприяє значному росту злочинності у КМ. Для власників важливих інформаційних даних, комп’ютерна злочинність, а саме атаки на інформаційні потоки призводять до небажаних великих фінансових збитків. Найпоширенішими видами лінійних атак в КМ є DoS/DDoS/DRDoS-атаки (Denial of Service / Distributed Denial of Service / Distributed Reflection Denial of Service). Тому актуальною задачею є удосконалення системи безпеки інформаційних даних в КМ.