УДК 681.3.06

В.Б. Дудикевич[1], Б.П. Томашевський[2]

[1] *Національний університет «Львівська політехніка», Львів*
[2] *Академія сухопутних військ, Львів*

МЕТОД ПОБУДОВИ КРИПТО-КОДОВИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА НЕДВІЙКОВИХ РІВНОВАГОВИХ КОДАХ

Проблема захисту комп'ютерних мереж від несанкціонованого доступу набула в останні десятиліття особливої гостроти. Бурхливе зростання комунікаційних і обчислювальних технологій дозволяє будувати мережі розподіленої архітектури, що об'єднують велику кількість сегментів, розміщені на значній відстані один від одного. Усе це викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі і доступу до конфіденційної інформації користувачів.

Для оцінки ефективності обміну даними в комп'ютерних системах і мережах введений узагальнений показник ефективності, який об’єднує показники конфіденційності, достовірності і безпеки.

Виникає протиріччя між зростанням обсягів інформації, які підлягають несиметричному криптографічному перетворенню із забезпеченням доказової стійкості, і лімітом часу для обробки інформації криптографічними засобами захисту. Потрібна наукова розробка нових методів, алгоритмів і технічних засобів на їх основі для ефективного криптографічного захисту інформації з високими показниками безпеки, яка забезпечується, достовірності і оперативності передавання даних.

Таким чином, розробка методу побудови крипто-кодових засобів захисту інформації для комплексного забезпечення безпеки і достовірності передавання даних в комп'ютерних системах і мережах є актуальним науковим завданням.

Для вирішення даного завдання необхідно розробити метод недвійкового рівновагового кодування і крипто-кодових засобів захисту на їх основі для забезпечення безпеки і достовірності передавання даних [1 – 3].

Перспективним напрямом у розвитку криптографічних засобів захисту інформації доказової стійкості є крипто-кодові механізми, побудова яких заснована на зведенні завдання злому ключових даних до рішення теоретико-обчислювальної задачі декодування випадкового коду. В деяких джерелах вони дістали назву теоретико-кодових схем [2]. Проведений аналіз показав, що для систем з автоперезапитом найбільше підходить схема Нідеррайтера, що дозволяє забезпечити максимальну швидкість кодування, чим і визначається остаточний вибір напряму досліджень. На сьогодні методи рівновагового кодування розроблені тільки на випадок двійкових кодових послідовностей, тобто існуючий науково-методичний апарат, застосовувані методи і обчислювальні алгоритми не дозволяють реалізувати недвійкове рівновагове кодування, зокрема і в крипто-кодових засобах захисту інформації [1].

Таким чином, вперше розроблено метод недвійкового рівновагового кодування, заснований на запропонованому узагальненому біноміально-позиційному представленні чисел і дозволяє, на відміну від відомих методів, формувати дискретні послідовності з елементами довільного недвійкового числового поля з фіксованою вагою Хемінга і практично реалізувати обчислювальні алгоритми недвійкового рівновагового кодування.

Отримав подальший розвиток математичний апарат крипто-кодового захисту інформації для комплексного забезпечення безпеки і достовірності передавання даних у комп’ютерних системах і мережах: запропоновано метод формування сеансових ключових даних, який реалізується з використанням розроблених процедур рівновагового недвійкового кодування в режимі прямого виправлення помилок; запропоновано формальне математичне визначення крипто-кодової системи захисту інформації, яке враховує особливості формування криптограм з використанням недвійкових рівновагових кодів і їх зворотного крипто-кодового перетворення на приймаючій стороні, у режимі виявлення помилок і автоматичного перезапиту [3].

Список літератури

1. Борисенко А.А. Биномиальный счет. Теория и практика: монография / А.А. Борисенко. – Сумы: ИТД «Университетская книга», 2004. – 170 с.

2. Дудикевич В.Б. Метод недвійкового рівновагового кодування / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації: науково-технічний журнал. – 2010. – № 3. – С. 57-68.

3. Дудикевич В.Б. Крипто–кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації: науково-технічний журнал. – 2010. – № 2. – С. 14-23.