УДК 621.396.253

Дослідження механізмів формування псевдовипадкових чисел

Лисенко І.А., асистент
Центральноукраїнський національний технічний університет, м. Кропивницький

Життєвий цикл системи захисту інформації складається з декількох етапів, найважливішими з яких є визначення послуг безпеки і вибір механізмів безпеки.

Визначено п'ять загальноприйнятих послуг безпеки: автентифікація, управління доступом, конфіденційність даних, цілісність даних, неможливість відмови (причетність).

Приведені послуги безпеки забезпечуються за допомогою механізмів безпеки, які складаються з таких основних елементів, як: механізми шифрування, механізми цифрового підпису, механізми керування доступом, механізми цілісності даних, механізми автентифікації.

Механізми шифрування припускають використання криптографічних перетворень даних. Значну частину серед них займає розробка перспективних методів і алгоритмів формування псевдовипадкових чисел.

До криптографічних методів формування псевдовипадкових чисел ставляться все більш високі вимоги як до швидкодії так і до стійкості. Особливе місце в області формування псевдовипадкових чисел займають методи, засновані на зведенні задачі криптоаналізу до розв'язання деякої добре відомої теоретико-числової задачі. Проте методи, засновані на доказово стійких перетвореннях володіють високими характеристиками статистичної безпеки, але є складними в реалізації і не формують псевдовипадкових послідовностей максимального періоду.

Таким чином існуючий математичний апарат, відомі методи та алгоритми формування псевдовипадкових чисел не дозволяють повною мірою забезпечити високі показники ефективності.

Для розв'язання цієї задачі необхідна розробка методів і алгоритмів формування псевдовипадкових чисел доказової стійкості, реалізація яких дозволить будувати генератори псевдовипадкових чисел з необхідними для практики властивостями.

Перспективним напрямком у цьому випадку є генератори псевдовипадкових чисел з використанням надлишкових кодів. Тоді завдання криптоаналізу зводиться до розв'язання задачі декодування випадкового коду, а відповідні методи формування псевдовипадкових чисел відносять до групи доказово стійких генераторів, які до того ж володіють високими показниками швидкодії як при програмній так і при апаратній реалізації.