розрядності згідно з вимогами застосовуваного криптографічного алгоритму.

Особливістю реалізації етапу 3 є розподіл видозміненої стиснутої двійкової послідовності на кодові комбінації фіксованої розрядності $K_j''$ без урахування характеру входження в неї початкових символів повідомлення $K_i$, що зумовлює можливість виникнення нетипових ситуацій.

Оскільки характер розподілу нерівномірних кодових комбінацій $K_i'$ між рівномірними кодовими комбінаціями $K_j''$ без урахування особливостей реалізації алгоритму ОНК апріорно є непередбачуваним зловмиснику, такий підхід, окрім зменшення розмірів призначеного для передачі двійкового коду вихідного тексту, збільшує ентропійні властивості зашифрованого тексту і його стійкість до зламу незалежно від застосовуваного методу криптографічного шифрування.

***к.т.н., доц. Чорненький В.І. (ХмНУ)***
***к.т.н., доц. Чешун В.М. (ХмНУ)***
***д.т.н., проф. Яцків В.В. (ЗНУ***
***Солодєєва Л.В. (ВІКНУ)***

## Смарт-генерація псевдовипадкових чисел для формування криптоключів системи клієнт-банк

Генератори псевдовипадкових чисел (ГПВЧ) або послідовностей сьогодні є одним із основних елементів систем захисту інформаційних ресурсів від зловмисних посягань. Перевагою генерованих ГПВЧ паролів доступу порівняно з створюваними людиною є значно більший показник ентропії, оскільки символи таких паролів є незалежними і позбавлені апріорної вади зручності запам’ятовування для користувача, якою першочергово користуються хакери систем авторизації.

Завдяки здатності генерувати двійкові коди з високою ентропією ГПВЧ широко застосовуються в системах криптографічного захисту починаючи від формування ключів шифрування таблиць Віженера, реалізації алгоритмів симетричного і асиметричного шифрування, і до формування векторів ініціалізації режимів застосування алгоритмів шифрування, хешування з паролями, створення систем цифрового підпису в системах клієнт-банк тощо. Недостатня ентропія джерела псевдовипадкових чисел системи клієнт-банк може стати причиною її краху.

Оскільки алгоритмічно-генеровані псевдовипадкові послідовності характеризуються циклічною повторюваністю, для підвищення їх «непередбачуваності» застосовується додаткове джерело ентропії, призначення якого може полягати у визначенні стартового значення генерованої послідовності або у підвищенні показників ентропії генерованих значень іншим чином.

Перенесення банківських послуг в сферу мобільних технологій зумовлює зацікавленість в створенні повноцінних, зручних і надійних систем клієнт-банк на базі пристроїв мобільного зв’язку. Відповідно, однією із функцій подібних пристроїв мають стати функції ГПВЧ.

Перевагою сучасних смартфонів є наявність великої кількості датчиків, які можуть бути джерелами  ентропії для ГПВЧ. Як показали дослідження, в роботі ГПВЧ цього можуть бути використані вектори обертання, акселерометр, давач лінійного прискорення, давач гравітації, давач орієнтації, гіроскоп, давач близькості, барометр, магнітометр.

Пропонований ГПВЧ як додаткове джерело ентропії використовує випадкові дані з датчиків андроїд-пристроїв, які надсилаються на вхід хеш-функції. Вихід хеш-функції використовується як ключ для алгоритму генерації псевдовипадкових чисел. Для генерації випадкових чисел в мобільних пристроях використано комбінований підхід зі зчитуванням оперативних вимірів кількох активних датчиків пристрою і подальшим комбінуванням отриманої послідовності з даними вбудованих ГПВЧ.

***к.т.н. доцент Шваб В.К. (ВІКНУ)***
***к.т.н. доцент Браун В.О. (ВІКНУ)***
***Шевченко В.В. (ВІКНУ)***

## Принципові протиріччя побудови систем захисту конфіденційної інформації та вимоги до них

Операційна система є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній операційній системі багато в чому залежить і загальна безпека інформаційної системи.

У зв'язку із цим розглянемо відповідність засобів захисту сучасних ОС класу автоматизованих систем на яких обробляється конфіденційна інформація. Спочатку зупинимося на принциповому, навіть, концептуальному протиріччі між реалізованими в ОС механізмами захисту й прийнятими формалізованими вимогами.

Протиріччя складається в принциповому розходженні підходів до побудови схеми адміністрування механізмів захисту й, як наслідок, це докорінно позначається на формуванні загальних принципів реалізації політики безпеки, розподілення відповідальності за захист інформації, а також на визначенні того, кого відносити до потенційних зловмисників (від кого захищати інформацію).

Для демонстрації цього із сукупності формалізованих вимог до системи захисту конфіденційної інформації розглянемо наступні дві вимоги:

- право змінювати правила розмежування доступу повинне надаватися виділеним суб'єктам (адміністрації, службі безпеки, тощо);
- повинні бути передбачені засоби управління, що обмежують поширення прав на доступ.

Дані вимоги жорстко регламентують схему (або модель) адміністрування механізмів захисту. Це повинна бути централізована схема, єдиним елементом якої виступає виділений суб'єкт, зокрема , адміністратор. При цьому кінцевий користувач виключений у принципі зі схеми адміністрування механізмів захисту.