Одержаний оптимальний режим процесу розчинення фосфогіпсу в пристрої [2], приведений в таблиці 3.

Таблиця 3

Оптимальний режим процесу розчинення фосфогіпсу

Коефіцієнт масовіддачі Y, м/с	**Амплітуда коливань рідини $X_1 \cdot 10^3$, м**	**Діаметр частинок фосфогіпсу $X_2 \cdot 10^3$, м**	**Температура рідкої фази X_3, К**
12,5	7,2	14,0	312,6

Отже, одержані в роботі теоретичні та експериментальні дослідження можуть бути використані для практичного застосування в реальній технологічній схемі переробки надзвичайно токсичних відходів, до яких належить фосфогіпс, який забруднює всі складові частини біосфери.

СПИСОК ЛІТЕРАТУРИ:

1. *Солтис М. М., Закордонський В. П. Теоретичні основи процесів хімічної технології. – Львів: Вид. центр ЛНУ ім. Івана Франка, 2003. – 340 с.*
2. *Малик Ю.К., Юрим М.Ф., Гумницький Я.М., та ін. Пристрій для хімічного розчинення фосфогіпсу. Деклараційний патент на корисну модель № 19571, 2006, Бюл. № 12. - 42 с.*
3. *Рудавський Ю.К., Мокрий Є.М., Піх З.Г. та ін. Математичні методи в хімії та хімічній технології. – Львів: Світ, 1993. – 206 с.*
4. *Налимов В.В., Чернова Н.А. Статистические методы планирования экстремальных экспериментов. – М. : Наука, 1985. – 340 с.*
5. *Батунер Л.М., Позин М.Е. Математические методы в химической технике. – Л.: Химия, 1988. – 820 с.*
6. *Ахназарова С.А. Кафаров В.В. Оптимизация эксперимента в химии и химической технологии. – М.: Высшая школа, 1978. – 318 с.*
7. *Бондарь А.Г. Математическое моделирование в химической технологии. К.: Вища школа, 1973 – 279 с.*
8. *Астрелін І.М., Запольський А.К., Супрунчук В.І. та ін. Теорія процесів виробництв неорганічних речовин. – К.: Вища школа, 1992. – 397 с.*

УДК 621.394.147.3 + 519.711.3

Я.Ю. Варецький, к. т. н., м. н. с. (ФМІ ім. Г.В. Карпенка НАН України)
А.О. Ігнатович (Національний університет "Львівська політехніка")

МОДЕЛЬ ВЗАЄМОДІЇ КОРИСТУВАЧА ІЗ СИСТЕМОЮ КРИПТОГРАФІЧНОГО ЗАХИСТУ

Стаття присвячена проблемі застосування біометричних ознак людини у системах криптографічного захисту. Для цього створено математичну модель взаємодії користувача із системою захисту, яка дозволила врахувати особливості біометричних даних, а саме нечіткість і стабільність

Постановка проблеми. Стрімкий розвиток обчислювальної техніки та розвиток телекомунікаційних мереж веде до необхідності створення систем безпечного зберігання та

передавання конфіденційної інформації. Сучасні вирішення задач захисту даних немислимі без використання криптографічних перетворень – шифрів. Центральним поняттям більшості шифрів є поняття таємного ключа - порівняно невеликої кількості інформації необхідної для здійснення криптографічних перетворень усієї інформації.

Довжина ключа визначає стійкість криптографічної системи захисту в обчислювальному сенсі. Але така стійкість дає лише теоретичну оцінку надійності захисту і, на жаль, стійкість відомих криптосистем визначається не стійкістю стандартизованого криптоалгоритму чи параметрами використаного ключа, а, насамперед, стійкістю найслабшої ланки у всій архітектурі криптографічного захисту. Більшість криптосистем "підводять" через помилки у реалізації взаємодії користувача із системою. Таку ситуацію називають атакою з врахуванням "людського фактора" (соціальна інженерія).

Максимальний рівень надійності кожного шифру досягається лише за умови повної секретності, випадковості та відповідної довжини використовуваних ключів, ці задачі вирішуються з допомогою ключової підсистеми. Ключі записуються на електронному носії інформації та захищаються додатковими методами захисту. Найбільш популярними методами захисту є методи, що ґрунтуються на використанні пароля - певної достатньо короткої для запам'ятовування фрази. Уся система захисту виглядає таким чином: користувач надає пароль, за допомогою пароля звільняється ключ, який використовується для безпосереднього шифрування цінних конфіденційних даних. Згідно з законом криптографії про те, що надійність системи захисту визначається надійністю її найслабшої ланки, отримуємо: конфіденційні дані, які захищені надійним криптоалгоритмом, є безпечними лише на стільки, на скільки безпечним є пароль. Тобто, короткі паролі – низький рівень захисту, довгі – рівень захисту високий, але виникає складність при запам'ятовуванні. Та найважливішою проблемою є відсутність зв'язку між паролем доступу до системи і власником цього пароля. Іншими словами, будь-кого, хто знає пароль користувача, система ідентифікує саме як цього користувача.

Останнім часом при розробці криптографічних систем захисту спостерігається зміщення акцентів у процесах управління ключами до застосування особистих ознак користувача системи, яким притаманні такі властивості: 1) індивідуальність або неповторність; 2) стабільність упродовж тривалого періоду; 3) неможливість фальсифікації; 4) неможливість розподілу серед декількох користувачів; 5) неможливість забути, загубити чи вкрасти. Саме тому актуальною проблемою є створення науково обґрунтованих моделей та методів взаємодії людини (користувача) із системою захисту.

Аналіз досягнень та публікацій. Основною ідеєю криптографічних систем з біометричним захистом ключів є створення ланок біометричного блокування (розблокування) ключів подібно до ланок парольного захисту ключів. Вирішенню поставлених проблем присвячені роботи [1-14].

У своїх роботах [3-5] Сутар (Soutar) запропонував алгоритм зв'язування ключа у кореляційній системі розпізнавання відбитків пальців. Алгоритм "інтегрує" у процесі реєстрації користувача в системі криптографічний ключ K у функцію кореляції. Використовуючи т. зв. тренувальні відбитки пальців (автор пропонує мінімум п'ять), утворюється кореляційна функція $H(u) = |H(u)|\, e^{-i\varphi_H(u)}$. Далі відкидається модуль $H(u)$, а добуток фази та випадкового комплексного числа утворює нове значення фази для величини, що записується на сервері, $H_{stored}(u)$ (відповідає $h(\,)$. Модуль $|H_{stored}(u)|$ утворюється з деякого випадково вибраного ключа K. Крім H_{stored} на сервері записується хеш ключа. Повна структура даних, що відповідає конкретному користувачу, називається *Bioscrypt*. У процесі ідентифікації користувач надає свої відбитки пальців (теж мінімум п'ять раз), які корелюються з допомогою функції кореляції. Використовуючи оригінальну процедуру відновлення, що використовує коди корекції помилок, автор виділяє ключ, який хешується та

порівнюється із хешем записаним у *Bioscrypt*. Результатом відновлення є або реальний ключ, або відмова у декодуванні. Алгоритм ніколи не видає неправильний ключ.

Недоліками методу є: 1) не розраховано втрати ентропії криптографічного ключа, який зв'язується даним методом; 2) не наведено значень залежностей FAR та FRR системи розпізнавання; 3) непривабливим для користувачів системи є необхідність кількаразового сканування пальця; 4) низькі коректуючі властивості (до 5% помилок). Збільшуючи коректуючі властивості методу, збільшуємо імовірність неправильної ідентифікації.

Девіда (Davida) [1,6] запропонував алгоритм з використанням біометрії рогівки ока та розглядав відображення рисунка рогівки у 2048 бітну двійкову послідовність (*IrisCode* [7]). У процесі ідентифікації розраховував віддаль Хемінга між наданою користувачем та збереженою у базі даних біометрією. Автор показав, що відмінність між різними взірцями однієї рогівки може досягати 10% (204 біт), а відмінність між рогівками різних людей – 45% (922 біт). У процесі реєстрації користувача в системі, отримуються декілька зображень рогівки ока та для кожної генеруються відповідний K бітний *IrisCode*. Із отриманих кодів за допомогою мажоритарного декодера утворюється "канонічний" *IrisCode* **T** довжини K. Далі вибирають (N, K) – код корекції помилок довжиною N, завадостійкі властивості якого дозволяють коректувати до 10% помилок. Кодове слово C, що відповідає послідовності **T**, хешують, підписують цифровим підписом системи та записують у базі даних разом із $R = N - K$ перевірочними бітами, доданими до **T** у процесі кодування. У процесі ідентифікації користувач надає *IrisCode* **T'**, до якого додається R, утворена двійкова послідовність вважається спотвореним кодовим словом. Застосовуючи функцію декодування, отримують кодове слово C', яке хешується, підписується цифровим підписом. Результат порівнюється з даними збереженими у базі. Автор стверджує, що *IrisCode* може використовуватись як криптографічний ключ, а для збільшення ентропії пропонується використання додаткового символьного пароля. Алгоритм є дуже швидким та надійним настільки наскільки надійною є використовувана хеш-функція. У методі чітко окреслена величина втрати ентропії використовуваного ключа (10% згідно з використовуваним кодом корекції помилок)

Недоліки алгоритму такі: 1) на відміну від попереднього, даний метод розглядається як метод генерації ключа, тобто біометричним даним користувача можливо поставити у відповідність лише один ключ; 2) на жаль, як показано у роботі [7], відмінність між різними взірцями однієї і тієї ж рогівки може досягати 30%, що, відовідно вказує на низькі коректуючі властивості методу, або на необхідне збільшення втрати ентропії до 30% для збільшення коректуючих властивостей.

Монроуз (Monrose) [8] запропонував об'єднати пароль користувача з біометрією динаміки роботи з клавіатурою. Ця робота є продовженням досліджень [15, 16], у яких пропонується метод рандомізації паролів перед хешуванням. Під рандомізацією, у даному випадку, розуміється приєднання до пароля (*psw*) випадкової послідовності довжиною s-біт, у результаті утворюється т.зв. "зміцнений" пароль (*hpsw*). У процесі реєстрації користувача системою зберігається така інформація: випадкове число r довжиною k біт; "таблиця інструкцій" зашифрована за допомогою *psw*. Таблиця інструкцій містить інформацію про процес генерації з r та *psw* значень *hpsw*. Процес генерації є толерантним до певної кількості помилок (параметр системи): "файл історії", зашифрований за допомогою *hpsw*.

У процесі ідентифікації користувач надає *psw'*. Під час набору пароля отримується біометрія. Обидві величини об'єднуючись утворюють *hpsw'*, яке використовується для розшифрування файла історії. У разі невдачі система розшифровує таблицю інструкцій за допомогою наданого пароля, та за допомогою схеми розподілу таємниці Шаміра генерує інше значення *hpsw'*, яке знову використовується для спроби розшифрування. Процес повторюється n раз, де n – параметр безпеки алгоритму.

Автор пропонує використовувати *hpsw* як ключ шифрування. Але, насправді, використовувана біометрія лише на 15 біт збільшує ентропію пароля, що лише несуттєво

збільшує ефективність звичайної парольної системи ідентифікації. У наступних модифікаціях алгоритму [9-11] Монроуз використовує біометрію голосу, що дозволило збільшити додаткову ентропію до 60 біт. Позитивним фактором є незалежність вибору ключа від біометричних даних, недоліком – відсутність інформації про втрату ентропії ключа.

Тайлз (Tuyls) [12, 13] запропонував алгоритм захисних функцій для збільшення конфіденційності ("Shielding Functions to Enhance Privacy"). У процесі реєстрації користувачем вибирається довільний криптографічний ключ S, який у вигляді хешу V записують у базі даних. Далі знаходять таке значення W, яке задовольняє умові $G(W, X) = S$, де X – біометрія користувача, $G(\ )$ – функція "δ-зв'язування", функція яка для усіх X', що знаходяться у δ-околі значення X, видає S. Автор вказує, що будь-яка детермінована функція володіє властивістю 0-звя'зування, ∞-звя'зуванням володіє функція $G(W, X) = \text{constant}$. Величина W записується у базі даних. У процесі ідентифікації користувачем надається біометрія X', а сервером ідентифікації величина W, які подаються у $G(W, X')$. Отримане значення S' хешується та порівнюється із V. На основі результату приймається рішення про ідентифікацію. Робота функції δ-звя'зування зв'язування ґрунтується на використанні завадостійкого кодування. Робота автора носить суто теоретичний характер. Не проводились дослідження із застосуванням конкретного виду кодів корекції, не розраховувались значення втрати ентропії, не вказано рівень стійкості системи.

У схемі "нечіткого зв'язування" (fuzzy commitment) [14] Джулс і Ватеннберг (Juels and Wattenberg) продовжили дослідження Девіди для збільшення коректуючих властивостей алгоритму. У процесі реєстрації користувач вибирає секретний ключ C, який одночасно є кодовим словом БЧХ - коду. Нехай d – це відстань між C та $\mathbf{T}$ –біометричною двійковою послідовністю. Структура fuzzy commitment містить d та хеш ключа C. У процесі ідентифікації користувач надає біометрію $\mathbf{T}'$. З допомогою d знаходять найближче кодове слово C', яке хешується та порівнюється з записаним на сервері. Перевагами цього алгоритму є його простота реалізації та можливість використання будь-якого коду корекції помилок. Але алгоритм має ряд суттєвих недоліків: автор пропонує використання методу із будь-яким типом біометрії, але не пропонує жодного методу перетворення біометрії у бітову послідовність ключа $\mathbf{T}$; алгоритм не працює при перестановці символів у $\mathbf{T}$, що відповідає спотворенням, які пов'язані зі скануванням; алгоритм вимагає рівномірного закону розподілу ключа, що неможливо для біометричних даних; вибір ключів обмежений множиною кодових слів.

Постановка цілей публікації. Нехай у процесі реєстрації біометричною системою зберігається не сам біометричний сигнал w, а його відображення $h(w, K)$, де K – це криптографічний ключ, який захищається системою. Трансформація $h(\ )$ – це, у певному сенсі, аналог криптографічної хеш-функції, тобто для різних входів w отримуються різні виходи, а отримання w або K із $h(w, K)$ є важкою проблемою.

У роботі [1] результат трансформації $h(w, K)$ носить назву "таємний шаблон" (private template), а у [2] – "скасовувана біометрія"(cancelable biometric). У літературі за процесом трансформації закріпився термін "зв'язування ключа" ("key binding").

Згідно такою постановкою задачі, у процесі ідентифікації відбувається трансформація вхідного біометричного сигналу користувача w' за допомогою функції $h(\ )$, а процес порівняння здійснюється у просторі відображень.

У різних системах ідентифікації, які використовують саме такий метод, необхідно використовувати різні перетворення, або те ж перетворення $h(\ )$, але з різними параметрами. І якщо у будь-якій із систем скомпрометовано $h(w, K)$, то інші системи, де використовувались ті ж біометричні дані, але з іншими ключами, функціонуватимуть далі без внесення змін.

У випадку використання необоротних функцій (хеш-функції, односторонні перетворення), стійкість $h(\ )$ є доведено високою, але FRR такої системи є великою. Причина

– відмінність у послідовних зчитування біометричних даних. Очевидно, що для різних біометричних даних w', w відображення $h(w')$ та $h(w)$ теж будуть різними.

За умови використання оборотних функцій (шифрування з ключем) – FRR системи на рівні звичайної біометричної системи ідентифікації, але безпека біометричних даних є пропорційною до стійкості оборотної функції, тобто знову виникають проблеми пов'язані з управлінням ключами. Враховуючи вищевказані проблеми, конкретна конструкція трансформації $h(\ )$ повинна враховувати такі особливості:

1) Нечіткість біометричних відображень: відмінності у наданні біометричних даних, відмінності у послідовних зчитуваннях біометричних даних, особливості апаратури та алгоритмів отримання біометричних даних.

2) Стабільність біометричних ознак: неможливість зміни або обмежена кількість змін біометричних даних після компрометації, застосування одних біометричних даних у кількох системах захисту.

3) Вразливість до атак з використанням "троянських коней".

Основна частина. Для моделювання процесу захисту криптографічних ключів класичними парольними методами використовується математична модель екстрактора випадкових величин [17-20], яка описує процеси отримання потоків квазівипадкових бітів, тобто бітових послідовностей, які жодним поліноміальним алгоритмом не можливо відрізнити від рівномірно розподілених послідовностей такої ж довжини. Відомими реалізаціями екстракторів є: важкооборотні функції та генератори псевдовипадкових бітів.

Означення 1. (n, m, l, ε) *– екстрактор* – це імовірнісна функція, яка відображає випадкову величину W визначену на $\{0, 1\}^n$ з мінімальною ентропією $H_\infty(W) \le m$ та випадкову величину рівномірного розподілу (паросток) $U_d \in_U \{0, 1\}^d$ у випадкову величину $Ext(W, U_d)$, яка є ε-близькою до $U_l \in_U \{0, 1\}^l$:

$$Ext: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^l,$$

$d = log(n - m) + 2\ log(1 / \varepsilon)$ – довжина паростка,

$l = m + d - 2\ log(1 / \varepsilon)$ – довжина виходу,

втрата ентропії екстрактора: $\triangle H(\ Ext(\ )\ ) = m + d - l = 2 \log(1 / \varepsilon)$, $\varepsilon > 0$ – як завгодно мала величина.

Для ефективного використання біометричних даних у блоках захисту криптографічних ключів пропонується розширити модель екстрактора до нової моделі біометричного екстрактора, яка, на відміну від моделі екстрактора випадкових величин, дозволить зв'язати криптографічні ключі з нечіткими та нерівномірно розподіленими біометричними даними і, тим самим, змоделювати безпосередню взаємодію користувача із системою захисту.

Означення 2. ($\mathcal{F}$, m, l, t, ε) - біометричний екстрактор – *це пара функцій:*

FG – імовірнісна генеруюча функція, що відображає $W \in \mathcal{F}^n$ *із* $H_\infty(W) \ge m$ та випадковий паросток $U_d \in_U \mathcal{F}^d$ у таємну стрічку $S \in \mathcal{F}^l$ та відкриту стрічку $Q \in \mathcal{F}^*$, які для двійки величин $(S, Q) \leftarrow FG(W, U_d)$ задовольняють умову $D[S, U_d] \le \varepsilon$:

$$FG: \mathcal{F}^n \times \mathcal{F}^d \to \mathcal{F}^l \times \mathcal{F}^*;$$

FR – відновлювальна функція, відображає $W' \in \mathcal{F}^n$ *та* $Q \in \mathcal{F}^*$ *у* $S' \in \mathcal{F}^l$, яке для усіх $W, W' \in \mathcal{F}^n$ *із* $\rho(W, W') \le t$ та $(S, Q) \leftarrow FG(W, U_d)$ задовольняє $S' = S$.

$$FR: \mathcal{F}^n \times \mathcal{F}^* \to \mathcal{F}^l;$$

де $\mathcal{F}$ – скінченне поле, $\rho(\ )$ – метрика у векторному просторі над $\mathcal{F}$,

$D[\ ,\ ]$ – статистична віддаль між розподілами ймовірностей випадкових величин.

Залишкова ентропія біометричного екстрактора: $\tilde{H}_\infty(W \mid Q) = l \ge m + d - 2\ log(1 / \varepsilon)$.

Біометричний екстрактор враховує проблему стабільності біометричних даних, а саме дозволяє поставити у відповідність до біометричних даних один або більше випадково вибраних ключів. Біометричний екстрактор зводиться до "чіткого" якщо $t = 0$, $Q = U_d$. Для врахування проблеми нечіткості введемо поняття біометричного ідентифікатора. Біометричний ідентифікатор відображає вхідні біометричні дані у певну структуру, нечутливу до визначеного рівня змін у біометричних даних.

Означення 3. $(\mathcal{F}, m, m', t)$ - біометричний ідентифікатор – це пара функцій:

FI – імовірнісна ідентифікуюча функція, що відображає $W \in \mathcal{F}^n$ із $H_\infty(W) \geq m$ та випадковий паросток $U_d \in_U \mathcal{F}^d$ у величину $p \in \mathcal{F}^*$ – ідентифікатор, який задовольняє умову $\tilde{H}_\infty(W \mid p) \geq m'$:

$$FI : \mathcal{F}^n \times \mathcal{F}^d \to \mathcal{F}^*,$$

причому втрата ентропії біометричного ідентифікатора за умови, що відомо p:

$$\Delta H(\, FI(\,)\,) = m - m';$$

FC – коректуюча функція, яка відображає $W' \in \mathcal{F}^n$ та p у таке $W'' \in \mathcal{F}^n$, що для усіх $p \leftarrow FI(W, U_d)$ та $\rho(W, W') \leq t$ виконується $W'' = W$:

$$\mathrm{FC} : \mathcal{F}^n \times \mathcal{F}^* \to \mathcal{F}^n.$$

Покажемо, що біометричний екстрактор – це складена конструкція, а саме, побудований з біометричного ідентифікатора та чіткого екстрактора. Перепишемо пару функцій біометричного екстрактора таким чином:

$FG(W, \langle U_{d1}, U_{d2}\rangle)$:

- розраховуємо $p \leftarrow FI(W, U_{d1})$ та $S \leftarrow Ext(W, U_{d2})$;
- виводимо $\langle S, Q\rangle$, де $Q \leftarrow \langle p, U_{d2}\rangle$.

$FR(W', \langle p, U_{d2}\rangle)$:

- відновлюємо $W \leftarrow FC(W', p)$;
- виводимо $S \leftarrow Ext(W, U_{d2})$.

Генеруюча функція FG отримує на вхід випадкову величину W деякого нерівномірного розподілу та двійку паростків $\langle U_{d1}, U_{d2}\rangle$ для роботи імовірнісних функцій. Функція FI створює ідентифікатор p вхідної величини W, а чіткий екстрактор видає таємну стрічку S, що застосовуватиметься у криптографічних алгоритмах у ролі ключа чи пароля. Цій стрічці ставиться у відповідність відкрита величина Q, яка використовуватиметься надалі функцією FR для відновлення таємної стрічки S.

На відміну від генеруючої функції, яка використовується лише один раз для створення S та її ідентифікатора Q, відновлююча функція використовуватиметься постійно для отримання із вхідних даних W', які є близькими у певному розумінні до W, таємної стрічки S. Саме міра близькості W' до W визначатиме алгоритми, що реалізують біометричний екстрактор.

Висновки та перспективи досліджень. Створено математичну модель процесу взаємодії користувача із криптографічною системою захисту – біометричний екстрактор, яка дозволяє врахувати такі проблеми безпосереднього застосування біометрії у ключовій підсистемі: нечіткість біометричних відображень, стабільність біометричних ознак. Показано, що біометричний екстрактор побудовано із дещо модифікованого екстрактора випадкових величин та нового криптографічного примітиву – біометричного ідентифікатора. На даний момент залишається відкритим питання створення ефективних алгоритмів для реалізації запропонованої моделі. Основним напрямком досліджень є застосування модифікованих БЧХ кодів або кодів Ріда-Соломона, які б дозволили реалізувати функціональність біометричного екстрактора з корекції нечіткості у послідовних зчитуваннях біометричних даних.

СПИСОК ЛІТЕРАТУРИ:

1. *Davida G.I., Frankel Y., Matt B.J. On enabling secure applications through off-line biometric identification // Proc. IEEE Symp. Privacy and Security. – 1998. – P. 148-157.*
2. *Ratha N., Connell J., Bolle R. Enhancing security and privacy in biometrics-based authentication systems // IBM System Journal. – Vol. 40, №3. – 2001. – P. 614-634.*
3. *Soutar C., Roberge D., Stojanov S. A., Gilroy R., Vijaya Kumar B. V. K. Biometric encryption using image processing // Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II. – Vol.3314. – 1998. – P. 178-188.*
4. *Soutar C., Roberge D., Stojanov S. A., Gilroy R., Vijaya Kumar B. V. K. Biometric encryption-enrollment and verification procedures // Proc. SPIE, Optical Pattern Recognition IX. – Vol.3386. – 1998. – P. 24-35.*
5. *Soutar C., Roberge D., Stojanov S.A., Gilroy R., Vijaya Kumar B. V. K. Biometric encryption // ICSA Guide to Cryptography. – R. K. Nichols, Ed. – New York: McGraw-Hill. –1999-480 p.*
6. *Davida G.I., Frankel Y., Matt B.J., Peralta R. On the relation of error correction and cryptography to an offline biometric based identification scheme // Proc. Workshop Coding and Cryptography (WCC'99). –1999. – P.129-138.*
7. *Daugman J. G. High confidence visual recognition of persons by a test of statistical independence // IEEE Trans. Pattern Anal. Machine Intell. – Vol.15. – 1993. – P. 1148-1161.*
8. *Monrose F., Reiter M. K., Wetzel S. Password hardening based on keystroke dynamics // Proc. 6th ACM Conf. Computer and Communications Security. – 1999. – P. 73-82.*
9. *Monrose F., Reiter M. K., Li Q., Wetzel S. Using voice to generate cryptographic keys // Proc. of A Speaker Odyssey, Speaker Recognition Workshop. – 2001. – P. 237-242.*
10. *Monrose F., Reiter M. K., Li Q., Wetzel S. Cryptographic key generation from voice // Proc. of IEEE Symp. Security and Privacy. – 2001. – P. 202-213.*
11. *Monrose F., Reiter M.K., Li Q., Lopresti D.P., Shih C. Toward speech-generated cryptographic keys on resource constrained devices // Proc. of 11th USENIX Security Symp. – 2002. – P. 283-296.*
12. *Linnartz J.-P., Tuyls P. New shielding functions to enhance privacy and prevent misuse of biometric templates // Proc. of 4th Int. Conf. Audio- And Video-Based Biometric Person Authentication. – 2003. – P. 393-402.*
13. *Verbitskiy E., Tuyls P., Denteneer D., Linnartz J.P. Reliable biometric authentication with privacy protection // Proc. Of SPIE Biometric Technology for Human Identification Conf. – Orlando, FL. – 2004.*
14. *Juels A., Wattenberg M. A fuzzy commitment scheme // Proc. of 6th ACM Conf. Computer and Communications Security. – G. Tsudik, Ed. – 1999. – P.28-36.*
15. *Manber .U. A simple scheme to make passwords based on one-way functions much harder to crack // Computers & Security. – Vol.15, №2. – 1996. – P.171-176.*
16. *Monrose F., Rubin A. Authentication via keystroke dynamics // Proc. of the 4th ACM Conference on Computer and Communications Security. – 1997. – P.48-56.*
17. *Nisan N., Zuckerman D. Randomness is linear in space // Journal of Computer and System Sciences. – 1996. – Vol.1, № 52. – P. 43-52*
18. *Zuckerman D. General weak random sources // Proc. of 31-st Annual Symposium on Foundations of Computer Science. – Vol.2. – 1990. – P. 534-543.*
19. *Zuckerman D. Simulating BPP using a general weak random source // Algorithmica. – Vol.4, №16. – 1996. – P. 367-391.*
20. *Santha M., Vazirani U.V. Generating quasi-random sequences from semi-random sources // Journal of Computer and System Sciences. – №33. – 1986. – P. 75-87.*