УДК 681.325.5.068

Н.В. САЧАНЮК-КАВЕЦЬКА, І.О. БОНДАРЕНКО

ІДЕНТИФІКАЦІЯ СУБ'ЄКТІВ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ ЗА ДОПОМОГОЮ ІДЕНТИФІКАЦІЙНОЇ ЛОГІКО-ЧАСОВОЇ ФУНКЦІЇ, ЯК ЕФЕКТИВНИЙ МЕТОД КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вінницький Національний технічний університет,
21021, Хмельницьке шосе, 95, м. Вінниця, Україна
E-mail: skn1901@gmail.com

Анотація. Розглянуто можливість підвищення ефективності захисту доступу до інформації із застосуванням спеціальної ідентифікаційної логіко-часової функції. Запроповано використання такої функції для парольної та біометричної ідентифікації суб'єктів.

Ключові слова: ідентифікаційна логіко-часова функція, Δ-інтервал, поліном, ключ, пароль**.**

Abstract.. As an identifier of the subject of access to information resources, you can use a special identification logic-time function (LTF) – the unequal difference in the user's biometric LTF characteristics, ranked by the degree of their importance. The possibility of increasing the efficiency of the protection of the access to information with the use of this special function is considered. The reliability of passwords can be greatly improved if you use some image converted to a logic-time function.

Keywords: identification logic-time function, Δ-interval, polynomial, key, password.
DOI: 10.31649/1681-7893-2018-35-1-14-23

ВСТУП

Впровадження сучасних інформаційних технологій створює підґрунтя для розвитку нової культури праці [1]. Організація – це динамічна структура, стан якої визначається як зовнішньою взаємодією з оточуючим середовищем, так і внутрішньою взаємодією між її елементами. Інформація має певну цінність, вона не локалізована в просторі і може легко поширюватись та є важливим ресурсом підприємства чи організації. Використання комп'ютерних систем та мереж для вирішення різноманітних підприємницьких завдань, стратегічного розвитку, реалізації зв'язків підприємств з їх партнерами, клієнтами, керуючими установами в On-line режимі дало можливість не обмежувати інформаційні потоки та інформаційні процеси межами окремого підприємства. За різними оцінками фахівців, керівники-управлінці витрачають від 30 до 95% свого часу на роботу з інформацією [2]. З кожним днем з'являються нові загрози, які здатні нанести збитків організації. Це зокрема хакерські дії, соціальна інженерія, втручання до системи, злом, несанкціонований доступ до системи, продаж інформації, перегляд інформації з обмеженим доступом, фальсифікація та підроблення даних тощо. Можна стверджувати, що такі загрози з часом набуватимуть все більшого поширення. Посилення залежності організацій від інформаційних, комунікаційних систем та послуг робить їх більш вразливими до порушень режиму безпеки.

Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів. З погляду безпеки всі види інформації потребують надійного захисту. Однак, управління доступом – ефективний метод комплексного захисту інформації, що регулює використання ресурсів інформаційної системи і включає в себе такий важливий елемент, як ідентифікацію користувача. Слід відмітити, що захисні заходи є ефективнішими, якщо вони вбудовані в інформаційні системи та послуги на етапах формування технічного завдання та проектування.

Віднедавна, все більше уваги привертає біометрія, як одна з новітніх інформаційних технологій, в якій використовуються унікальні характеристики об'єктів ідентифікації та веріфікації. Тому актуальним є питання захисту доступу до інформаційних ресурсів.

ОГЛЯД ПРОБЛЕМ ТА ПОСТАНОВКА ЗАДАЧІ СТВОРЕННЯ ЗАСОБІВ ІДЕНТИФІКАЦІЇ СУБ'ЄКТІВ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ, З ВИКОРИСТАННЯМ УНІКАЛЬНИХ ХАРАКТЕРИСТИК ОБ'ЄКТІВ

З появою і розвитком інформаційних технологій актуальною стала проблема інформаційної безпеки, пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах [3]. До передавання інформації каналами зв'язку ставлять такі вимоги:

– забезпечення конфіденційності інформації;
– забезпечення цілісності інформації;
– автентичність сторін інформаційного обміну [4].

Саме тому управління та розмежування доступу до інформаційних ресурсів є одними із важливих аспектів інформаційної безпеки. Методи і системи захисту інформації, що спираються на управління доступом виконують функції: ідентифікації користувачів; впізнання і встановлення достовірності користувача за обліковими даними; допуск до певних умов роботи згідно регламенту. Ідентифікація та автентифікація застосовуються для обмеження доступу випадкових та незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси) [5]. Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що підтверджує його особу, перевірити її достовірність і потім надати (чи не надати) цьому користувачу можливість роботи із системою. Наявність процедур ідентифікації та автентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки усі механізми захисту інформації розраховані на роботу іменованими суб'єктами і об'єктами інформаційних систем. Слід відмітити, що сучасні засоби ідентифікації/автентифікації повинні підтримувати концепцію єдиного входу в мережу – вимогу зручності для користувачів. Потрібно пам'ятати, що сервіс ідентифікації/автентифікації може стати об'єктом атак на доступність. Якщо конфігурація системи така, що після певного числа невдалих спроб пристрій введення ідентифікаційної інформації блокується, то зловмисник може зупинити роботу легального користувача буквально декількома натисканнями клавіш.

Існують такі види ідентифікації суб'єктів [6].

1) Парольна ідентифікація, заснована на конфіденційних ідентифікаторах суб'єктів (пароль, таємний ключ, персональний ідентифікатор і т. п.). В цьому випадку при введенні суб'єктом свого пароля підсистема автентифікації порівнює його з паролями, що зберігаються в базі еталонних даних у зашифрованому вигляді. У випадку співпадіння паролів підсистема автентифікації дозволяє доступ до інформаційних ресурсів. Головна перевага паралельної ідентифікації – простота реалізації й використання пари логін-пароль. Головним недоліком такої ідентифікації є залежність її надійності від користувачів, точніше, від обраних ними паролів (так званий людський фактор).

2) Апаратна ідентифікація, з використанням ключів, токенів або карт, що перебувають в ексклюзивному користуванні суб'єктів ідентифікації. Апаратні ідентифікатори умовно можна розділити на два типи: пасивні (картки з пам'яттю) та активні (інтелектуальні картки). Найбільш розповсюдженими є пасивні картки з магнітною стрічкою, при використанні яких користувач вводить свій ідентифікаційний номер. У разі його співпадіння з електронним варіантом, закодованим у картці, користувач одержує доступ до системи. Інтелектуальні картки мають власний мікропроцесор. Це дозволяє реалізувати різноманітні варіанти парольних методів захисту, наприклад, багаторазові паролі, паролі, що динамічно змінюються. Головною перевагою такої ідентифікації є її досить висока надійність. Однак велика вартість таких пристроїв, їх крадіжка у зареєстрованих користувачів, а також можливість дублювання знижує цікавість до засобів апаратної ідентифікації.

3) Біометрична ідентифікація [7], з використанням унікальних властивостей та ознак людини, забезпечує майже 100% ідентифікацію, вирішуючи проблеми втрати паролів та особистих ідентифікаторів. Біометричних характеристик є два класи:

– статистичні, які ґрунтуються на фізіологічних унікальних характеристиках об'єктів (за відбитком пальця, за термограмою обличчя, за формою долоні, за сітківкою ока, за ДНК, за розташуванням вен на лицьовій стороні долоні і т. ін), що практично не змінюються з часом;

– динамічні, які ґрунтуються на поведінковій характеристиці суб'єктів, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії (за почерком, за клавіатурним почерком, за голосом і ін.). Головною перевагою біометричних технологій є найвища надійність, а основним недоліком – вартість устаткування. Однак, ці методи не можливо використовувати при ідентифікації процесів чи даних (об'єктів даних), вони тільки починають розвиватися, вимагаються поки складного та дороговартісного обладнання.

4) Ідентифікація за допомогою доведення істинності віддаленого користувача за його місце знаходженням. Даний захисний механізм базується на використанні системи космічної навігації, типу *GPS (Global Positioning System)*. Користувач, який має апаратуру *GPS*, багаторазово надсилає координати заданих супутників, які знаходяться у зоні видимості. Підсистема автентифікації, яка знає орбіти супутників, може із точністю до метра визначити місце знаходження користувача. Висока надійність автентифікації визначається тим, що орбіти супутників піддаються коливанням, передбачити які достатньо важко. Окрім того, координати постійно змінюються, що виключає їх перехоплення. Це найновіший метод ідентифікації, що може бути використаний у випадках, коли авторизований віддалений користувач повинен знаходитись у потрібно місці.

Підходи 1–3 захисту доступу до інформації досить легко реалізувати в логіко-часовому середовищі перетворивши всі необхідні параметри на логіко-часові функції (ЛЧФ) [8], яких є три функціонально повні класи, замкнуті відносно булевих операцій, спеціальної операції нерівнозначного віднімання та диференціювання. Наприклад, елементарна ЛЧФ першого класу, що між двома нулями приймає стале значення:

$$f(t,t_1,T_1)=\begin{cases} t-t_1, & якщо\ t_1 < t \le t_1+T_1 \\ 0, & якщо\ \ t_1+T_1 < t \le t_1 \end{cases}, \qquad (1)$$

де t – поточне значення параметра часу, t_1 – часова координата, T_1 – тривалість відрізку існування.

ЛЧФ розглядаються на часовому проміжку $[t_k, t_{k+1}]$, дискретизованому за допомогою Δ- інтервалу (Δ- дискретизації) – мінімального часового інтервалу, довжиною Δ_i ($\Delta_i = t_{i+1} - (t_i + T_i)$), між двома часовими координатами ЛЧФ. Операцію нерівнозначного віднімання ($|k|$), яка базується на Δ- дискретизації, визначають так:

$$f_1(t,t_{11},T_{11},a_1)\,|k|\,f_2(t,t_{21},T_{21},a_2)=\left\{(t-(t_1+i\Delta_i))\cdot|a_{i1}-a_{i2}|, t_1=\min(t_{11},t_{21})\right\}, \qquad (2)$$

де t_{11}, t_{21} — часові координати змінних,

T_{11} та T_{21} - тривалості відрізків існування першої та другої функції,

a_1 та a_2 - відповідні амплітуди,

i - кількість Δ- інтервалів в обраному часовому інтервалі,

Δ_i - тривалість Δ-інтервалу,

a_{i1}, a_{i2} - відповідні амплітуди на i -му Δ-інтервалі.

Результатом цієї операції буде знову ЛЧФ, яку можна назвати нерівнозначною різницею. Надалі, для простоти викладення матеріалу, ЛЧФ будемо позначати $f_i(t)$.

На довільному Δ-інтервалі розбиття ЛЧФ може змінювати своє значення. В таких випадках доцільно коригувати значення відповідної функції. Це коригування ідентичне квантуванню, але для ЛЧФ таке коригування виконується за тією ж координатою, що й дискретизація. У цьому контексті краще використати термін «фільтрація». Тобто, для математичного опису повідомлення використовуються фільтровані функції.

Метою даної статті є розробка можливих варіантів підвищення ефективності захисту доступу до інформації з використанням ідентифікаційної логіко-часової функції.

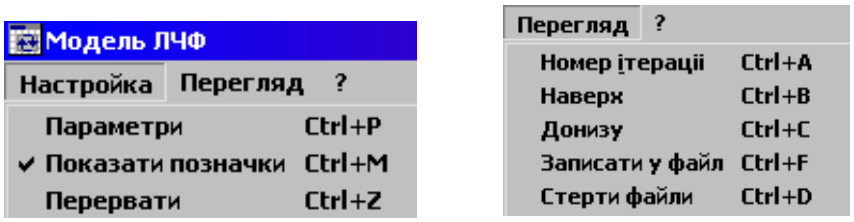
ОСНОВНІ ПОЛОЖЕННЯ

Головною перевагою парольної системи захисту є простота і звичність. Паролі давно вбудовані в системи і сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох підприємств рівень безпеки доступу до інформаційних ресурсів. Однак надійність таких паролів можна значно підвищити, якщо використовувати не звичний набір букв та знаків, а деяке зображення, перетворене на ідентифікаційну логіко-часову функцію [9]. В роботі [8] було розроблено програмне забезпечення (**Модель ЛЧФ**), яке дозволяє виділяти контури довільних зображень, з використанням традиційної математичної операції диференціювання, у вигляді спеціальної логіко-часової функції.

Діалогове вікно програмного забезпечення **Модель ЛЧФ** має рядок заголовку з назвою програми, рядок меню і рядок панелі інструментів. Рядок меню містить два пункти: **Настройка, Перегляд,** що використовуються для управління програмою.

Випадаюче меню **Настройка** включає команди, що не потребують додаткових пояснень і їх дія зрозуміла з назви. Зовнішній вигляд меню **Настройка** зображено на рис. 1а.

Окремого пояснення вимагає меню **Перегляд** (рис. 1б). Воно дозволяє детально розглянути перед друкуванням потрібну нам функцію. Зображення (картинка) може бути записано у файл. Всі попередньо записані файли можна при бажанні стерти.



а) б)

Рис. 1. Зовнішній вигляд меню Настройка та Перегляд

Маємо ще три контекстних меню правої кнопки миші: меню зображення, меню таблиці і графіка. Останнє меню копіює потрібний графік в буфер обміну для подальшого його використання в інших додатках.

Контекстне меню зображення дозволяє вставити зображення з файлу у форматі *.bmp з числом кольорів не більше 256 і розміром 32x32 пікселя. Файл зображення повинен бути розміщений у тій же директорії, що і сама програма. Файл попередньо має бути підготовлений програмою **Paint.**

Для дослідження, напівтонові зображення краще готувати програмою **Photoshop**, та зберегти для **WEB** з необхідними параметрами і перетворити програмою **Paint** в bmp-файл (рис. 2).

Сформувати образ використовується для занесення стартових (вихідних) даних в програму Модель ЛЧФ перед запуском розрахунку.

Порахувати – запустити роботу програми зі сформованими даними.

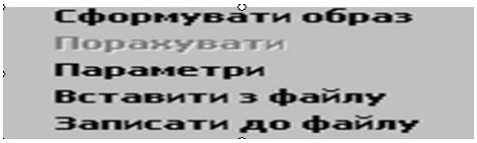


Рис. 2. Контекстне меню зображення

Контекстне меню правої кнопки в режимі таблиці показане на рис. 3.

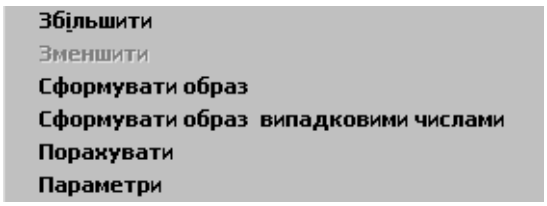


Рис. 3. Контекстне меню таблиці

Збільшити, зменшити – показати всю таблицю чи її частину. Решта пунктів зрозуміла з назви або розглядалась раніше і не потребує додаткових пояснень.

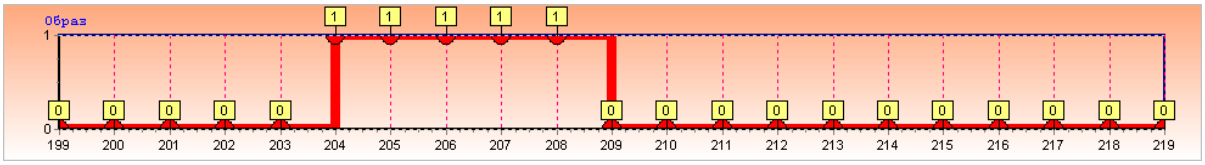
Для прикладу наведемо зображення „кругу" і його другу і сьому похідні та графіки відповідних ЛЧФ (рис. 4).

а) б) в)

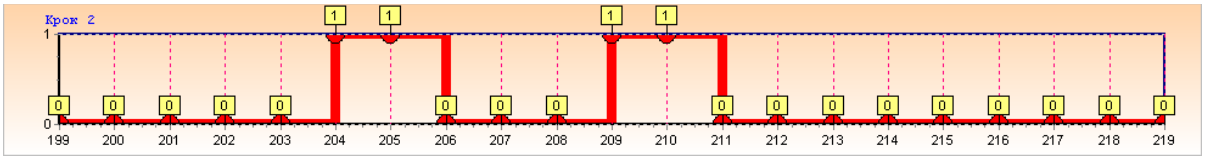
Рис. 4. Приклади моделювання:

а – початкове зображення, б – друга похідна, в – сьома похідна

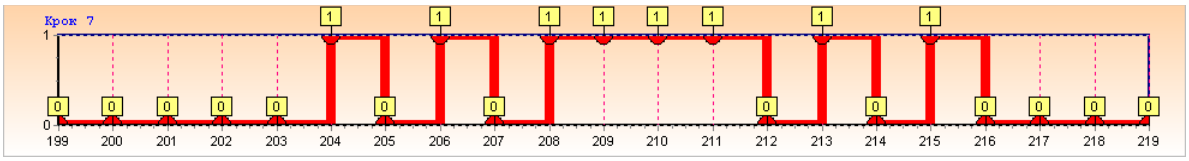
На рис. 5. наведені фрагменти графіків ЛЧФ зображення „круг”.



а)



б)



в)

Рис. 5. Фрагменти ЛЧФ:
а – початкова ЛЧФ, б – друга похідна ЛЧФ, в – сьома похідна

Нумерація пікселів виконана зліва направо і починається з нуля. Горизонтальна смуга прокрутки дозволяє вибрати відповідний фрагмент графіку. Аналогічну операцію можна зробити клацнувши лівою кнопкою миші на відповідному елементі зображення.

Нехай маємо деяку ЛЧФ *k*-значної логіки $f(t,t_1,...,t_m,T_1,...,T_m,a_1,...,a_m)$,

де $t_1,...,t_m$ - часові координати,

$T_1,...,T_m$ - відповідні відрізки існування,

$a_1,...,a_m$ - амплітуди, що відповідають даним відрізкам існування.

Тоді похідна вказаної функції визначається наступним чином:

$$f'(t,t_1,...,t_m,T_1,...,T_m,a_1,...,a_m)=\begin{cases}\left(t-\left(t_k+i\Delta_i\right)\right)\left|a_{k,i+1}-a_{k,i}\right|,\ де\ i-порядковий\ номер\\ \Delta-інтервалу,\ i=\overline{0,\frac{T_k}{\Delta_i}+1},\ k=\overline{1,m}\\ 0,\ якщо\left(t\le t_1\right)\wedge\left(t_k+T_k+\Delta_i<t\le t_{k+1}\right)\wedge\\ \wedge\left(t>t_m+T_m+\Delta_i\right),\ k=\overline{1,m}\end{cases} \quad (3)$$

Зауважимо, що у випадку двійкової логіки формула (3) дещо спроститься, оскільки амплітуди можуть приймати нульове або одиничне значення.

Похідну довільної ЛЧФ можна зобразити графічно (рис. 6).

За необхідності можна посилити виділений контур шляхом повторного диференціювання ідентифікаційної функції.

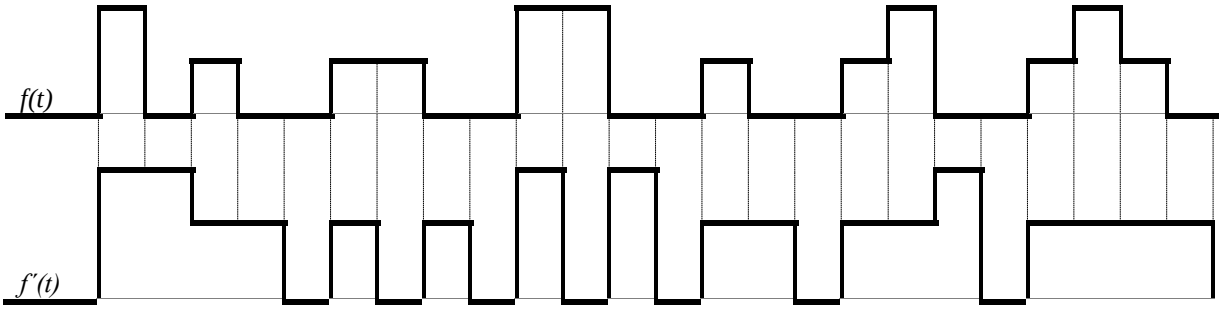


Рис. 6. Можливий варіант графічного знаходження похідної довільної ЛЧФ 3-значної логіки

В якості пароля користувача можна використати будь-яке зображення, відоме лише йому. Причому це зображення може бути як чорно-біле (бінарна ЛЧФ першого та другого класів), так і кольорове (ЛЧФ *k*–значної логіки першого-третього класів). Можна, для більшої складності, об'єднувати декілька картинок у одну ЛЧФ *k*–значної логіки, як результат нерівнозначного віднімання ЛЧФ, які відповідають контуру кожного зображення. Такий пароль у вигляді логіко-часової функції можна використовувати досить тривалий час, оскільки відтворити зображення за функцією-контуром практично неможливо. Більше того, існує можливість математично досліджувати швидкість зміни такого пароля та робити певні прогнози.

Обліковий запис користувача – сукупність ідентифікатора і його пароля. В якості ідентифікатора можна використовувати спеціальну ідентифікаційну логіко-часову функцію, яка є нерівнозначною різницею біометричних ЛЧФ-характеристик суб'єкта, ранжованих за мірою важливості. Ця функція є унікальною для даного користувача і може включати як статистичні, так і динамічні ознаки і властивості. Ідентифікують суб'єкт шляхом порівняння отриманої ідентифікаційної функції з еталонними зразками бази знань. За умови неповної ідентифікації здійснюється розширення бази знань, шляхом запису отриманого результату порівняння в пам'ять в якості нового зразка та визначення найбільш близького до отриманого еталонного зразка. Зазначимо, що системи біометричної ідентифікації – це, по суті, доповнення до стандартної парольної ідентифікації (при вході користувача в систему). Однак в майбутньому прогнозується зниження відсотка парольної ідентифікації до загального числа систем ідентифікації і збільшення питомої ваги систем біометричної автентифікації.

Оскільки біометричні системи можуть працювати в двох режимах: веріфікації, завдання якої звірити відповідність вимірюваної біометричної характеристики записаному шаблону заявленого індивідуума; та ідентифікації, при якій вимірюється біометрична характеристика, що буде порівнюватись з базою раніше записаних шаблонів усіх «відомих» об'єктів, то це значно розширює можливості використання ідентифікаційної ЛЧФ.

Слід відмітити, що в окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Оскільки не існує двох людей з однаковим біометричними характеристиками, то доцільно саме їх використовувати при побудові криптосистеми. Більше того, в ідентифікаційній ЛЧФ можна

використовувати декілька характеристик, ранжованих за важливістю. Порівняльні характеристики найбільш уживаних біометричних систем наведено в таблиці 1.

З точки зору безпеки, помилка хибного допуску є більш суттєвою, ніж помилка хибної відмови, яка впливає лише на зручність користування системою. Слід деталізувати, що до геометрії руки відносять: параметри долоні, рисунок вен, форму долоні. А до геометрії обличчя відносять 2D і 3D моделі та термограму.

Оскільки при виділенні ознак використовується похідна ЛЧФ, яка виділяє контури зображень, то при побудові ЛЧФ-ключа, враховуючи ймовірність несанкціонованого допуску, доцільно використовувати такі 5 характеристик (від кращих до гірших): райдужка ока, сітківка ока, відбиток пальця, розміщення вен на долоні, 3D модель обличчя.

Таблиця 1

Порівняльні характеристики біометричних систем

№	Модель	Біометричний метод	Ймовірність хибної відмови	Ймовірність хибного допуску
1	Eyedentify ICAM	Сітківка ока	0,0001	0,4
2	Iriscan	Райдужка ока	0,0008	0,0007
3	FingerScan	Відбиток пальця	0,0001	1,0
4	BioMet	Геометрія руки	0,1	0,1
5	Vocord (2D)	Геометрія обличчя	0,01	0,2
6	Hitachi VeinID	Вени руки	0,0008	0,01

Причому, ключ відправника може містити його біометричні характеристики, а ключ для розшифровування повідомлення і доступу до інформації – характеристики отримувача.

При побудові ключів криптоалгоритмів з використанням біометричних характеристик необхідно дотримуватись таких правил:

1. Для кожної біометричної характеристики суб'єкта доступу будуємо ЛЧФ $f(t_1,...,t_m,T_1,...,T_m,a_1,...,a_m)$,

   де $t_1,...,t_m$ – часові координати;

   $T_1,...,T_m$ – відповідні відрізки існування;

   $a_1,...,a_m$ – амплітуди, що відповідають даним відрізкам існування;

   з використанням операції диференціювання. Зауважимо, що найкраща характеристика має амплітуду $a=5$ (райдужка ока), а найгірша – $a=1.$
2. Одержуємо ЛЧФ-ключ, як результат нерівнозначного віднімання одержаних в попередньому пункті функцій.
3. Записуємо ЛЧФ-ключ у вигляді полінома, де коефіцієнт біля відповідного ступеня змінної t дорівнює значенню відповідної амплітуди a_i. Зауважимо, що даний ключ можна подати не тільки у вигляді полінома, а і як матрицю амплітуд розмірністю $1\times m$.

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів в базі даних облікових записів: у відкритому виді; у вигляді згорток (хешування); зашифрованими за деяким ключем. Найчастіше застосовують другий і третій способи. Для більшої надійності збереження паролів пропонується зберігати не саму ідентифікаційну ЛЧФ, а відповідний їй поліном [10], тобто шифрування паролів. Наприклад, ЛЧФ другого класу, яка містить два відрізки існування, що не перетинаються між собою (рис. 7), відповідає поліном: $P_6(t)=t^2+t^3+t^6$, а монотонно зростаючій ЛЧФ, що зображена на рис. 8, відповідає поліном: $P_2(t)=t+2t^2$. Слід відмітити, що запис ЛЧФ у вигляді поліномів дозволяє відобразити формалізованим чином операцію циклічного зсуву вихідної ЛЧФ.

Для спрощення зберігання паролів у логіко-часовому середовищі можна використати циклічні коди, оскільки це є ціле сімейство завадостійких лінійних кодів, що забезпечують досить велику гнучкість з точки зору можливості реалізації коду з необхідною здатністю виявлення та виправлення помилок.

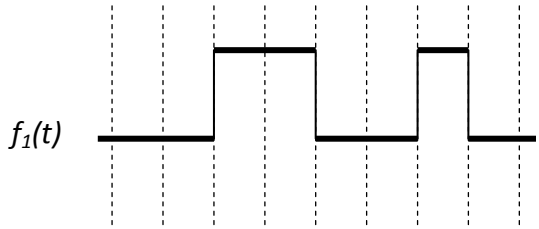


Рис. 7. Можливий варіант ЛЧФ з двома відрізками існування

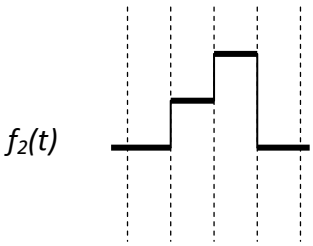


Рис. 8. Можливий варіант зростаючої ЛЧФ

Циклічний код відноситься до систематичних блочних (n, k) кодів, у яких k перших розрядів є комбінацією первинного коду, а наступні $(n-k)$ розрядів є перевірними.

В основі побудови циклічних кодів лежить операція ділення заданої ЛЧФ на породжуючий незвідний поліном ступеня r. Остача від ділення використовується при формуванні перевірних розрядів. При цьому операції ділення передує операція множення, яка здійснює зсув вліво k-розрядної інформаційної кодової комбінації на r розрядів.

Для представлення вихідного повідомлення, переданого у вигляді ЛЧФ, циклічним кодом, дотримуються наступного алгоритму:

1. Подаємо вихідне повідомлення (ЛЧФ) у вигляді поліному $\mathrm{P_r(t)}$.
2. Визначаємо контрольне число Δ-інтервалів (r — порядок поліному повідомлення). Визначаємо відповідно контрольному числу породжуючий поліном $P(t)$.
3. Домножуємо $P_r(t)$ на t^r
4. Ділимо $P_r(t)\cdot t^r$ на породжуючий поліном. Остачу такого ділення позначаємо через $R(t)$.
5. Формуємо поліном кодованого повідомлення $A(t) = P_r(t)\cdot t^r + R(t)$ та будуємо відповідну йому ЛЧФ.

Слід зауважити, що кодоване повідомлення немає помилок (інформація передана правильно), якщо остача від ділення цього повідомлення на породжуючий поліном дорівнює нулю. Операція ділення є звичайним діленням многочленів, однак замість віднімання використовуємо операцію нерівнозначного віднімання.

ВИСНОВКИ

Автентифікацію за рівнем інформаційної безпеки можна поділити на три категорії:

1. статична автентифікація;
2. стійка автентифікація;
3. постійна автентифікація.

Перша категорія забезпечує тільки від несанкціонованих дій в системах, в яких зловмисник може прочитати автентифікаційну інформацію (традиційні постійні паролі). Стійка автентифікація використовує динамічні дані, що змінюються з кожним сеансом роботи (одноразові паролі та електронні підписи). Така автентифікація не забезпечує захист від активних атак. Постійна автентифікація забезпечує ідентифікацію кожного блоку даних, що передаються. Це захищає дані від несанкціонованої модифікації чи вставки.

На основі аналізу загроз інформаційній безпеці та існуючих методів ідентифікації та автентифікації користувачів інформаційних систем, можна стверджувати, що парольний захист сьогодні є одним із найпоширеніших способів захисту доступу до інформації як в окремих комп'ютерах і мережах, так і в мережах світового масштабу. Надійність паролів можна значно підвищити, якщо використовувати деяке зображення, перетворене на логіко-часову функцію. В якості ідентифікатора суб'єкта доступу до інформаційних ресурсів можна використовувати спеціальну ідентифікаційну логіко-часову функцію, яка є нерівнозначною різницею біометричних ЛЧФ-характеристик користувача, ранжованих за мірою важливості.

Спосіб циклічного кодування ідентифікаційних ЛЧФ, що містять усі важливі характеристики переданого повідомлення, значно підвищує захист інформаційної інфраструктури від несанкціонованого доступу. Використання логіко-часового середовища дозволяє передати велику кількість інформації з мінімальною кількістю помилок. Запропонований спосіб циклічного кодування досить легко апаратно реалізувати на базі регістрів зсуву з прямими та зворотними зв'язками.

Унікальність ключів з біометричними характеристиками на базі ідентифікаційних ЛЧФ полягає у неможливості відновлення та читання повідомлення несанкціонованим користувачем, швидкому реагуванні на атаки та достатньо малому часі шифрування та дешифрування та унеможливлює порушення конфіденційності. Ключі з біометричними характеристиками на базі ідентифікаційних ЛЧФ можуть бути використані для підтвердження авторства та мають легку процедуру обміну та просте математичне дослідження, оскільки вони подаються у вигляді поліномів. Можна стверджувати, що досить легко керувати такими ключами у великій мережі.

СПИСОК ЛІТЕРАТУРИ

1. Смит С. (2012). Цифровая обработка сигналов. Практическое руководство для инженеров и научных ра-ботников; пер. с англ. А.Ю. Линовича, С.В. Витязева, И.С. Гусинского. Москва: Додэка XXI.
2. Птіцина Л. А. (2010) Основні підходи до управління інформаційними потоками бізнес діяльності промислових підприємств України. Вісник економічної науки України, 2, 121-124.
3. Русин Б. П., Варецький Я. Ю. (2010) Біометрична аутентифікація та криптографічний захист. Львів: Коло.
4. Галатенко В. А. под ред. академика РАН В. Б. Бетелина (2008) Основы информационной безопасности: учебное пособие, 4-е изд. Москва: Интернет-Университет Информационных технологий; Бином. Лаборатория знаний.
5. Кошева Н. А., Мазниченко Н. І. (2013) Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. Системи обробки інформації, 6 (113), 215-223.
6. Ахрамович В. М. (2016) Ідентифікація й аутентифікація, керування доступом. Сучас. захист інформації, 4, 47-51.
7. Гнідець Т. Я. (2014) Біометрія: сильні та слабкі сторони. Науковий вісник Львівського державного університету внутрішніх справ, 2, 273–282.
8. Сачанюк-Кавецька Н.В., Кожем'яко В.П. (2004) Елементи око-процесорної обробки зображень у логіко-часовому середовищі. Монографія. Університум-Вінниця.
9. Сачанюк-Кавецька Н.В. (2017) Визначення чутливості ідентифікаційної функції до зміни вхідних характеристик обробки зображень для розпізнавання суб'єктів у системах захисту інформації. Реєстрація, зберігання і оброб. даних, 19, 1, 55–64.
10. N. Sachaniuk-Kavets″ka, V. Kozhemiako, W. Wojcik, D. Kassymkhanova, A. Kalizhnova (2015). The use polynomials as a possible variant analytical processing on logic-time functions. Optical Fibers and Their Applications 2015 Proceedings of SPIE, 9816, Lublin, Poland.

REFERENCES

1. Smyt S. (2012). Tsyfrovaya obrabotka syhnalov. Praktycheskoe rukovodstvo dlya ynzhenerov y nauchnykh ra-botnykov; per. s anhl. A.YU. Lynovycha, S.V. Vytyazeva, Y.S. Husynskoho. Moskva: Dodéka KHKHI.
2. Ptitsyna L. A. (2010). Osnovni pidkhody do upravlinnya informatsiynymy potokamy biznes diyal′nosti promyslovykh pidpryyemstv Ukrayiny. Visnyk ekonomichnoyi nauky Ukrayiny, 2, 121-124.
3. Rusyn B. P., Varets′kyy YA. YU. (2010). Biometrychna autentyfikatsiya ta kryptohrafichnyy zakhyst. L′viv: Kolo.
4. Halatenko V. A. (2008). pod red. akademyka RAN V. B. Betelyna Osnovy ynformatsyonnoy bezopasnosty: uchebnoe posobye, 4-e yzd. Moskva: Ynternet-Unyversytet Ynformatsyonnykh tekhnolohyy.
5. Kosheva N. A., Maznychenko N. I. (2013). Identyfikatsiya korystuvachiv informatsiyno-komp″yuternykh system: analiz i prohnozuvannya pidkhodiv. Systemy obrobky informatsiyi, 6 (113), 215-223.

6. Akhramovych V. M. (2016). Identyfikatsiya y autentyfikatsiya, keruvannya dostupom. Suchas. zakhyst informatsiyi, 4, 47-51.
7. Hnidets′ T. YA. (2014). Biometriya: syl′ni ta slabki storony. Naukovyy visnyk L′vivs′koho derzhavnoho universytetu vnutrishnikh sprav, 2, 273–282.
8. Sachanyuk-Kavets′ka N.V., Kozhem″yako V.P. (2004) Elementy oko-protsesornoyi obrobky zobrazhen′ u lohiko-chasovomu seredovyshchi. Monohrafiya. Universum-Vinnytsya.
9. Sachanyuk-Kavets′ka N.V. (2017). Vyznachennya chutlyvosti identyfikatsiynoyi funktsiyi do zminy vkhidnykh kharakterystyk obrobky zobrazhen′ dlya rozpiznavannya sub″yektiv u systemakh zakhystu informatsiyi. Reyestratsiya, zberihannya i obrob. danykh, 19, 1, 55–64.
10. N. Sachaniuk-Kavets″ka, V. Kozhemiako, W. Wojcik, D. Kassymkhanova, A. Kalizhnova (2015). The use polynomials as a possible variant analytical processing on logic-time functions. Optical Fibers and Their Applications 2015 Proceedings of SPIE, 9816, Lublin, Poland.

Надійшла до редакції 04.04.2018

НАТАЛІЯ ВАСИЛІВНА САЧАНЮК-КАВЕЦЬКА – кандидат технічних наук, доцент, кафедра Вищої математики та кафедра Менеджменту безпеки інформаційних систем, Вінницький Національний технічний університет, м. Вінниця, Україна.

ІРИНА ОЛЕКСІЇВНА БОНДАРЕНКО – студентка групи УБ-15б, факультет менеджменту та інформаційної безпеки , Вінницький національний технічний університет, м. Вінниця, Україна.