МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

**ІГНАТОВИЧ АНАТОЛІЙ ОЛЕКСАНДРОВИЧ**

**УДК 004.021:004.027:004.6:004.77**

# МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КОМПОНЕНТІВ БЕЗПЕКИ КОМП’ЮТЕРНИХ СИСТЕМ З ВИКОРИСТАННЯМ МАСКУЮЧИХ ЕЛЕМЕНТІВ ТЕКСТОВИХ ТА БІОМЕТРИЧНИХ ДАНИХ

**05.13.05 – комп’ютерні системи та компоненти**

**АВТОРЕФЕРАТ**
дисертації на здобуття наукового ступеня
кандидата технічних наук

**Львів – 2016**

Дисертацією є рукопис.

Роботу виконано у Національному університеті “Львівська політехніка” Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
**Парамуд Ярослав Степанович,**
доцент кафедри електронних обчислювальних машини Національного університету “Львівська політехніка”.

Офіційні опоненти: доктор технічних наук, доцент
**Рак Тарас Євгенович,**
проректор з науково-дослідної роботи Львівського державного університету безпеки життєдіяльності,
м. Львів

доктор технічних наук, доцент
**Яцків Василь Васильович,**
доцент кафедри інформаційно-обчислювальних систем та управління Тернопільського національного економічного університету,
м. Тернопіль

Захист відбудеться “24” лютого 2017 року о 16 год. на засіданні спеціалізованої вченої ради Д 35.052.08 у Національному університеті “Львівська політехніка” (79013, Львів-13, вул. С. Бандери, 28а, ауд. 711 V навчального корпусу).

З дисертацією можна ознайомитись в бібліотеці Національного університету “Львівська політехніка” за адресою 79013, Львів-13, вул. Професорська, 1.

Автореферат розісланий “23” січня 2017 року.

Учений секретар спеціалізованої
вченої ради Д 35.052.08, д.т.н., проф. Я.Т.Луцик

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми дисертації.** Захист інформації є важливою складовою комп'ютерних технологій. Реалізація сучасних систем інформаційної безпеки покладається на компоненти безпеки комп'ютерних систем та мереж. Компонентами безпеки будемо вважати апаратні та/або програмні засоби комп'ютерних систем та мереж, що забезпечують рівень захищеності інформації, необхідний для конкретного застосування. Вони мають стійкі сфери використання в сучасному інформатизованому суспільстві. Компоненти безпеки реалізовуються за відповідними методами функціонування, алгоритмічно-програмними та схемотехнічними рішеннями. На теперішній час розроблена велика кількість таких рішень.

При конкретному застосуванні треба враховувати витрати на захист інформації та на очікуваний ефект захищеності, тобто знаходити компроміс між вартістю створення і використання компонентів безпеки та необхідною мірою забезпечення інформаційної безпеки. За рівнем очікуваного ефекту захищеності доцільно класифікувати сфери застосування компонентів безпеки, що полегшить пошук конкретного компромісного рішення. Саме найкращий варіант цього компромісу визначає рівень ефективності компонентів безпеки.

Для сфери захисту інформації слід відмітити важливу особливість, що різко виділяє її із загальної царини прикладних напрямків інформаційних технологій. Якість та ефективність пропонованих рішень тут оцінити складно. Усі дослідження стосовно ефективності компонентів безпеки комп'ютерних систем є доцільними, оскільки збагачують базу знань у відповідній сфері та розширюють функціональні можливості при створенні засобів безпеки.

На теперішній час дослідженням методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних приділено недостатньо уваги. Відповідно розробка та дослідження методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних є актуальним науковим завданням.

**Зв'язок роботи з науковими програмами, планами, темами.**

Дисертаційна робота відповідає науковому напряму кафедри електронних обчислювальних машин Національного університету "Львівська політехніка": "Питання теорії, проектування та реалізації комп'ютерних систем та мереж, а також комп'ютерних засобів, вузлів, приладів і пристроїв вимірювальних, інформаційних, керуючих, телекомунікаційних та кіберфізичних систем" та науково-дослідної роботи "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем", шифр ДБ/КІБЕР, реєстраційний номер 0115U000446.

**Мета і завдання дослідження.** *Метою* дисертаційної роботи є розробка та дослідження методів підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та

біометричних даних. Для досягнення поставленої мети необхідне розв'язання наступних задач:

- виконати аналіз сучасного стану розробки та дослідження методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж, визначити особливості застосування маскуючих елементів текстових та біометричних даних;
- розробити та дослідити математичну модель процесу взаємодії користувача із криптографічною системою захисту та біометричний визначник, що демонструє можливості застосування біометрії у ключовій підсистемі;
- розвинути та дослідити метод та алгоритм автентифікації користувачів в комп'ютерних мережах із використанням біометричних даних за відбитками пальців з використанням маскуючих елементів;
- використовуючи засоби статистичного аналізу дослідити характеристики блокових шифрів та можливість використання у компонентах маскуючих елементів для текстових та біометричних даних з метою розширення функціональних можливостей криптосистем;
- дослідити можливість вдосконалення методу шифрування інформації на основі блокових шифрів із використанням маскуючих елементів для текстових та біометричних даних з метою підвищення ефективності компонентів безпеки комп'ютерних систем;
- розробити критерій оцінювання ефективності компонентів безпеки та провести їх тестові дослідження.

***Об'єктом досліджень*** є процес функціонування компонентів безпеки в системах контролю доступу з використанням біометричних даних та в криптографічних системах захисту інформації.

***Предметом досліджень*** є методи та алгоритми підвищення ефективності компонентів безпеки комп'ютерних систем та мереж, які базуються на використанні маскуючих елементів текстових та біометричних даних.

**Методи досліджень.** Під час розв'язання наукових завдань використано основні положення дискретної математики, теорії алгоритмів, теорії ймовірності теорії статистичного аналізу. Використання математичного моделювання та методів тестування комп'ютерних засобів, що надають можливість ідентифікації параметрів, дозволило оцінити ефективність запропонованих засобів.

**Наукова новизна одержаних результатів.**

1. Запропоновано модифікований метод автентифікації користувачів в комп'ютерних мережах як подальший розвиток засобів управління доступом, який полягає у використанні маскуючих елементів біометричних даних за відбитками пальців, та у порівнянні із відомими розширює функціональні можливості методів та засобів автентифікації, що дозволяє поліпшити їх ефективність при використанні за схемою "відкритий ключ користувача – закритий ключ користувача".

2. Вперше запропоновано вдосконалений метод шифрування інформації в компонентах безпеки комп'ютерних систем, який полягає у статичному використанні маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації блоковими криптографічними засобами, та

на відміну від відомих покращує частотний розподіл символів у шифрованому тексті, що дає можливість підвищити ефективність компонентів безпеки;

3. Вперше запропоновано вдосконалений метод шифрування інформації в компонентах безпеки комп'ютерних систем, який полягає у динамічному використанні маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації блоковими криптографічними засобами, який на відміну від відомих покращує частотний розподіл символів у шифрованому тексті та наближує до рівноймовірного, що дає можливість поліпшити ефективність компонентів безпеки;

4. Вперше розроблено та апробовано критерій оцінювання ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних, яких враховує сукупність важливих показників ефективності та у порівнянні із відомими не вимагає значного збільшення обчислювальних ресурсів, що дозволяє отримати узагальнену оцінку ефективності компонентів безпеки.

**Практичне значення одержаних результатів.**

1. На основі аналізу сучасного стану компонентів безпеки комп'ютерних систем та мереж визначені основні напрямки покращення їх ефективності з використанням маскуючих елементів текстових та біометричних даних.

2. Використання запропонованого методу автентифікації користувачів в комп'ютерних системах та мережах на основі біометричних даних за відбитками пальців з маскуючими елементами за схемою "відкритий ключ користувача – закритий ключ користувача" розширює функціональні можливості компонентів безпеки.

3. Шифрування інформації на основі статичного чи динамічного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної системи покращує частотний розподіл символів у шифрованому тексті та ефективність компонентів безпеки.

4. Запропонований критерій оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж на основі блокових шифрів із використанням маскуючих елементів дозволяє отримати узагальнену кількісну оцінку їх ефективності.

5. Основні результати теоретичних досліджень дисертації впроваджено в навчальний процес студентів базового напряму "Комп'ютерна інженерія" Національного університету "Львівська політехніка" у лабораторні практикуми з курсів "Захист інформації в комп'ютерних системах", "Комп'ютерні системи"; при виконанні науково-дослідницького проекту "Удосконалення та розвиток ґрід-кластеру Фізико-механічного інституту ім. Г.В. Карпенка НАН України"; при виконанні науково-дослідницької роботи "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем", шифр ДБ/КІБЕР; при розробці програмного забезпечення компонентів безпеки в міжнародній аутсорсинговій компанії "KindGeek (ТзОВ "КайндГік")".

**Особистий внесок здобувача**. Положення та результати, що виносяться на захист дисертаційної роботи, основний зміст роботи, всі теоретичні та практичні розробки, висновки та рекомендації отримано здобувачем особисто. З праць, опублікованих у співавторстві, використано лише ті положення та ідеї, які є результатом особистих досліджень здобувача.

**Апробація роботи**. Основні теоретичні положення та практичні результати дисертаційної роботи доповідалися і обговорювались на семінарах та конференціях: наукових семінарах кафедри "Електронні обчислювальні машини" Національного університету "Львівська політехніка" (2009-2015); Відкритій науково-технічній конференції молодих науковців і спеціалістів Фізико-механічного інституту ім. Г.В. Карпенка НАН України "Проблеми корозійно-механічного руйнування, інженерія поверхні, діагностичні системи" (м. Львів, 2009); 4-ій Міжнародній науково-технічній конференції ACSN-2009 "Сучасні комп'ютерні системи та мережі: розробка та використання" (м. Львів, 2009); 3-ій Міжнародній конференції молодих учених CSE-2009 (м. Львів, 14-16 травня 2009); 4-ій Міжнародній конференції молодих учених CSE-2010 (м. Львів, 25-27 листопада 2010); IV-ій науково-практичній конференції "Електроніка та інформаційні технології ЕлІТ - 2012", ФМІ НАН України (м. Львів – Чинадієво, 30 серпня -2 вересня 2012); V-ій Всеукраїнській школі-семінарі молодих вчених і студентів АСІТ'2015 "Сучасні комп'ютерні інформаційні технології", ТНЕУ (м. Тернопіль, 22-23 травня 2015); першому науковому семінарі "Кіберфізичні системи: досягнення та виклики" (25-26 червня 2015, м. Львів); 5-му міжнародному форумі молодих науковців "LITTERIS ET ARTIBVS" (м. Львів, 26-28 листопада 2015).

**Публікації.** Основні результати наукових досліджень опубліковано в 17 наукових працях, зокрема: 9 статтях в періодичних наукових виданнях (в тому числі 7 статтях у фахових виданнях та 2 статтях в іноземних виданнях), 8 тезах доповідей на конференціях та семінарах. Отримано 1 патент на корисну модель на новий спосіб шифрування інформації.

**Структура та обсяг дисертації.** Дисертаційна робота складається із вступу, чотирьох розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації складає 143 сторінки основного тексту, в т.ч. 28 рисунків, 3 таблиці. Список використаних джерел складається з 91 бібліографічного найменування. Додатки містять акти про впровадження результатів роботи, лістинги програм, додаткові дані тестових випробувань.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, сформульовано основні завдання та мету роботи. Названо об'єкт, предмет та використані методи дослідження. Визначено наукову новизну та практичну цінність отриманих результатів, показано зв'язок роботи з науковими програмами, планами та темами. Наведені дані про впровадження результатів роботи, її апробацію та особистий внесок здобувача, публікації, обсяг і структуру дисертації.

У **першому розділі** проведено аналіз особливостей побудови існуючих компонентів безпеки комп'ютерних систем та мереж. Наведена класифікація методів ідентифікації та автентифікації. Показана ефективність побудови компонентів безпеки на основі біометричних даних. Наведена класифікація компонентів захисту комп'ютерних систем та мереж за класифікаційною ознакою, що визначає рівень очікуваного ефекту захищеності. Аналіз сучасного стану досліджень ефективності компонентів безпеки комп'ютерних систем та мереж показав, що актуальними та доцільними є дослідження методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних.

У **другому розділі** запропоновано метод автентифікації та алгоритм захисту інформації в комп'ютерних мережах на основі біометричних даних з використанням маскуючих елементів. Акцентовано, що захист комп'ютерних мереж, кіберфізичних систем необхідно виконувати на основі системного підходу, забезпечуючи необхідний рівень захищеності на всіх рівнях – на апаратному, програмному, криптографічному і системному. Низький рівень ефективності на будь-якому рівні може суттєво погіршити загальну захищеність. Перспективним вважаємо метод автентифікації користувача за біометричними даними, в якому важливим етапом є використання індивідуальних ключів. Біометрична інформація про всі десять пальців рук кожного користувача надає можливість адаптувати реалізацію індивідуальних ключів до конкретних особливостей мережі. Адаптацію можна реалізувати використанням різних ключів, рознесених в часі за наперед визначеним розкладом, узгодженим між учасниками повідомлень. Використання різних ключів можна реалізувати за формулою: $A = (C1 * C2) \bmod a$ , де $A$ – номер індивідуального ключа із врахуванням відбитку пальця, $C1, C2$ - ідентифікаційні числа, $a$ – довільне число від 2-х до 10. Ідентифікаційні числа $C1, C2$ можуть бути як випадковими, так і нести наперед визначене інформаційне навантаження. Збільшення числа $a$ розширюєфункціональні можливості автентифікації.

При реалізації методу автентифікації користувача за біометричними даними із вставленням маскуючих елементів доцільно використати модель та алгоритм взаємодії між користувачем та засобами криптографічного захисту. Використовуємо деякий криптографічний примітив, який зв'яже закриті (приватні) ключі користувача мережі з фрагментами даних відбитків пальців. Необхідно створити певний масив даних, які в певний спосіб блокують закриті ключі. Такий процес формування необхідного масиву даних відбувається під час реєстрації нового користувача, або коли існуючий користувач змінює ключ.

Запропонований алгоритм створює з $N$ вхідних наборів фрагментів біометричних даних, блокуючи множину $W = \{w_0,..., w_s\} \subset F$ закритого ключа шифрування $M = \{m_0,..., m_{k-1}\} \subset F$, який записується у вигляді коефіцієнтів полінома $f(x)$ ступеня $k-1$ у полі $F: f(x) = m_1 + m_2 x + ... + m_k x^{k-1}$.

Підвищення криптографічної ефективності алгоритму блокування можна досягнути додаванням до множини $W$ ряду фіксованих фрагментів. Загальна кількість фрагментів буде $r$ (визначається як мінімальне можливе значення відстані $L$ між фрагментами, яка строго більша ніж $2\sigma_s$, де $\sigma_s$ – середня порогова відстань, яка залежить від технології отримання наборів фрагментів).

На виході з алгоритму блокування отриманий набір кортежів $B_P$, який складається з $s$ пар $\{w_i, f(x_i)\}$ і $r-s$ пар фіктивних точок $\{\alpha_i, \beta_i\}$ з $F$, які задовольняють умові $f(\alpha_i) \neq \beta_i$. Щоб відкрити систему, яка використовує $B_P$, зловмисник повинен виявити цей набір точок, що належать многочленові $f(x)$, тобто виявити закритий (приватний) ключ. Очевидно, що чим більше значення $r$, тим більшою буде кількість подібних до $f(x)$ недостовірних (фальшивих) многочленів, а, отже, буде і вища стійкість системи до взлому. Для зареєстрованого (легального) користувача системи потрібно і достатньо представити принаймні $\tau \geq k$ дійсних точок, щоб успішно інтерполювати неявний поліном. Для алгоритму розблокування формується набір $W' \subset F$, в якому міститься тільки частина елементів множини $W$. Таким чином різниця двох наборів фрагментів дорівнює $\#(W - W') = t$. Щоб розблокувати ключ шифрування з $B_P$, користувач надає набір особистих фрагментів, утворюючи відкриваючу множину $W' = \{w_1', ..., w_r'\}$. Розблокування відбувається, коли користувач запитує у системи закритий ключ.

Через $W'$ і $B_P$ видобувається множина $B_P'$ найближчих (із граничною відстанню $\sigma_s$) фрагментів з потужністю $r$, де $r \approx s$ для зареєстрованого (легального) користувача, та $r >> s$ – для незареєстрованого (нелегального) користувача. $k$ є досить важливим параметром, який впливає на ефективність алгоритму.

Треба відмітити, що алгоритм захисту біометричної інформації в ланках автентифікації користувачів у ґрід-середовищі має наступні особливості. Сучасні інформаційні технології надають користувачам широкі можливості щодо збільшення обчислювальних ресурсів. Однією з таких технологій є ґрід – інфраструктури. Питання безпеки при розподіленій та просторово рознесеній організації обчислювальних процесів виходять на передній план. При цьому необхідно розв'язати задачі забезпечення автентифікації, контролю доступу, конфіденційності та цілісності даних. Використання в біометричних даних маскуючих елементів підвищує ефективність розв'язання цих задач.

Зауважимо, що структура сертифікату X.509.v3 пропонує спеціальний механізм біометричних доповнень, що дозволяє зареєструвати у створюваному

сертифікаті необхідну біометричну інформацію. Кожне таке доповнення можна подати у вигляді кортежу

$$F = \{ P, R, Z \},$$

де P – тип використовуваного доповнення; R – прапорець критичності, який вказує чи інформація, яка подана в даному доповненні , повинна бути опрацьована; Z – безпосередньо дані значення, які подаються за допомогою цього доповнення.

Якщо у якості множини блокування та розблокування використовуються, наприклад, дактилоскопічні дані людини, то набором блокування $W$ у цьому випадку є набір координат пікселів, які відповідають місцеположенню ознак на відбитку пальця, тобто $F = GF(n)$, де $n = g^2$ , а $g$ – просте число. Отриманий набір $B_p$ пропонується вносити у спеціальне "біометричне" доповнення сертифікату X.509.v3.

Досліджена модель взаємодії користувача з системою криптографічного захисту має наступні особливості. Довжина ключа в значній мірі визначає стійкість криптографічної системи захисту. Останнім часом при розробці криптографічних систем захисту спостерігається зміщення акцентів у процесах управління ключами до застосування особистих ознак користувача системи, яким притаманні такі властивості: - індивідуальність або неповторність; - стабільність впродовж тривалого періоду; - складність фальсифікації; - неможливість розподілу серед декількох користувачів; - неможливість забути, загубити чи вкрасти. Саме тому створення науково обґрунтованих моделей та методів взаємодії людини (користувача) із системою захисту, використовуючи біометричні дані із маскуючими елементами, підвищує ефективність компонентів захисту.

Основною ідеєю криптографічних систем з біометричним захистом є створення ланок біометричного блокування (розблокування) ключів подібно до ланок парольного захисту ключів. Аналіз алгоритму автентифікації користувачів в комп'ютерних системах та мережах на основі біометричних даних за відбитками пальців з маскуючими елементами дозволяє зробити такі висновки. В 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 $h(w, K)$ – це в певному сенсі аналог криптографічної функції, тобто для різних входів $w$ отримуються різні виходи, а отримання $w$ або $K$ із $h(w, K)$ є важкою проблемою. Результат трансформації $h(w, K)$ носить назву "таємний шаблон", або "скасовувана біометрія". Згідно з такою постановкою задачі, у процесі ідентифікації відбувається трансформація вхідного біометричного сигналу користувача $w'$ та за допомогою функції $h(w, K)$, а процес порівняння здійснюється у просторі відображень.

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

У випадку використання необоротних функцій (хеш-функції, односторонні перетворення), стійкість *h (w, K)* є доведено високою. Однак потрібно враховувати, щоб імовірність відмови в авторизації людині, яка має доступ такої системи (FRR), була мінімальною. Причина – відмінність у послідовності 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) – величина FRR є на рівні звичайної біометричної системи ідентифікації, але безпека біометричних даних є пропорційною до стійкості оборотної функції, тобто знову виникають проблеми, пов'язані з управління ключами. Враховуючи вищевказані проблеми, конкретна конструкція трансформації *h (w, K)* повинна враховувати такі особливості: нечіткість біометричних відображень, відмінності у наданні біометричних даних, відмінності у послідовних зчитуваннях біометричних даних, особливості апаратури та алгоритмів отримання біометричних даних; стабільність біометричних ознак, неможливість зміни або обмежена кількість змін біометричних даних після компрометації, застосування одних біометричних даних у кількох системах захисту; вразливість до атак з використанням "троянських коней".

Досліджено процес захисту криптографічних ключів з використанням математичної моделі визначника випадкових величин. Для моделювання процесу захисту криптографічних ключів класичними парольними методами використовується математична модель визначника випадкових величин, яка описує процеси квазівипадкових бітів, тобто бітових послідовностей, які жодним поліноміальним алгоритмом неможливо відрізнити від рівномірно розподілених послідовностей такої ж довжини. Відомими реалізаціями визначників є важкооборотні функції та генератори псевдовипадкових бітів.

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

Біометричний визначник враховує проблему стабільності біометричних даних, а саме дозволяє поставити у відповідність до біометричних даних один або більше випадково вибраних ключів. Біометричний визначник при заданих умовах зводиться до "чіткого". Для врахування проблеми нечіткості введено поняття біометричного ідентифікатора. Біометричний ідентифікатор відображає вхідні біометричні дані у певну структуру, яка нечутлива до визначеного рівня змін у біометричних даних. Відповідно біометричний визначник це складена конструкція - побудована з біометричного ідентифікатора та чіткого визначника.

Результати досліджень реалізовано та використано у ґрід-кластері Фізико-механічного інституту.

У **третьому розділі** отримали подальший розвиток методи шифрування інформації із використанням маскуючих елементів на основі блокових шифрів. Такі шифри виконують процедуру шифрування блоку символів за один цикл і

основна особливість така, що один і той символ в різних блоках по змісту буде шифруватися по-різному. Одні із показників ефективності криптосистеми визначається трудомісткістю і часом, який затрачується на шифрування та дешифрування тексту. Надійність криптосистеми визначається часом, який зловмисник затратить для того щоби розкрити алгоритм шифрування і дешифрування і знайде ключ шифру. До блокових шифрів відносяться такі шифри: шифр мережа Фейстеля, шифр Хілла, шифр Віженера, шифр RSA та інші. Шифр мережа Фейстеля, шифр RSA, DES – це сучасні комп'ютерні шифри, їх переваги і якості відомі. Майже всі відомі шифри мають свою методику злому. При застосуванні криптографічних методів захисту інформації необхідно визначити зловмисника (особу, чи організацію) від кого ми передбачаєм захистити інформацію. Важливо не тільки правильно вибрати шифр і ключ шифрування, не менш важливо приховати використаний шифр. Пошук нових алгоритмів і способів шифрування текстової інформації виконувався в напрямках використання маскуючих елементів для підвищення ефективності шифрів і приховування використаного методу шифрування.

Найбільш наглядно застосування маскуючих елементів у текстових даних компонентів безпеки демонструється для блокового шифру Хілла. Шифрування інформації відбувається за наступною процедурою: $C_i = A * B_i$, де $C_i$ - матриця-стовпчик і-того блоку шифрованого тексту (ШТ), А – матриця-ключ для шифрування інформації; $B_i$ – матриця-стовпчик і-того блоку відкритого тексту (ВТ). Розшифрування інформації реалізовується за наступною процедурою: $B_i = A^{-1} * C_i$, де $A^{-1}$ - обернена матриця-ключ для розшифрування інформації; $B_i$ – матриця-стовпчик і-того блоку відкритого тексту; $C_i$ - матриця-стовпчик і-того блоку шифрованого тексту. Ключем є матриця, яка представляється словом, чи довільним набором букв. Для шифрування використовується числова квадратна матриця (3х3, 4х4, 5х5, 6х6,...). Щоб розшифрувати повідомлення, необхідно звернути шифрований текст назад у вектор, а потім – помножити на обернену матрицю ключа.

Запропоновано на першому етапі процедури шифрування перед (або після) визначеними символами ВТ вставляти додаткові маскуючі елементи. Необхідно вставляти таку кількість маскуючих елементів, щоби в кожний блок шифрування потрапляв хоча би один маскуючий елемент. Маскуючі елементи вибираються керованим генератором псевдовипадкових чисел таким чином, щоби статистичний аналіз ВТ до вставлення і після вставлення маскуючих елементів змінювався в сторону рівномірної частоти вживання символів. Якщо при перемноженні у матрицю символів ВТ вставляється хоча би один маскуючий елемент, то при перемноженні змінюються всі результуючі символи ШТ. Запропонований спосіб шифрування інформації нескладно реалізується апаратним, програмним або комбінованим способом.

За необхідності отримати високі показники ефективності компонентів безпеки, забезпечити наближений до рівномірного розподіл частоти символів у ШТ необхідно вставляти достатньо маскуючих елементів, кількість яких може перевищувати кількість символів відкритого тексту. Загальний алгоритм вставлення маскуючих елементів у ВТ подано на рис. 1.


Рис.1. Алгоритм вставлення маскуючих елементів у ВТ

Розглянемо алгоритм вставлення маскуючих елементів: вставляється один маскуючий елемент перед кожним символом ВТ і один маскуючий елемент після символу ВТ. В цьому випадку ВТ з маскуючими елементами буде мати таку конфігурацію: в кожному блоці (якщо $\boldsymbol{\mu} = 3$) буде один маскуючий елемент перед символом ВТ, символ ВТ і один маскуючий елемент після символу ВТ. Блок має такий вигляд*:* $\{m_i; v_i; m_i;\}$, де $m_i$ – маскуючий елемент, $v_i$ – символ ВТ. Якщо конфігурація ВТ з маскуючими елементами буде така, що розглядалася вище, а $\boldsymbol{\mu} = 4$, тоді блоки будуть мати такий вигляд: перший - $\{m_i; v_i; m_i; m_i;\}$, другий - $\{v_i; m_i; m_i; v_{i;}\}$, третій - $\{m_i; m_i\, v_i; m_i;\}$, четвертий - $\{m_i; v_i; m_i; m_i\}$, п'ятий - $\{m_i; v_i; m_i; m_i;\}$, такий як перший і весь цикл з періодом чотири буде повторюватися.

Приймемо інший алгоритм вставлення маскуючих елементів: вставляється два маскуючі елементи перед кожним символом ВТ і нуль маскуючих

елементів після символу ВТ при **μ** = 3. В цьому випадку блок має такий вигляд *:* *{$m_i$; $m_i$; $v_i$;},* де $m_i$ – маскуючий елемент, $v_i$ – символ ВТ.

Запропоновано декілька методів вставлення маскуючих елементів – вибирати їх з можливого набору, які визначаються нерівномірністю статистичної характеристики розподілу символів за принципом: кожний маскуючий елемент, який вставляється, повинен покращувати рівномірність статистичної характеристики розподілу символів ВТ, до якого добавляються маскуючі елементи.

Розглянемо статичний метод вставлення маскуючих елементів - маскуючі елементи завжди вставляються у наперед визначені місця відносно символів відкритого тексту. Наведені три варіанти статичного методу вставлення маскуючих елементів для формату **μ** = 3: 1 - *{$v_i$; $v_i$; $m_i$;},* 2 - *{$v_i$; $m_i$; $v_i$;},* 3 - *{ $m_i$; $v_i$; $v_i$;},* де $m_i$ – маскуючий елемент, $v_i$ – символ ВТ. Один із варіантів графічної статичної моделі наведено на рис. 2.

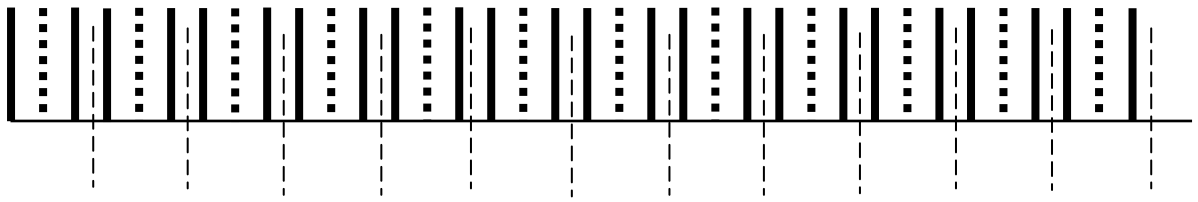

Рис. 2. Варіант графічної статичної моделі з форматом {$v_i$; $m_i$; $v_i$;}, де $m_i$ – маскуючий елемент - пунктирна лінія, $v_i$ – символ ВТ - відтин лінії. Блоки розділені штрихованими лініями. Довжина блоку – 3 символи.

Динамічний метод вставлення маскуючих елементів – маскуючі елементи вставляються за кількістю і на позиції в залежності від номера символу відкритого тексту і їх кількість буде мінятися на кожному раунді процедури вставлення. Дослідження виконувались для формату **μ** = 5. Після кожного символу ВТ вставляється обчислена кількість маскуючих елементів згідно з формулою *{ $v_i$ + [ $n_j$ mod 5 ] * $m_i$;},* де $n_j$ - порядковий номер символу ВТ. Досліджені як статичні, так і динамічні моделі вставлення маскуючих елементів. Фрагмент графічної динамічної моделі приведено на рис. 3.

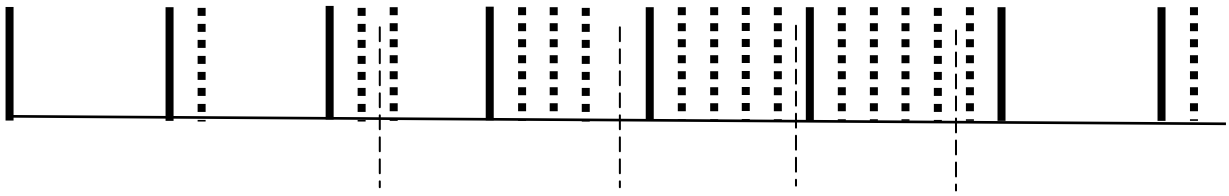

Рис.3. Фрагмент графічної динамічної моделі з форматом {$v_i$; $n_j$*$m_i$;}, де $m_i$ – маскуючий елемент - пунктирна лінія, $v_i$ – символ ВТ - відтин лінії. , $n_j$ – коефіцієнт поступово змінюється від 0 до 5 (в залежності від порядкового номеру символу ВТ $v_i$). Блоки розділені штрихованими лініями. Довжина блоку – 5 символів.

Динамічна функція вставлення маскуючих елементів дає додатковий ефект. Якщо у звичайному шифрі Хілла повторення в тексті можуть появлятися на відстанях, які кратні довжині ключа (число **μ** не може бути дуже велике), то

у вставлянні маскуючих елементів після кожного символу відкритого тексту у кількості від 0 до 5 при **μ** = 5 період повторення буде 105 символів (було 5). Можна використати наступний поліном для розрахунку місця і кількості вставлення маскуючих елементів:

$$N = ( n_1 + n_2 * z + n_3 * z^2 + \ldots + n_k * z^{k-1} ) \bmod \mu,$$

де $N$ – кількість маскуючих елементів, які вставляються після $z_i$ – го символу відкритого тексту, $n_i$ – коефіцієнти поліному, **μ** – довжина блоку (формат шифрування).

Сама процедура вставлення маскуючих елементів і їх вилучення є процедурою, яка не зменшує продуктивність роботи криптографа. При цьому маскуючі елементи підбираються з допомогою генератора випадкових чисел з найменш вживаних символів у тексті. Такий алгоритм підбору маскуючих елементів можна рахувати додатковим ключем для формування ШТ.

Складність вилучення маскуючих елементів не визначається їх номером чи назвою, так як вилучаються символи на відповідних позиціях ШТ. Якщо кількість маскуючих елементів становить більше 50%, тоді частотний розподіл символів у шифрованому тексті наближається до рівноймовірного. Використання маскуючих елементів має перспективу в напрямку створення шифрів підвищеної ефективності, які достатньо просто реалізовуються на сучасних комп'ютерних засобах.

Розшифрування ШТ, не маючи ключа, методом перебору всіх можливих варіантів ключа передбачає отримати ВТ, який читається. Якщо зловмисники переберуть всі можливі варіанти ключа, вони не отримають ВТ, який читається, оскільки відбувалася модифікація ВТ перед шифруванням. Основні інструменти криптоаналітика – аналіз статистичних характеристик шифрованого тексту і аналіз повторень ШТ. В запропонованому методі шифрування вирішальним є спотворення інформації про повторення, які могли би повторитися у ШТ по аналогії з ВТ. І ця задача успішно вирішується у запропонованому блоковому шифрі з використанням маскуючих елементів. Тому ця особливість, разом з вирівнянням статистичних характеристик, забезпечує скриття використаного методу шифрування, що має важливий ефект.

Середнє інтегральне відхилення частотного розподілу символів у шифрованому тексті досліджено та визначено за допомогою запропонованої в роботі формули:

$$\sigma = \left[ \frac{1}{2} \sum_{i=1}^{n} \frac{(x_{i\max} - x_i)}{x_{i\max}} \right] * 100\%, \qquad (1)$$

де $x_i$ – статистичний параметр для і-того символу тексту, який виражається у кількості випадків використання символу у досліджуваному тексті; $x_{imax}$ – максимальне значення $x_i$ для символу, який найчастіше зустрічається у досліджуваному тексті.

Розроблено та досліджено графічні моделі для статичного та динамічного методів вставлення маскуючих елементів для формату μ = 3. Середнє статистичне інтегральне відхилення частотного розподілу символів у шифрованому тексті методом Хілла без маскуючих елементів рівне 27,3%, а для

шифрованого тексту з статичним вставленням маскуючих елементів рівне 19,6%. Покращення майже в 1,4 рази частотного розподілу символів у шифрованому тексті свідчить про підвищення ефективності методу шифрування інформації в компонентах безпеки комп'ютерних системах статичним вставленням маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації блоковими криптографічними засобами. Метод шифрування інформації в компонентах безпеки комп'ютерних системах динамічним вставленням маскуючих елементів дозволяє покращити до двох разів частотний розподіл символів у шифрованому тексті.

У **четвертому розділі** наведені практичні результати досліджень методів та моделей покращення ефективності компонентів безпеки в комп'ютерних системах та мережах.

Запропонований модифікований метод автентифікації користувачів в комп'ютерних мережах із використанням маскуючих елементів в біометричних даних за відбитками пальців досліджено на ґрід-кластері Фізико-механічного інституту. Використано модель та алгоритм взаємодії між користувачем та засобами криптографічного захисту. Запропонований метод автентифікації у порівнянні із відомими розширює функціональні можливості засобів автентифікації, що дозволяє поліпшити їх ефективність при використанні за схемою "відкритий ключ користувача – закритий ключ користувача".

Досліджено особливості біометричної інформації в структурі сертифікату X.509.v.3 та механізм доповнень/розширення, що дозволяє зареєструвати у створюваному сертифікаті необхідну біометричну інформацію. Зокрема, є можливість реєстрації розширень у відповідних інституціях. Система безпеки ґрід-системи використовує хеш-дані п'яти відбитків пальців на одного користувача, кожен елемент даних розміщений в окремому атрибуті Authenticationlnfo. Це дозволяє алгоритмові автентифікації, використовуючи зазначену інформацію, перевірити атрибути і обрати відповідні.

Ефективність запропонованих методів шифрування текстових даних із використанням маскуючих елементів досліджена тестовими засобами. Якість шифрованого за запропонованими методами одного із прикладів відкритого тексту досліджена тестами NIST USA (The National Institute of Standards and Technology). Для тестування використано шифр, отриманий запропонованим способом шифрування з маскуючими елементами, які вставлялися динамічним способом (кількість маскуючих елементів мінялася від 0 до 5, $\{v_i; (n_i \bmod 5)*m_i\}$, формат шифрування $\boldsymbol{\mu} = 4$). Якість шифрування перевірялася за допомогою чотирьох основних тестів.

Отримано та досліджено шифрований текст та його бінарний код (наведено в дисертації). Перевірка шифрованого тексту за допомогою чотирьох основних тестів комплексного тесту NIST дала наступні результати.

1. *Частотний побітовий тест.* Для шифрованого тексту визначаємо загальну довжину бінарного коду N = 8500 та величину S=214, що вказує, на стільки одиниць в бінарному коді більше за нулів. Отримана узагальнена характеристика цього тесту для шифрованого тексту: $P_{value1}$ =0.0202559 > 0,01. Отримане значення вказує, що частотний побітовий тест успішно пройдений.

2.*Частотний блочний тест.* Шифрований текст за умовами тесту розбивається на 10 блоків по 850 бітів. Отримана узагальнена характеристика цього тесту для шифрованого тексту: $P_{value2}$ =0.176 > 0,01. Отримане значення вказує, що частотний блочний тест успішно пройдений.

3.*Тест на біти, що ідуть підряд.* Отримана узагальнена характеристика цього тесту для шифрованого тексту: $P_{value3}$ =0.176 > 0,01. Отримане значення вказує, що тест на біти, що ідуть підряд, успішно пройдений.

4.*Тест на найдовшу послідовність із одиниць у блоці.* Шифрований текст за умовами тесту розбивається на 50 блоків по 170 символів. Отримана узагальнена характеристика цього тесту для шифрованого тексту: $P_{value4}$ =0.9063 > 0,01. Отримане значення вказує, що тест на найдовшу послідовність із одиниць у блоці успішно пройдений.

Успішне проходження чотирьох основних тестів NIST вказує на високі показники ефективності методів шифрування текстових даних із вставленням маскуючих елементів.

Досліджені на моделях статистичні характеристики шифрованого тексту при використанні статичного і динамічного методу встановлення маскуючих елементів. Формат запропонованого методу – 4х4, (**μ** = 4). Моделювання виконувались для статичного методу з вставленням одного маскуючого елементу в блок. Розглянуто різні варіанти формату блоків. Середньоквадратичне відхилення частоти використання символів у шифрованому і відкритому текстах розраховувалося за формулою (1). Результати моделювання показали покращення показника $\sigma$ на величини 27,7 % -35,5%.

Досліджена динамічна графічна модель з форматом $\{v_i; n_j*m_i;\}$, де $m_i$ – маскуючий елемент, $v_i$ – символ ВТ, $n_j$ – коефіцієнт динаміки, що поступово змінюється від 0 до 5 (в залежності від порядкового номеру символу ВТ $v_i$). Формат шифрування – 4х4, (μ = 4).

Динамічна функція вставлення маскуючих елементів дає додатковий ефект. Якщо у звичайному блоковому шифрі повторення в тексті можуть появлятися на відстанях, які кратні довжині ключа (число **μ** не може бути дуже велике), то у встановленні маскуючих елементів після кожного символу відкритого тексту у кількості від 0 до 5 при μ = 4 період повторення буде 84 символи, що виявлено при аналізі графічної моделі. Середнє інтегральне відхилення при шифруванні запропонованим методом покращилося на 60%.

Метод вставлення маскуючих елементів можна використовувати і у випадку використання таких блокових шифрів як мережа Фейстеля, шифр Віженера та інших. Досліджено, що середнє інтегральне відхилення шифрованого тексту методом Віженера з маскуючими елементами, вставленими статичним методом, зменшується у 1,4 рази, а інтегральне відхилення шифрованого тексту методом Фейстеля з маскуючими елементами, вставленими статичним методом, зменшується середньостатистично у 1,3 рази.

Оцінювання ефективності доцільно виконувати для однотипних компонентів безпеки комп’ютерних систем, так як воно може надати найбільш об’єктивні результати. Складність задачі – знайти універсальний підхід для визначення ефективності полягає в тому, що при формуванні оцінки є

необхідність об'єднати в один критерій різні параметри за природою, розмірністю, фізичними величинами.

На теперішній час відсутній загальноприйнятий та уніфікований аналітичний вираз для обчислення критерія ефективності компонентів безпеки комп'ютерних систем. Одним із варіантів такої оцінки запропоновано вираз:

$$E = \left(\sum_{j=1}^{n} E_j\right) : n,\ j = \overline{1,n}$$

де $E_j$ – параметр, який визначається як відносна нормована величина j – го показника ефективності, що може прямувати до максимального значення 1; Нормований показник ефективності можна обчислити за виразом: $E_j = E_{jo} : E_{jm.}$ де $E_{jo}$ – оцінений j – ий показник ефективності для конкретного засобу безпеки; $E_{jm}$ – максимальне (чи оптимальне) значення j – го показника ефективності.

До найбільш поширених показників ефективності компонентів безпеки можна віднести наступні: $E_1$ – надійність використаних засобів, $E_2$ – стійкість криптографічних засобів, $E_3$ – продуктивність при роботі з засобами безпеки, $E_4$ - оцінка зменшення середнього інтегрального відхилення частоти вживання символів для запропонованих засобів захисту, $E_5$– ймовірність зменшення частоти повторень в шифрованому тексті, які відповідають повторенням відкритого тексту, $E_6$ – кількість можливих варіантів ключів, $E_7$ – відношення вартості засобів безпеки до вартості захищеного продукту.

При оцінюванні ефективності можна виключати деякі параметри, які не мають великої ваги для конкретної ситуації, або добавляти більш важливі. Доцільно розглядати різні підходи зі зведенням параметрів, які впливають на ефективність, до одного логічного ряду. Ці підходи (нормованість показників ефективності, різні залежності, "дзеркальна інверсія", "мультиплікативна інверсія", вживання рівнів пріоритету, використання методу експертних оцінок) дають можливість оцінювати в одному ряді величини, які на перший погляд несумісні. При використанні одних і тих засобів захисту в різних умовах експлуатації їх критерій ефективності буде відрізнятися. Пріоритети повинен надавати замовник, котрий їх використовує, і його вимоги є переважаючими. З урахуванням пріоритетів замовника критерій ефективності засобів безпеки можна оцінювати за запропонованим у роботі виразом:

$$E = \left(\sum_{j=1}^{n} P_j \cdot E_j\right) : n,\ j = \overline{1,n}$$

де $p_j$ – рівень пріоритету замовника ($p_j$ може мінятися від 0 до 1 і надавати перевагу тим показникам ефективності, які є найбільш пріоритетними); n – кількість врахованих показників.

Визначення ефективності є найбільш об'єктивним при порівнянні оцінюючого засобу з відомим засобом шифрування (аналогом). При цьому є деякі початкові умови, які бажано виконати. Це однаковий відкритий текст, алгоритми шифрування одного класу, використання аналогічних технічних засобів (комп'ютери, операційні системи, прикладні програми).

Для визначення ефективності пристрою шифрування з маскуючими елементами в якості аналога використано пристрій, який використовує класичний метод шифрування Хілла з форматом і ключем, які використані в досліджуваному пристрою, а також однаковими рівнями пріоритету.

Оцінено ефективність пристрою шифрування з маскувальними символами (формат 3х3, режим використання маскувальних символів статичний, формат $\{v_i; m_i; v_i;\}$ за такими параметрами: $E_1$ – надійність використаних засобів, $E_2$ – стійкість криптографічних засобів, $E_3$ – продуктивність користувача при роботі з засобами безпеки, $E_4$ - оцінка зменшення середнього інтегрально відхилення частоти вживання символів для запропонованих засобів захисту. $E_5$– ймовірність зменшення частоти повторень символів в шифрованому тексті, які відповідають повторенням відкритого тексту.

За отриманими розрахунками у відповідності із запропонованим критерієм для компоненту безпеки, що використовує статичне вставлення маскуючих елементів, узагальнений критерій ефективності $E_m = 0,5014$, а для компоненту безпеки, що використовує класичний метод шифрування Хілла, узагальнений критерій ефективності $E_a = 0,3778$. Порівняння критеріїв ефективності $E_a$ та $E_m$ показує на підвищення ефективності методу шифрування з маскуючими елементами у порівнянні з класичним методом шифрування Хілла у 1,327 рази або на 32,7 %. Наведені оцінки показують тенденцію покращення ефективності запропонованих компонентів безпеки у порівнянні із аналогом.

Додатково необхідно враховувати, що запропоновані засоби розширюють функціональні можливості при виборі чи побудові компонентів безпеки для конкретних застосувань та відповідно покращують їх ефективність. Запропоновані підходи та формули стосовно визначення ефективності можна використати для різних засобів захисту.

## ОСНОВНІ РЕЗУЛЬТАТИ І ВИСНОВКИ РОБОТИ

За результатами аналізу особливостей застосування компонентів безпеки в комп’ютерних системах та мережах встановлена доцільність проведення постійних досліджень щодо підвищення їх ефективності.

У дисертаційній роботі вирішене наукове завдання з розробки та дослідження методів підвищення ефективності компонентів безпеки комп’ютерних систем із використанням маскуючих елементів текстових та біометричних даних. При цьому отримано такі основні результати :

1. На основі аналізу сучасного стану застосування компонентів безпеки комп’ютерних систем та мереж визначені основні напрямки покращення їх ефективності з використанням маскуючих елементів текстових та біометричних даних.
2. Запропоновано модифікований метод автентифікації користувачів в комп’ютерних мережах як подальший розвиток засобів управління доступом, який полягає у використанні маскуючих елементів в біометричних даних за відбитками пальців, та у порівнянні із відомими розширює функціональні можливості методів та засобів автентифікації, що дозволяє поліпшити їх ефективність при використанні за схемою “відкритий ключ користувача – закритий ключ користувача”
3. Вдосконалено метод шифрування інформації на основі статичного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної

системи, що покращує частотний розподіл символів у шифрованому тексті, розроблено та досліджено відповідні графічні моделі, підтверджена ефективність тестовими випробуваннями.

4. Вдосконалено метод шифрування інформації на основі динамічного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної системи, що покращує частотний розподіл символів у шифрованому тексті та наближує до рівноймовірного, розроблено та досліджено відповідні графічні моделі, підтверджена ефективність тестовими перевірками.

5. Розроблено та апробовано новий критерій оцінювання ефективності блокових шифрів, в яких використовуються маскуючі елементи, на основі врахування основних важливих показників ефективності компонентів безпеки, який надає можливість отримати узагальнену оцінку та у порівнянні із відомими забезпечує покращення якості оцінювання ефективності.

## СПИСОК ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ігнатович А.О. Концепція застосування модифікованих блокових шифрів у телекомунікаційних середовищах кіберфізичних систем/ А. О. Ігнатович // Вісник Національного університету "Львівська політехніка" серія “Комп’ютерні системи та мережі”. – 2015. – № 830. – С. 40 – 51.
2. Варецький Я. Модель взаємодії користувача із системою криптографічного захисту/ А. Ігнатович, Я. Варецький // Збірник праць. Вісник Львівського державного університету безпеки життєдіяльності МНС України, 2007. – С. 143 - 149.
3. Ігнатович А.О. Підходи до фільтрації спотворених гаусівським шумом зображень/ А.О. Ігнатович, Я.С. Парамуд, О.В. Капшій// Вісник Національного університету “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2007. -№603. - С.53-58.
4. Ігнатович А.О. Метод адаптивної автентифікації користувачів в комп’ютерних мережах на основі біометричних даних / А.О. Ігнатович // Вісник Національного університету “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2014. -№806. – С.78-82.
5. Ігнатович А.О. Моделі підвищення ефективності та надійності блокових шифрів/ А.О. Ігнатович, Н.Я. Павич // Збірник наукових праць. Вісник Львівського державного університету безпеки життєдіяльності МНС України, 2015.- №11. – С.101-110.
6. Ігнатович А.О. Методи шифрування інформації із використанням маскуючи символів / А.О. Ігнатович, Я.С. Парамуд // Вісник Національного університету “Львівська політехніка”. Збірник наукових праць. Серія “Комп’ютерні науки та інформаційні технології”. – 2015.- № 826. - С. 21 – 27.
7. Ігнатович А.О. Критерій ефективності для визначення стійкості блокових шифрів / А.О. Ігнатович //Вісник Хмельницького національного університету, серія: Технічні науки. -2015. – Вип.3.- №225. - С.233-236.

8. Varectskyy J., Rusyn B., Molga A. and Ignatovych A. A New Method of Fingerprint Key Protection of Grid Credential.- Advances in Intelligent and Soft Computing. Springer – Verlag Berlin Heidelberg. – 2010. –P. 99-104.
9. Warecki J., Rusyn B., Ignatowych A. Biometric data embedding in X.509 certificates for grid systems // Informatyka w dobie XXI wieku. Technologie informatyczne w nauce, technice i edukacji. Politechnika Radomska im. Kazimierza Putaskiego. Radom, 2009 – p. 181 – 183.
10. Патент України на корисну модель №99073, "Спосіб шифрування інформації", заявка №a201500619 від 26.01.2015, Ігнатович А.О., Іванців В. Р., Іванців Р-А. Д., Павич Н. Я., опубліковано бюлетень № 9 від 12.05.2015р.
11. Ігнатович А. Математична модель взаємодії з криптографічною системою захисту/ Анатолій Ігнатович // Комп'ютерні науки та інженерія: Матеріали 3-ої Міжнародної конференції молодих учених CSE-2009. – Львів, 14-16 травня 2009. – С.139-143.
12. Ігнатович А. Алгоритм захисту біометричної інформації в ланках автентифікації користувачів у ҐРІД-середовищі / Анатолій Ігнатович // Сучасні комп'ютерні системи та мережі: розробка та використання. Матеріали 4-ої Міжнародної науково-технічної конференції ACSN-2009. – Львів, Україна., 9-11 листопада, 2009. – С.79-80.
13. Варецький Я. Особливості застосування біометричної інформації в ланках аутентифікації грід-середовища/ Я. Варецький, А. Ігнатович, // "Проблеми корозійно-механічного руйнування, інженерія поверхні, діагностичні системи" - Матеріали відкритої науково-технічної конференції молодих науковців і. спеціалістів Фізико-механічного інституту ім.. Г.В.Карпенка НАН України. - Львів.- 2009. –С.287-289.
14. Ігнатович А. Алгоритм біометричного захисту ключів мандатів безпеки грід-середовища. / Анатолій Ігнатович // Комп'ютерні науки та інженерія: Матеріали IV-ої Міжнародної конференції молодих учених CSE-2010. – Львів, 25-27 листопада 2010. – С. 378-379.
15. Варецький Я.Ю. Результати та особливості удосконалення і використання грід-кластеру Фізико-механічного інституту / Я.Ю. Варецький, Б.П. Русин, О.В. Капшій, В.В. Корній, А.О. Ігнатович. // Електроніка та інформаційні технології (ЕлІТ – 2012) – Матеріали IV-ої науково-практичної конференції. ФМІ НАН України. –Львів – Чинадієво, Україна. - 30.08.-2.09.2012.
16. Ignatowych A., Effectiveness evaluation of modified block ciphers using standardized NIST statistical tests / A. Ignatowych // 5th Interntional Youth Science Forum "LITERIS ET ARTIBUS" – Lviv Polytechnic Publishing House. – Lviv, Ukraine. - 26 – 28.11.2015. – P. 76.
17. Глухова О.В. Критерій ефективності для визначення стійкості блокових шифрів на основі внесених змін статистичних характеристик шифрованого тексту / О.В. Глухова, А.Я. Лозинський, Р.І. Яремкевич, А.О. Ігнатович // ACIT'5. "Сучасні комп'ютерні інформаційні технології". ТНЕУ. - Тернопіль. 22-23 травня 2015. – С. 167-168.
18. Ігнатович А. О. Моделі застосування модифікованих блокових шифрів у кіберфізичних системах / А. О. Ігнатович // Кіберфізичні системи досягнення та

виклики : матеріали І Наукового семінару, 25–26 червня 2015 року, Львів / Національний університет “Львівська політехніка”. – Львів : НВФ “Українські технології”, 2015. – С. 144–149.

## АНОТАЦІЯ

**Ігнатович А.О. Методи підвищення ефективності компонентів безпеки комп’ютерних систем з використанням маскуючих елементів текстових та біометричних даних. –** На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – “Комп’ютерні системи та компоненти”. - Національний університет “Львівська політехніка” Міністерства освіти і науки України. – Львів, 2016.

Дисертаційне дослідження присвячується підвищенню ефективності компонентів безпеки комп’ютерних систем та мереж і визначені основні напрямки покращення їх ефективності на основі використанням маскуючих елементів текстових та біометричних даних. Отримав подальший розвиток метод автентифікації користувачів в комп’ютерних мережах на основі біометричних даних за відбитками пальців з використанням маскуючих елементів – фіктивних частинок. Запропоновано алгоритм біометричного захисту для процедур автентифікації користувачів у ґрід-середовищі з використанням механізму доповнень сертифікату X.509.v.3. Вдосконалено метод шифрування інформації на основі статичного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної системи. Метод покращує частотний розподіл символів у шифрованому тексті, розроблено та досліджено відповідні графічні моделі, підтверджена ефективність тестовими випробуваннями. Розвинуто метод шифрування інформації на основі динамічного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної системи, що покращує частотний розподіл символів у шифрованому тексті та наближує до рівноймовірного, розроблено та досліджено відповідні графічні моделі. Підтверджена ефективність метода тестовими випробуваннями із використанням відомого тесту NIST USA. Запропоновано показники та критерій оцінювання ефективності методів та засобів шифрування текстових даних. Показана ефективність компонентів безпеки, в яких використовуються маскуючі елементи, в першу чергу за рахунок наближення частотного розподілу символів у шифрованому тексті до рівноймовірного.

*Ключові слова:* ефективність компонентів безпеки комп’ютерних систем та мереж, маскуючі елементи біометричних даних, маскуючи елементи текстових даних, критерій оцінювання ефективності шифрування.

## АННОТАЦИЯ

**Игнатович А.А. Методы повышения эффективности компонентов безопасности компьютерных систем с использованием маскирующих элементов текстовых и биометрических данных.** - На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 - "Компьютерные системы и компоненты". - Национальный университет "Львовская политехника" Министерства образования и науки Украины. - Львов, 2016.

В работе решена задача научная повышения эффективности компонентов безопасности компьютерных систем и сетей и определены основные направления улучшения их эффективности на основе использованием маскирующих элементов текстовых и биометрических данных. Получил дальнейшее развитие метод аутентификации пользователей в компьютерных сетях на основе биометрических данных по отпечаткам пальцев с использованием маскирующих элементов - фиктивных частиц. Усовершенствован метод шифрования информации на основе статического использования маскирующих элементов в открытом тексте сообщения с последующим преобразованием информации с помощью блочной криптографической системы. Метод улучшает частотное распределение символов в зашифрованном тексте, разработаны и исследованы соответствующие графические модели, подтверждена эффективность тестовыми испытаниями. Развит метод шифрования информации на основе динамического использования маскирующих элементов в открытом тексте сообщения с последующим преобразованием информации с помощью блочной криптографической системы, что улучшает частотное распределение символов в зашифрованном тексте и приближает к равновероятному, разработаны и исследованы соответствующие графические модели. Определена эффективность метода испытаниями с помощью известного теста NIST USA. Предложены показатели и критерий оценки методов та средств шифрования текстовых данных. Показано, что эффективность компонентов безопасности, в которых используются маскирующие элементы, достигается в первую очередь за счет приближения частотного распределения символов у шифрованном тексте до равновероятного.

*Ключевые слова*: эффективность компонентов безопасности компьютерных систем и сетей, маскирующие элементы биометрических данных, маскирующие элементы текстовых данных, критерий оценки эффективности.

## ABSTRACT

**Ihnatovych A. Efficiency improvement methods for security components of computer systems with the usage of masking elements of text and biometric data.** – On the rights of manuscript.

Thesis for scientific degree of candidate of technical sciences, speciality: 05.13.05 – Computer Systems and Components. – Lviv Polytechnic National University, Lviv, 2016.

The thesis is devoted to the solution of the problem of the effectiveness increasing of the security components of computer systems and networks and the main directions of improving their efficiency through the use of masking elements of text and biometric data. A method for adaptive user authentication in computer networks on the basis of biometric data of a print of fingers using masking elements - fictitious

particles. An algorithm for biometric security for user authentication procedures in a grid environment using X.509.v.3 certificate supplements the mechanism that improves the efficiency of data biometric key access control subsystem (biometric blurred reflections, the stability of biometric features).

Efficiency of biometric data with masking fragments usage within authentication procedures in grid systems is shown. Mathematical model of interaction between user and cryptographic information protection system based on usage of biometric determinant that allows to consider biometric features of the user is explored. Block ciphers peculiarities and increase of their efficiency is researched. New method of efficiency improvement of block ciphers constructed by modification on the basis of inclusion of masking fragments is proposed.

Improved data encryption method based on the use of static masking elements in plain text messages, followed by the transformation of information using block cryptographic system, it improves the frequency distribution of characters in encrypted text, developed and investigated by the appropriate graphical models, confirmed the effectiveness of tests. A method for encrypting data based on the dynamic use of masking elements in plain text messages, followed by the transformation of information using block cryptographic system, improves the frequency distribution of characters in the ciphertext, and closer to the equally probable, developed and investigated by the appropriate graphical models, confirmed the effectiveness of tests. A criterion for evaluating the effectiveness of block ciphers, which use masking elements based on a comparison of the statistical characteristics of cryptographic systems, does not require substantial computing resources in the practical application, and provides an estimate of the frequency distribution of characters in the ciphertext.

Graphic models of the proposed methods are developed and explored. Effectiveness of the proposed security components using the National Institute of Standards and Technology (NIST USA) statistical tests is proven.

New criterion of efficiency evaluation of security components of computer systems based on masking elements of text and biometric data usage, that takes into account few important efficiency evaluating indicators for security components, is proposed. Quantitative results of the comparative evaluation of the proposed solutions and existing analogues of construction of security components, which confirmed the effectiveness of the proposed methods, is obtained.

Research results are implemented within academical courses for bachelor students of the specialty "Computer engineering", scientific and research projects.

*Keywords*: efficiency of the security components of computer systems and networks, masking elements of biometric data, text data masking elements, criterion for evaluating the effectiveness.

Підписано до друку 20.01.2017 р.
Формат 60×90 1/16. Папір офсетний.
Друк на різографі. Умовн. друк. арк. 1,5. Обл.-видав. арк. 0,89.
Тираж 100 прим. Зам. 170047.

Поліграфічний центр
Видавництва Національного університету “Львівська політехніка”
вул. Ф.Колесси, 4, 79013, Львів
*Реєстраційне свідоцтво серії ДК № 4459 від 27.12.2012 р.*