Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет

ДУБЧАК ЛЕСЯ ОРЕСТІВНА

УДК 004.75

МЕТОДИ ТА ЗАСОБИ РОЗПОДІЛУ ДОСТУПУ В КОМП'ЮТЕРНИХ СИСТЕМАХ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

05.13.05 – комп'ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2013

Дисертацією є рукопис.

Робота виконана у Тернопільському національному економічному університеті Міністерства освіти і науки, молоді та спорту України.

Науковий керівник — доктор технічних наук, професор
Карпінський Микола Петрович,
Тернопільський національний технічний університет імені Івана Пулюя,
професор кафедри комп'ютерних наук

Офіційні опоненти: доктор технічних наук, професор
Дудикевич Валерій Богданович,
Національний університет «Львівська політехніка»,
завідувач кафедри захисту інформації;

кандидат технічних наук, доцент
Мухін Вадим Євгенійович,
Національний технічний університет України «Київський політехнічний інститут»,
доцент кафедри обчислювальної техніки

Захист відбудеться «07» березня 2013 р. о $14^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради К 58.082.02 Тернопільського національного економічного університету (46020, Тернопіль, вул. Львівська, 11, зал засідань корпусу №11).

З дисертацією можна ознайомитись у бібліотеці Тернопільського національного економічного університету (46020, м. Тернопіль, вул. Бережанська, 4).

Автореферат розісланий «__» лютого 2013 р.

Учений секретар
спеціалізованої вченої ради
кандидат технічних наук, доцент В.В. Яцків

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Комп'ютерні системи (КС) широко використовуються в різних галузях народного господарства. В умовах розвитку сучасних інформаційних технологій особливо гостро постає задача розподілу доступу до інформаційних ресурсів КС та їх захисту.

Комп'ютерні системи функціонують в жорстких умовах експлуатації, тому необхідно враховувати на етапах їх розробки та виробництва не тільки швидкодію, мінімізацію фінансових витрат, але й стійкість до атак. Отже, виникає необхідність моделювання процесу експлуатації КС в процесі її розробки, тобто моделювання позаштатних ситуацій з метою вибору оптимальної політики безпеки (реконфігурації системи), що зумовлює необхідність розробки нових підходів, методів та засобів для їх реалізації.

Проблемі захисту комп'ютерних систем та мереж передачі інформації від атак на реалізацію присвячені дослідження відомих зарубіжних та вітчизняних науковців, прізвища яких зазначені у дисертації.

Постійне зростання об'ємів інформаційних ресурсів обумовлює жорсткі вимоги до криптозасобів стосовно швидкості опрацювання вхідних даних комп'ютерною системою. Природно, що для вирішення цієї задачі необхідно використовувати апаратну реалізацію відомих алгоритмів криптографічного захисту інформації. Проте такі тенденції щодо апаратної реалізації засобів криптографічного захисту інформації, в свою чергу, зумовили появу принципово нових видів криптоаналізу, які умовно можна назвати "атаки на реалізацію" або ж "атаки на основі нестандартних (побічних) каналів витоку інформації".

Для безпечної експлуатації комп'ютерних систем необхідно застосовувати програмно-апаратні засоби протидії пасивним типам атак з врахуванням обчислювальних ресурсів самих систем.

Тому розробка методів, алгоритмів та програмно-апаратних засобів розподілу доступу, які дозволяють підтримувати задану функціональність та стійкість комп'ютерної системи шляхом розподілення ресурсів в реальному часі, є актуальною задачею.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконувалася в рамках науково-дослідних робіт БІТ-72-05 «К» «Методи та засоби реалізації алгоритмів захисту інформації, стійких до атак на реалізацію» (номер державної реєстрації – 0105U008181, 2005-2010 рр.), ІОСУ-23-10 «К» «Методи та засоби виявлення вторгнень на комп'ютерні системи» (номер державної реєстрації 0110U000786, 2010-2012рр.).

Мета і завдання дослідження. Метою роботи є підвищення стійкості підсистем розподілу доступу комп'ютерних систем до часового аналізу в реальному часі з врахуванням наявних ресурсів систем.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1) проаналізувати сучасні атаки на реалізацію в комп'ютерних системах і мережах, що передають конфіденційну інформацію, та визначити атаки з найбільшим ступенем ризику, а також відомі криптосистеми, стійкі до часового

аналізу, та визначити їх недоліки;

2) дослідити часову складність та стійкість до часового аналізу сучасних методів модулярного експоненціювання, що використовуються в комп'ютерних системах та мережах;

3) розробити ефективний метод розподілу ресурсів комп'ютерної системи в режимі реального часу, зокрема, для оптимального вибору алгоритму модулярного експоненціювання та оброблення нечітких даних для налаштування сервера;

4) на основі запропонованого методу створити апаратно-програмний засіб розподілу доступу в комп'ютерних системах, ефективний для експлуатації в реальному часі.

Об'єкт дослідження – процес збору та передачі інформації в комп'ютерних системах різного рівня конфіденційності з динамічно розподіленим навантаженням і різним ступенем ризику в сегментах.

Предмет дослідження – методи та засоби підвищення стійкості комп'ютерної системи до атак на реалізацію в умовах динамічного розподілу доступу та ресурсів.

Методи дослідження – методи теорії ймовірності та математичної статистики, математичного аналізу, нечіткої логіки, теорії алгоритмів, прикладної теорії цифрових автоматів і структурного синтезу.

Наукова новизна отриманих результатів. В дисертації розв'язано важливу науково-технічну задачу розподілу доступу в комп'ютерній системі та отримано такі наукові результати:

1. Вперше запропоновано метод визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу, який базується на залежності часової складності алгоритму від ваги Хемінга, що дозволяє аналітично визначити стійкість будь-якого методу модулярного експоненціювання до часового аналізу.
2. Розроблено новий метод оптимального вибору алгоритму модулярного експоненціювання, який базується на методі визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу та механізмі нечіткого висновку Мамдані, що забезпечує зменшення часу реакції системи захисту інформації на зміну вхідних параметрів в реальному часі.
3. Вперше запропоновано метод оброблення нечітких даних для налаштування сервера, який базується на попередньому обробленні функцій належності входів, що дозволило зменшити часову складність нечіткого висновку Мамдані і, відповідно, забезпечити додаткове зменшення часу реакції системи захисту інформації.
4. Вдосконалено структуру засобу розподілу доступу в комп'ютерних системах, яка відрізняється від відомих тим, що забезпечує, на основі розробленого методу оброблення нечітких даних, адаптивний вибір оптимального методу модулярного експоненціювання та динамічну реконфігурацію в реальному часі при зміні середовища експлуатації та з врахуванням наявних ресурсів комп'ютерної системи.

Практичне значення отриманих результатів.

1. Створено методи та засоби, які дають можливість вирішувати задачу

ефективного розподілу доступу в комп'ютерних системах в умовах неповної, неточної і суперечливої інформації про клієнтів.

2. Розроблені методи дозволяють збільшити швидкість пошуку рішень, які забезпечують задані рівні захисту та продуктивності при необхідному обмеженні об'єму використаної пам'яті, що дає можливість створеним на їх основі апаратним засобам функціонувати в реальному часі.

3. Розроблено структуру засобу розподілу доступу в комп'ютерних системах, яка придатна для вирішення практичних задач захисту інформації.

Результати експериментальних досліджень підтверджують достовірність наукових положень дисертаційної роботи, а впроваджені засоби підвищують рівень захисту інформації в комп'ютерних системах.

Теоретичні та практичні результати роботи використані у: 1) ПП "НВПП «Спаринг-Віст Центр»"; 2) ТОВ "Шредер" для захисту від несанкціонованого доступу до інформації; 3) навчальному процесі при викладанні дисциплін «Моделювання комп'ютерних систем», «Захист інформації в комп'ютерних системах», «Комп'ютерна криптографія».

Особистий внесок здобувача. Усі основні результати, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих у співавторстві, здобувачу належать: у [5, 6] –класифікація атак спеціального виду, дослідження часової атаки та методів її протидії; [21] – визначення типів атак, які можуть здійснюватись при передачі захищеної інформації через комп'ютерну мережу; [2, 14] – дослідження застосування симетричних, асиметричних та криптосистем на основі еліптичних кривих; [1] – дослідження обчислювальної складності генераторів псевдовипадкових чисел; [15, 20] - визначення залежності часу виконання алгоритмів сучасних методів модулярного експоненціювання від ваги Хемінга; [3, 12, 22] - метод визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу; [7, 16, 17] – дослідження ризику витоку інформації, зашифрованої за допомогою бінарного методу модулярного експоненціювання, при проведенні часового аналізу; [4, 18, 19] - дослідження β-арного та методу ковзаючого вікна піднесення до степеня за модулем, імовірнісна оцінка ризику витоку інформації під час проведення часового аналізу, рекомендації щодо побудови криптосистем, стійких до даного типу атак; [8, 13, 23] - метод оптимального вибору алгоритму модулярного експоненціювання на основі класичного механізму нечіткого висновку Мамдані та його дослідження.

Апробація результатів дисертації. Основні результати дисертації були висвітлені та обговорені на науково-технічних конференціях: 12-ій науковій конференції Тернопільського державного технічного університету ім. І.Пулюя (м.Тернопіль, 2008); VII та VIII міжнародній науково-технічній конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" (CADSM'2003, 2005) (Львів-Славське, 2003, Львів-Поляна, 2005); міжнародній науково-технічній конференції "Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії" (TCSET'2004, 2006) (Львів-Славське, 2004, 2006); 2-ій міжнародній науково-технічній конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN-2005) (м.Львів, 2005);

міжнародній конференції “Безпека та менеджмент” (SAM’06) (Лас Вегас, США, 2006); III міжнародній науково-практичній конференції “Актуальные проблемы научных исследований - 2007” (м.Дніпропетровськ, 2007); другій міжнародній науково-практичній конференції «Методи та засоби кодування, захисту й ущільнення інформації» (м.Вінниця, 2009); VIII міжнародній конференції «Проблеми впровадження інформаційних технологій в економіці» (м.Ірпінь, 2012); II Всеукраїнській школі-семінарі «Сучасні комп’ютерні інформаційні технології» (АСІТ’2012) (м.Тернопіль, 2012).

Публікації. Усі основні положення дисертації знайшли повне відображення у 24 наукових працях, які містять 1 монографію (1, 4 розділи), 12 статей, з них 11 у фахових виданнях, 11 праць у збірниках наукових конференцій.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 210 сторінок, з яких 118 сторінок основного тексту. Робота містить 46 рисунків, 10 таблиць та 9 додатків. Список використаних джерел включає 151 найменування на 18 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми, сформульовано мету та завдання дослідження, представлено наукову і практичну цінність отриманих результатів, а також відомості про особистий внесок здобувача, апробацію роботи та публікації.

У **першому розділі** розглянуто особливості розподілу доступу в комп’ютерній системі, проаналізовано сучасні атаки спеціального виду на побічні канали витоку інформації КС та базові операції асиметричних криптосистем, сформульовано задачі дослідження.

В сучасних системах передачі даних типу клієнт-сервер можливі атаки зловмисника через комп’ютерну мережу з допомогою побічних каналів витоку інформації. Класифікація традиційних методів захисту проти атак спеціального виду дозволяє ґрунтовно визначати переваги та недоліки того чи іншого методу захисту, а також є корисною при розробці нових методів.

Найнебезпечнішою атакою на КС при передачі інформації є пасивна часова атака, оскільки її неможливо помітити в мережі та вчасно застосувати методи протидії. Аналіз операцій, які виконуються при реалізації алгоритмів модулярного експоненціювання (МЕ), дозволяє дослідити характеристики асиметричних криптосистем та визначити методи розподілу доступу під час передачі таємної інформації. Систему розподілу доступу в КС найкраще побудувати на базі нечіткої логіки шляхом оптимального вибору методу МЕ для кожного окремого клієнта та врахування поточних параметрів самої КС, що дозволить забезпечити стійкість КС до часового аналізу в реальному часі.

У **другому розділі** досліджено основні параметри методів МЕ: продуктивність, затрати пам’яті та стійкість алгоритму МЕ до атак на реалізацію, зокрема до часового аналізу, встановлено залежність часу виконання алгоритму бінарного, β-арного та методу ковзаючого вікна від довжини ключа. Найвищу

продуктивність та прийнятні затрати пам'яті має алгоритм β-арного методу МЕ.

Основні операції алгоритмів МЕ та затрати часу на виконання кожної з них можна позначити таким чином: просте присвоєння здійснюється за час c; операція присвоєння за модулем $z = x \bmod m$ - за час b; знаходження найдовшої послідовності бітів, такої, що $i - j + 1 \le w$ та $n_j = 1$ - за час q; зображення числа у двійковій системі числення – t; операція $y = x \cdot x \bmod m$ - за час r; на множення за модулем $z = x \cdot y \bmod m$ затрачається час s; на піднесення до степеня за модулем $z = y^{\beta} \bmod m$ - час d. При цьому співвідношення між значеннями затрат часу на виконання основних операцій алгоритмів МЕ є таким: $c \le b \le q \le t \le r \le s \le d$.

З врахуванням цього побудовано математичну модель обчислення часу, затраченого на виконання кожного з алгоритмів реалізації методів МЕ. Оскільки змінна n опрацьовується у бінарному вигляді, то через $\lceil \log n \rceil$ представляється довжина цієї бінарної послідовності. Через $H(n)$ позначено вагу Хемінга, тобто кількість одиниць у бінарному представленні n.

У таблиці 1 подано затрати часу на виконання досліджуваних алгоритмів реалізації методів МЕ, при цьому $W_0(n)$ – кількість нульових бітів у зображенні числа n за основою β, w – показник степеня двійки в $\beta = 2^w$, p – кількість вікон.

Таблиця 1 – Затрати часу на виконання досліджуваних алгоритмів МЕ

Алгоритм МЕ	Зчитування бітів експоненти зліва направо	Зчитування бітів експоненти справа наліво
Бінарний метод	$T1(n) = t + c + \lceil \log n \rceil \cdot r + H(n) \cdot s$	$T2(n) = t + c + b + H(n) \cdot s + \lceil \log n \rceil \cdot r$
β-арний метод	$T3(n,w) = t + 2c + \frac{\lceil \log n \rceil}{w} \cdot d + \left(\frac{\lceil \log n \rceil}{w} + 2^w - 1 \right) \cdot s$	$T4(n,w) = t + \left(2^w + 1\right)c + b + \frac{\lceil \log n \rceil}{w} \cdot d + \left(\frac{\lceil \log n \rceil}{w} - W_0(n) + 2^{w+1} - 2 \right) \cdot s$
Метод ковзаючого вікна	$T5(n,\lvert w_i \rvert) = t + b + pq + \lceil \log n \rceil r + \left(2 + p + \lceil \log n \rceil - H(n)\right)c + \left(2^{\lvert w_i \rvert} + p\right)s$	$T6(n,\lvert w_i \rvert) = t + b + \left(\lceil \log n \rceil - H(n)\right)r + \left(2^{2\lvert w_i \rvert - 2} + 2 + \lceil \log n \rceil - H(n) + p\right)c + \left(2^{2\lvert w_i \rvert - 1} + p\right)s + pq + pd$

Аналіз таблиці 1 показує, що залежність часу виконання алгоритмів МЕ від довжини n має лінійний характер.

На рисунках 1 та 2 зображено, відповідно, залежність швидкодії алгоритмів β-арного методу "зліва направо" та "справа наліво" від значення степеня основи w в залежності від різної довжини ключа n (256, 512, 1024, 2048, 4096 біт) та при усередненому значенні ваги Хемінга.

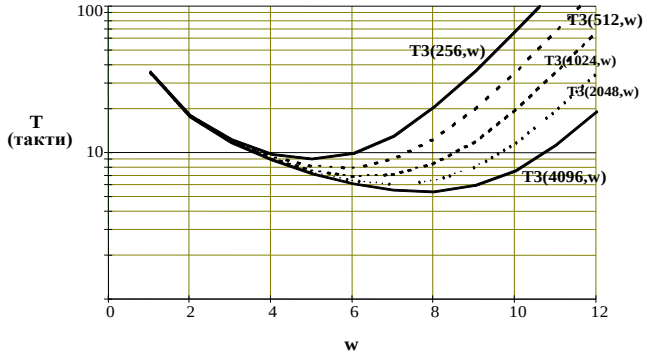


Рисунок 1 – Залежність швидкодії алгоритму β-арного методу “зліва направо” від значення степеня основи w

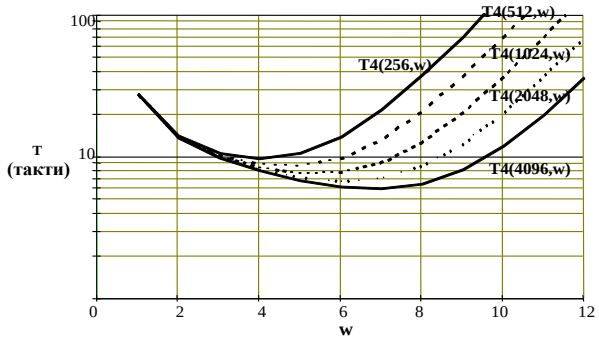


Рисунок 2 – Залежність швидкодії алгоритму β-арного методу “справа наліво” від значення степеня основи w

За даними рисунків 1 та 2 можна визначити оптимальну основу w, при якій затримка роботи алгоритму найменша і забезпечена його максимальна продуктивність при заданих значеннях експоненти n. Для алгоритмів β-арного методу найкращими будуть значення w, подані в таблиці 2.

Таблиця 2 – Оптимальні значення степеня основи β-арного методу

Довжина ключа n	Значення степеня двійки в β-арному представленні, w	
	B-арний метод “зліва направо”	β-арний метод “справа наліво”
4096	8	7
2048	7	6
1024	6	5
512	6	5

Об’ємна складність алгоритму МЕ стає критичною, коли обсяг опрацьовуваних даних сягає межі обсягу оперативної пам’яті. Затрати пам’яті у випадку виконання бінарного алгоритму максимально становлять 2 комірки, алгоритму ковзаючого вікна є найбільшими - $2^{|w_i|}$ комірок (оскільки найдовше вікно $|w_i|$ може дорівнювати половині довжини ключа). У випадку застосування алгоритму β-арного методу МЕ затрати пам’яті залежать від обраної системи числення, тобто від значення w, і становлять 2^w.

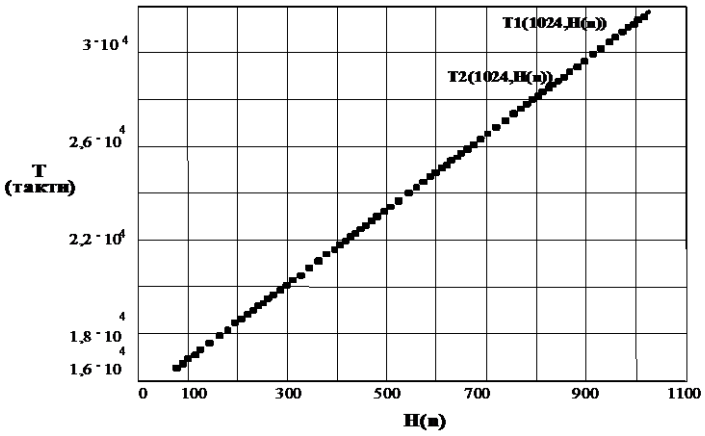


Рисунок 3 – Залежність часу виконання алгоритму бінарного методу від ваги Хемінга

На рисунку 3 зображено залежність часу виконання алгоритмів бінарного методу “зліва направо” та “справа наліво” від ваги Хемінга при довжині експоненти $\lceil \log n \rceil = 1024$ біти, яка задовільняє сучасні вимоги до довжини ключа криптосистеми. Аналіз графіка показує, що продуктивність даних алгоритмів суттєво залежить від ваги Хемінга, тому стійкість цих методів до часового аналізу мінімальна, адже зловмисник, за часом виконання алгоритму, оцінить кількість одиниць у двійковому зображенні числа n та визначить таємний ключ шляхом перебору у звуженому

ключовому просторі.

Аналіз графіка залежності швидкодії алгоритму β-арного методу "зліва направо" від ваги Хемінга (рисунок 4) показує, що час виконання цього алгоритму залежить лише від значення β. Тобто цей алгоритм є стійким до часової атаки. Дослідження залежності часу виконання алгоритму β-арного методу "справа наліво" від ваги Хемінга (рисунок 5) показує, що він залежить від кількості одиниць у двійковому зображенні числа n.

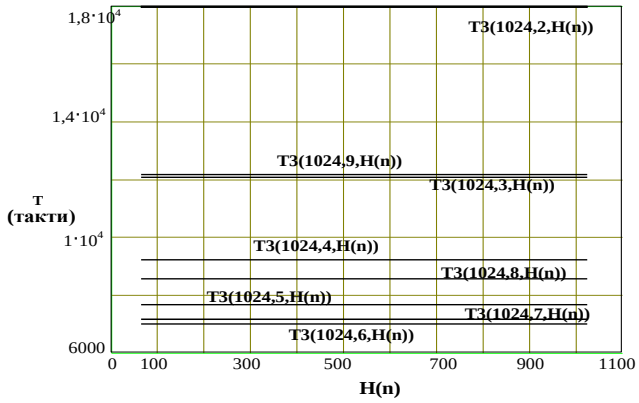


Рисунок 4 – Залежність часу виконання алгоритму β-арного методу "зліва направо" від ваги Хемінга

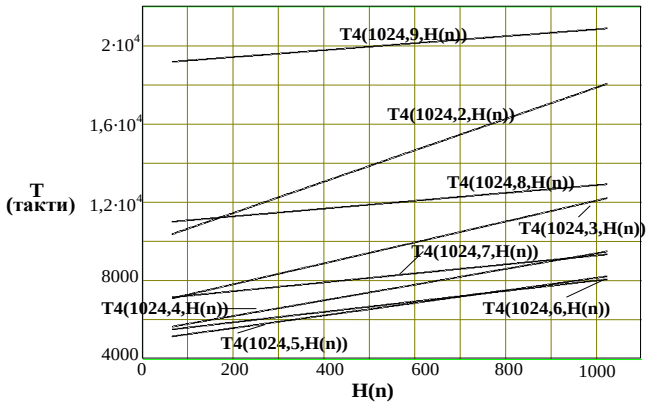


Рисунок 5 – Залежність швидкодії алгоритму β-арного методу "справа наліво" від ваги Хемінга

Для оцінки стійкості інших методів МЕ слід ввести критерій стійкості до часового аналізу, який відображає залежність часу виконання відповідних алгоритмів від ваги Хемінга.

З аналізу графіків залежності часу виконання алгоритмів МЕ від ваги Хемінга випливає, що: по-перше, стійким є той алгоритм, час виконання якого є сталим, тобто пряма зображення якого паралельна до осі абсцис; по-друге, чим більший кут нахилу прямої, тим легше зловмиснику визначити вагу Хемінга за часом. Тобто стійкішим до часової атаки є той алгоритм, для якого кут нахилу прямої $T(n, w, |w_i|)$ часу його виконання наближається до 0°. Оскільки $\frac{dT_i}{dH(n)} = tg\alpha_i$, де α_i – кут нахилу прямої $T_i(n, w, |w_i|)$ до осі OX, і $\cos 0^\circ = 1$, то для оцінки стійкості алгоритму МЕ до часової атаки запропоновано метод визначення нормованої стійкості S, який базується на співвідношенні

$$S = \cos\left(arctg \frac{dT_i}{dH(n)} \right). \quad (1)$$

У таблиці 3 подано оцінки параметрів кожного досліджуваного алгоритму при значеннях $w = 8$ та довжині одиничного вікна $|w_i| = 3$, що забезпечує високий рівень швидкодії β-арного методу та стійкості для методу ковзаючого вікна. З аналізу таблиці 3 випливає, що абсолютно стійким до часової атаки є β-арний метод "зліва направо".

Таблиця 3 – Результати досліджень часу виконання та нормованої стійкості алгоритмів ME

Алгоритм	Довжина n, біт	Час виконання, такти	Нормована стійкість до часового аналізу S
Бінарний метод “зліва направо”	1024	23550	0.062
	2048	47110	
	4096	94210	
Бінарний метод “справа наліво”	1024	23560	0.062
	2048	47110	
	4096	94210	
β –арний метод “зліва направо”	1024	9204	1
	2048	18160	
	4096	36080	
β –арний метод “справа наліво”	1024	7412	0.243
	2048	14320	
	4096	28150	
Метод ковзаючого вікна “зліва направо”	1024	22350	0.430
	2048	44570	
	4096	89020	
Метод ковзаючого вікна “справа наліво”	1024	21560	0.114
	2048	42590	
	4096	84640	

Наступним за стійкістю є метод ковзаючого вікна “зліва направо”. Найменшу стійкість до часового аналізу має бінарний метод. При заданих параметрах найшвидшим алгоритмом ME є β-арний метод “справа наліво”.

Ризик витоку таємної інформації (під час часового аналізу розглянутих методів ME)

$$P\left(Z > -\frac{\sigma_S}{\sigma_0}\frac{\sqrt{K}}{2}\right) = \Phi\left(\frac{\sigma_S}{\sigma_0}\frac{\sqrt{K}}{2}\right), \quad (2)$$

де $\Phi\left(\frac{\sigma_S}{\sigma_0}\frac{\sqrt{K}}{2}\right)$ - площа під стандартною нормальною кривою від $-\infty$ до Z (Z - множина прийнятних рішень); K – кількість проведених вимірювань.

З рисунків 6 та 7 (j_0 - порядковий номер біта у представленні експоненти) випливає, що ризик витоку таємної інформації найменший у випадку застосування в асиметричній криптосистемі типу RSA β-арного методу “зліва направо” чи методу ковзаючого вікна “зліва направо”, що підтверджує проведені вище дослідження.

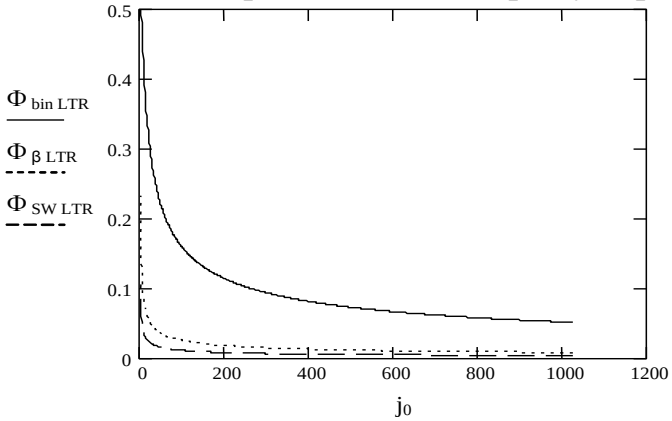


Рисунок 6 – Залежність ризику витоку таємної інформації від j_0 при зчитуванні бітів експоненти “зліва направо”

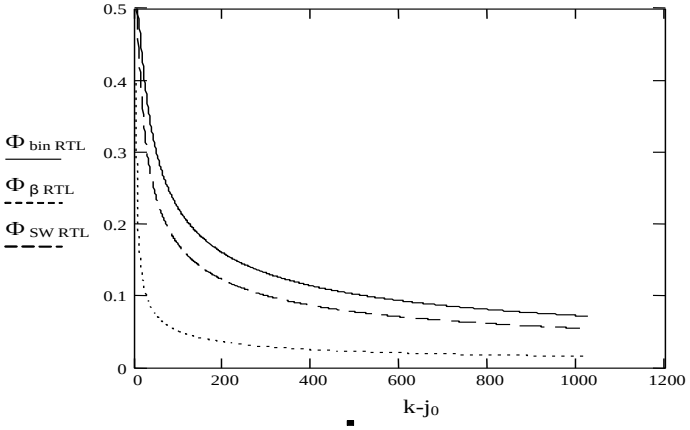


Рисунок 7 – Залежність ризику витоку таємної інформації від j_0 при зчитуванні бітів експоненти “справа наліво”

У **третьому розділі** запропоновано метод оптимального вибору алгоритму ME для розподілу доступу в КС на основі класичного механізму нечіткого висновку Мамдані, розроблено метод оброблення нечітких даних для налаштування сервера, а також проведено моделювання та дослідження засобів реалізації цих методів.

КС при передачі таємної інформації використовує, як правило, мережу, яку можна умовно поділити на захищену та незахищену частину (рисунок 8). У незахищеній частині мережі клієнти $K_1, K_2, ..., K_n$ випадкові, тому вони не є надійними для сервера з точки зору безпеки. Крім того, ця частина мережі, як правило, не захищена від збоїв внаслідок впливів зовнішнього середовища і є відкритою для проведення всіх видів сучасних атак на реалізацію. У захищеній частині мережі клієнти $K_{i1}, K_{i2}, ..., K_{im}$ вважаються надійними і, завдяки політиці безпеки, виключається існування внутрішнього зловмисника. Проте в цій частині мережі все-таки залишається можливість проведення пасивної атаки часового аналізу. Сервер КС складається з підсистеми ідентифікації клієнта, командної підсистеми та блоку обробки інформації (рисунок 9). Підсистема ідентифікації клієнта подає на блок обробки інформації дані про необхідний рівень стійкості до часового аналізу, враховуючи усі дані про користувача. Якщо клієнт для КС новий або має низький рівень довіри, то рівень стійкості до часового аналізу має бути максимальним, рівним 1. Для клієнта з дуже високим рівнем довіри значення стійкості може прямувати до 0, що підвищить швидкодію системи.

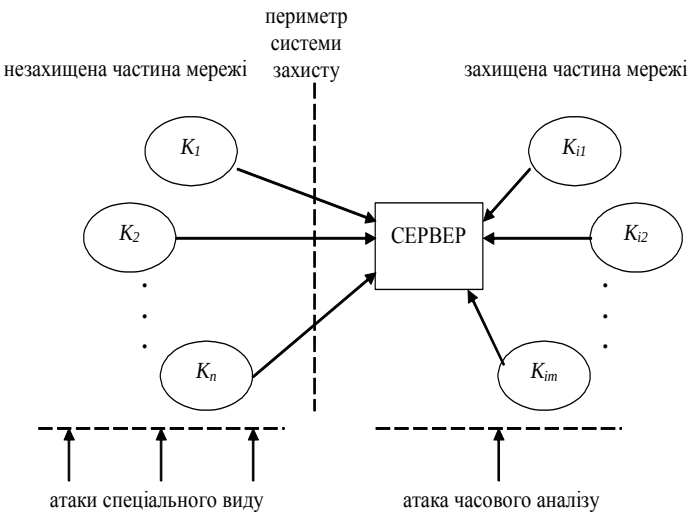


Рисунок 8 – Схема здійснення можливих атак на реалізацію при передачі даних в КС

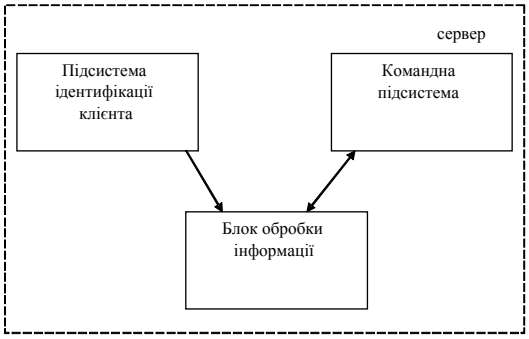


Рисунок 9 – Структура сервера для забезпечення розподілу доступу в КС

Командна підсистема сервера подає на блок обробки інформацію про саму КС, тобто допустимі затрати пам’яті та необхідний рівень продуктивності.

Для захисту інформації у КС необхідно оптимально вибрати метод МЕ для шифрування інформації або аутентифікації клієнта за допомогою криптоалгоритму RSA. Це завдання вирішує блок обробки інформації на базі нечіткої логіки, а саме на механізмі нечіткого висновку Мамдані. Він опрацьовує вхідні значення продуктивності, затрат пам’яті та стійкості до часового аналізу і подає оптимальний у кожному випадку метод МЕ на командну підсистему, яка застосовує цей метод для шифрування інформації. Основною перевагою цього блоку є можливість функціонування в реальному часі, що забезпечить вищу стійкість КС до атак зловмисника, який не буде достовірно знати алгоритму шифрування.

Загальну схему розподілу доступу в КС подано на рисунку 10. Основою системи захисту КС є блок обробки інформації на основі нечіткої логіки. На його вхід поступають критерії вибору методу МЕ: необхідний рівень стійкості до часового аналізу *R*, продуктивності криптосистеми *P* та допустимі затрати пам'яті сервера *M*. Підсистема оптимального вибору методу МЕ опрацьовує ці дані на основі нечіткого висновку за механізмом Мамдані. Виходом блоку обробки інформації є метод МЕ, що забезпечує оптимальну конфігурацію системи захисту відносно значень вхідних критеріїв вибору.

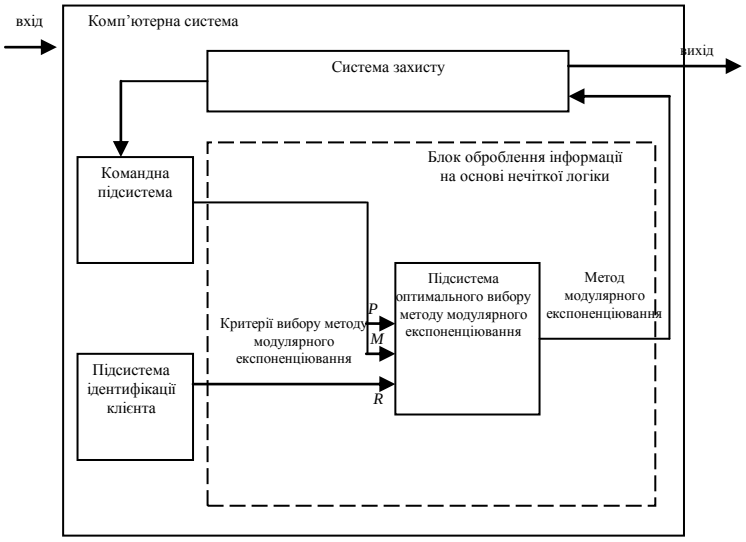
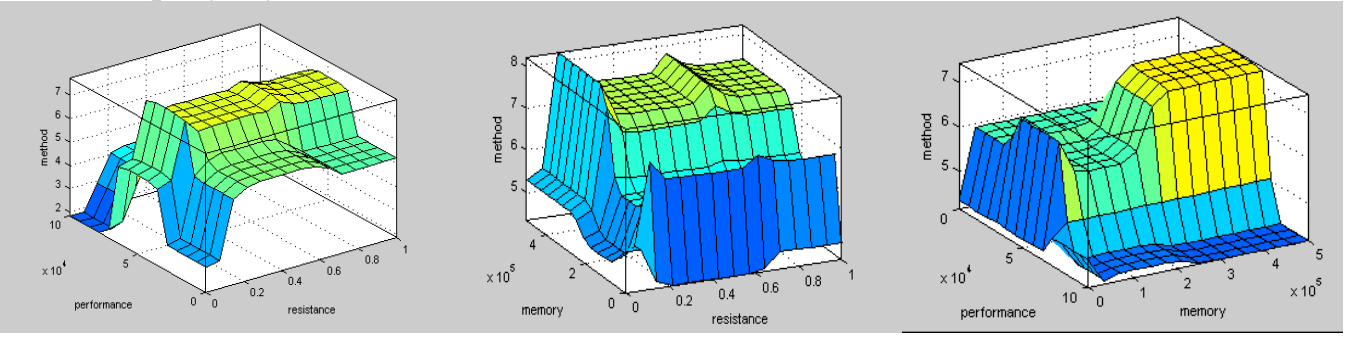


Рисунок 10 – Загальна схема розподілу доступу в КС на основі нечіткої логіки

Нечітку систему оптимального вибору методу МЕ (*method*) залежно від значень продуктивності (*performance*), стійкості до часового аналізу (*resistance*) та допустимих затрат пам'яті (*memory*) побудовано, застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB. Значення функцій належності вхідних змінних *resistance* та *memory* задається трапецевидною функцією, а вхідної змінної *performance* – дзвоноподібною функцією. Функція належності виходу *method* задається трикутною формою. Стійкість до часового аналізу описують змінні $low \in [0,0.014]$ (низький рівень), $middle \in [0.0145,0.72]$ (середній рівень) та $high \in [0.56,1]$ (високий рівень). Продуктивність описують змінні $high \in [0, 31000]$, $middle \in [27000, 75000]$ та $small \in [67000, 100000]$ (відповідно висока, середня та низька). Допустимі затрати пам'яті задаються змінними $small \in [0, 9920]$, $middle \in [9921, 2.52 \cdot 10^5]$ і $big \in [2.49 \cdot 10^5, 5 \cdot 10^5]$ (малі, середні та великі затрати, відповідно). Функції належності для вихідної змінної *method* позначаються однаковими інтервалами на осі ординат для визначення центру ваги, що є нечітким висновком системи. *Binary* позначає бінарний метод МЕ, *beta-aryRTL* та *beta-aryLTR* - β-арний "справа наліво" та "зліва направо", відповідно, *wRTL* – метод ковзаючого вікна "справа наліво", а *wLTR* – ковзаючого вікна "зліва направо". Для бінарного методу напрям зчитування бітів довільний, оскільки вони мають ідентичну стійкість до атаки часового аналізу (див. рисунок 3), а їх продуктивність практично однакова.

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то», усі вхідні змінні мають по три нечітких стани і ще один стан *none* (вхідна змінна не задана системою). Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \cdot 4 \cdot 4 - 1 = 63$.

Поверхні значень виходу нечіткої системи на основі механізму Мамдані подані на рисунку 11.



а) б) в)

Рисунок 11 – Поверхні значень виходу нечіткої системи на основі механізму Мамдані залежно від значень: а) стійкості до часового аналізу та продуктивності; б) затрат пам’яті та стійкості до часового аналізу; в) продуктивності та затрат пам’яті

Основним недоліком класичного механізму Мамдані є необхідність опрацювання усієї бази правил для будь-яких вхідних даних. Це знижує швидкодію системи та вимагає затрат пам’яті, тому варто розробити метод оброблення нечітких даних, використавши модифікований механізм Мамдані для збільшення швидкодії. Суть пропонованої модифікації полягає в тому, що обробку нечіткої інформації розділено на етапи навчання та експлуатації. Під час навчання визначено області функцій належності виходу для кожного з правил. А при експлуатації спочатку відбувається порівняння вхідних даних зі значеннями функцій належності виходу у визначених базою правил областях пам’яті, де зберігаються значення згаданих функцій належності виходу, відповідних до кожного правила нечіткого висновку. Далі відсікаються значення функцій належності виходу, які перевищують вхідні дані. Потім вибираються мінімальні значення функцій належності виходу, отриманих після відсікання, і будується з цих мінімальних значень відповідна фігура. Останньою операцією методу оброблення нечітких даних є пошук центра ваги фігури, отриманої в результаті додавання відсічених функцій належності виходу.

Для оцінки часової складність, як основного критерію оцінки алгоритму, розглянемо лише неспівпадаючі операції запропонованих методів нечіткого висновку на основі класичного та модифікованого механізму Мамдані (таблиця 4).

Аналіз таблиці 4 показує, що часова складність пропонованого методу оброблення нечітких даних є на $O(n^2)$ менша, ніж складність класичного механізму нечіткого висновку Мамдані. Тому пропонований метод має швидкодію вчетверо вищу, ніж базований на класичному. Це є наслідком пропонованої попередньої обробки функцій належності виходу на етапі навчання. При експлуатації засобу, коли задані значення вхідних даних, опрацьовуються лише ті області функцій належності виходу, які відповідають записаним областям функцій належностей входів згідно бази правил нечіткого висновку.

Дослідження бази правил нечіткої системи засобами MATLAB показали, що кількість областей рівна 14, тобто зменшилась в 4,5 рази порівняно з базою 63

правил, що використовується в методі оптимального вибору алгоритму модулярного експоненціювання на основі класичного механізму нечіткого висновку Мамдані. Відповідно пришвидшено опрацювання нечітких даних.

Таблиця 4 – Часова складність операцій нечіткого висновку за класичним механізмом Мамдані та пропонованого методу

Операції нечіткого висновку за класичним механізмом Мамдані (метод 1)	Часова складність операцій методу 1	Операції нечіткого висновку пропонованого методу (метод 2)	Часова складність операцій методу 2
1.Порівняння вхідних даних зі значеннями функції належності входів	$O(\log n)$	1.Порівняння вхідних даних зі значеннями функції належності виходів у відповідних областях ПЗП	$O(\log n)$
2.Знаходження найменшого значення функції належності входів щодо кожного з входів, які відповідають базі правил	$O(n)$	-	-
3.Відсікання на осі ординат функцій належності виходу значень, які перевищують значення, задане в п.2	$O(\log n)$	3.Відсікання на осі ординат функцій належності виходу у всіх відповідних областях багатоканального блоку пам'яті значень, які перевищують значення, знайдене в п.1	$O(\log n)$
4.Знаходження серед відсічених функцій належності виходу тих, що мають максимальну амплітуду	$O(n^2)$	4.Знаходження серед відсічених функцій належності виходу у всіх відповідних областях багатоканального блоку пам'яті тих, що мають мінімальну амплітуду	$O(n)$

Побудову моделі засобу оптимального вибору методу ME для забезпечення стійкості КС здійснено засобами Simulink (рисунок 12). Входами нечіткого контролера (Fuzzy Logic Controller) є значення стійкості (resistance), продуктивності (performance) та затрат пам'яті (memory), а виходом – значення центра ваги, який інтерпретує метод ME (method). Результат роботи моделі при заданих стійкості до часової атаки, продуктивності та допустимих затратах пам'яті КС з рівномірним розподілом, тобто значення центра ваги, подано на рисунку 13.

Схема нечіткого контролера (рисунок 14), що реалізує пропонований метод, містить три блоки опису функцій належності вхідних змінних (блоки Input MF), блок опису функцій належності виходу (Output MF), виходи яких поступають на вхід 63 правил (блоки Rule 1 … 63) (рисунок 14).

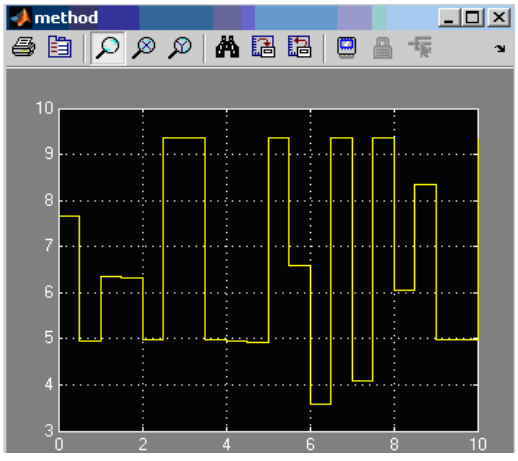


Рисунок 13 – Результати роботи розробленої нечіткої моделі

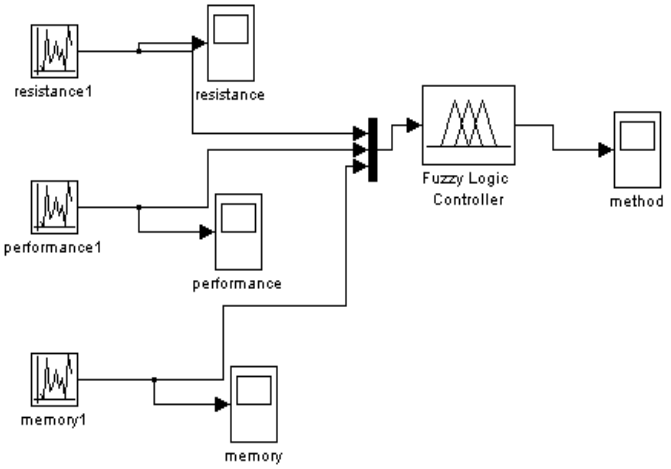


Рисунок 12 – Модель розробленого засобу

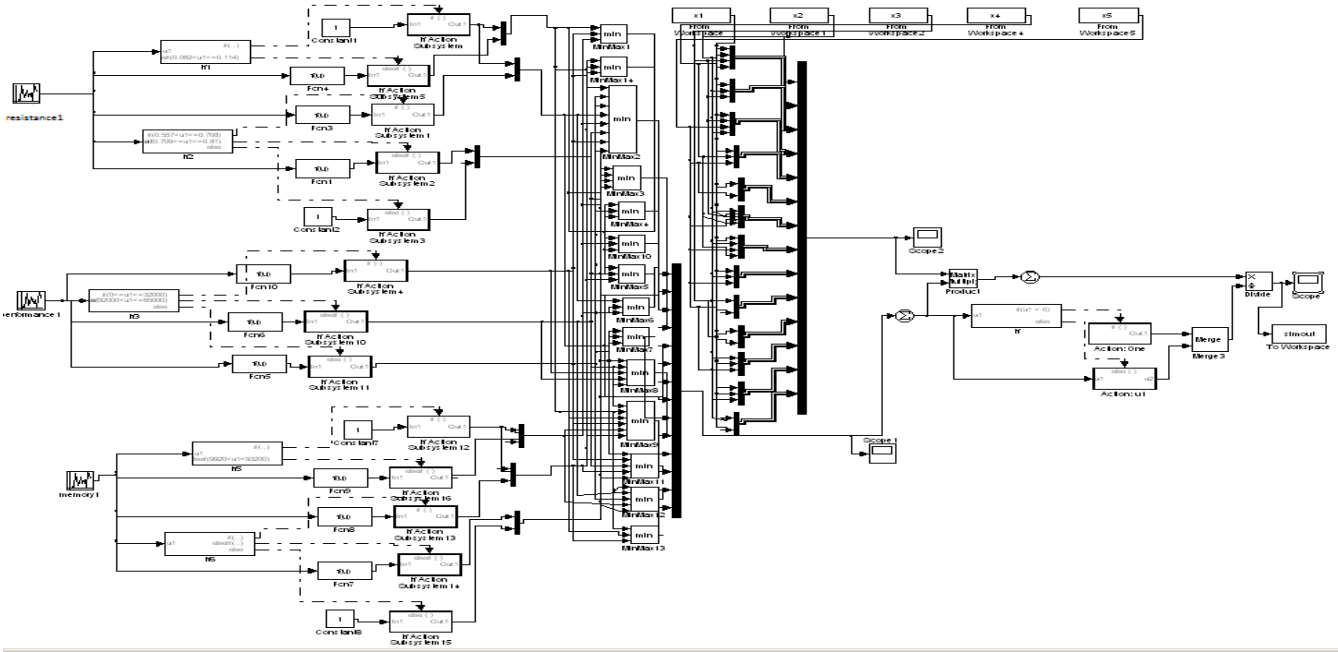


Рисунок 14 – Схема нечіткого контролера

Для задання областей функцій належності виходу використано додавання відповідних кожному з методів МЕ інтервалів, що інтерпретуються змінними $x1$ – $x5$ ($x1=[0,2]$ відображає бінарний метод, $x2=[2,4]$ - β-арний метод “зліва направо”, $x3=[4,6]$ - β-арний метод “справа наліво”, $x4=[6,8]$ - метод ковзаючого вікна “зліва направо”, $x5=[8,10]$ - метод ковзаючого вікна “справа наліво”).

Таблиця 5 – Результати симуляції нечіткого контролера за класичним нечітким висновком Мамдані та пропонованим методом

Вхідні змінні			Нечіткий висновок Мамдані	Пропонований метод
resistance	performance	memory	Method	Method
0.0452	1.68e+004	6.65e+003	3.59	3.64
0.0771	4.55e+004	9.31e+003	5.26	5.2
0.0239	6.2e+004	1.5e+005	4.79	4.81
0.104	3.64e+004	3.26e+005	7.27	7.25
0.157	7.85e+004	1.2e+004	3.88	3.91
0.604	6.3e+004	2.22e+005	6.27	6.4
0.96	9.49e+004	1.93e+005	2.43	2.39
0.0133	7.15e+004	3.99e+003	1.66	1.69
0.168	3.11e+004	3.5e+005	8.36	8.31
0.0452	2.95e+004	3.32e+004	2.6	2.65

Результати симуляції нечіткого контролера за класичним нечітким висновком Мамдані та пропонованим методом (див. рисунок 14) подано в таблиці 5.

Аналіз таблиці 5 показує, що середнє відхилення результату схеми рисунку 14 від значення виходу нечіткого контролера за класичним механізмом Мамдані становить в середньому 0,055, що підтверджує працездатність системи і правильність отриманих результатів.

Четвертий розділ присвячено розробці структури засобу розподілу доступу на основі нечіткої логіки та його експериментальним дослідженням.

Вибір методу МЕ згідно заданої продуктивності, стійкості до часового аналізу та допустимих затрат пам’яті реалізовано запропонованим в розділі 3 методом

оброблення нечітких даних. Для обчислення координат центру ваги припущено, що функцією належності є плоска фігура однакової товщини. Тоді радіус-вектор центра ваги

$$r_{ЦВ} = \frac{\sum r_i m_i}{\sum m_i} \quad , \quad (3)$$

де r_i і m_i – координата центра ваги та маса i-того прямокутника, з яких складена фігура, центр ваги якої слід знайти.

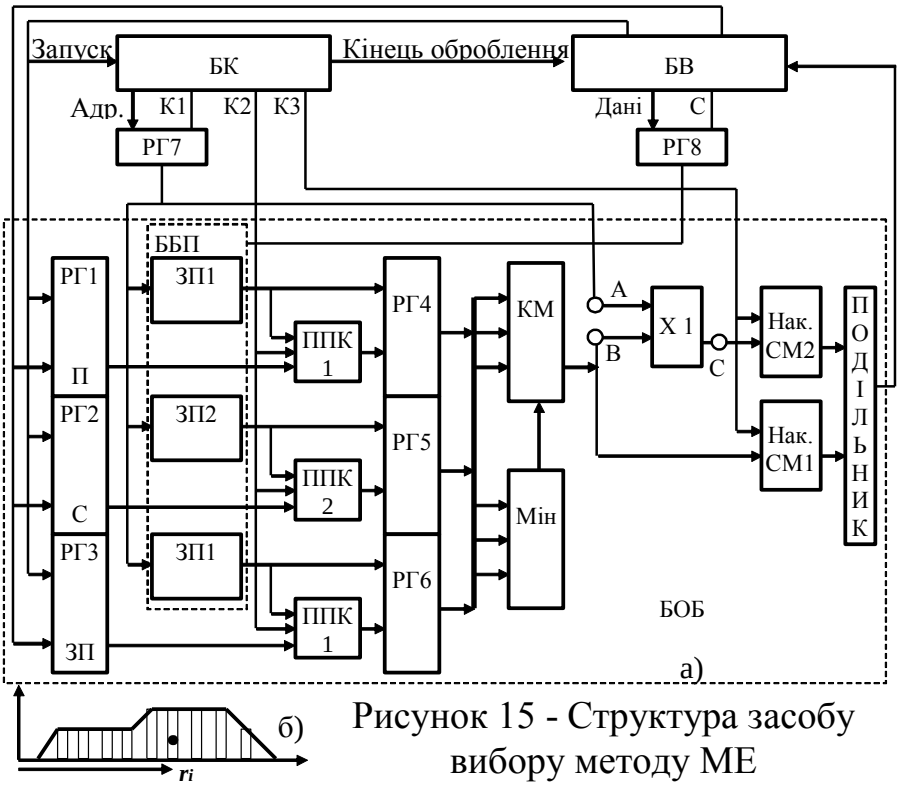


Рисунок 15 - Структура засобу вибору методу МЕ

На рисунку 15,а) представлено структурну схему розробленого засобу, що визначає центр ваги за спрощеною схемою, що має методичну похибку. Він складається з регістрів пам’яті РГ1-РГ3 заданої продуктивності, стійкості та об’єму пам’яті, багатоканального блоку пам’яті ББП оброблених згідно пропонованого методу оброблення нечітких даних функцій належності входу, пристроїв порівняння кодів ППК1-ППК3, проміжних регістрів РГ4-РГ5, вузла Мін знаходження мінімуму, комутатора КМ, перемножувача Х1, накопичуючих суматорів Нак. СМ1 і СМ2 та ПОДІЛЬНИКА. На рисунку 15,б) показано принцип дії розробленого засобу. Блок використання (БВ) оброблення даних запускає блок керування БК, який циклічно формує сигнали керування К1, К2, К3. Інші блоки формують прямокутники, що відображають функцію належності виходу (див. рисунок 15,б)). БК змінює адресу в РГ7, задаючи чергові цикли (прямокутники). В Нак. СМ2 формується чисельник, а в Нак. СМ1 – знаменник (3). Після перебору всіх адрес $r_{ЦВ}$ поступає на БВ за сигналом „кінець оброблення”.

Запропоновано також замінити Х1 схемою, що містить два квадратори, суматор і блок добування квадратного кореня. Вона дозволяє за теоремою Піфагора обчислити координату центра ваги без методичної похибки.

Для дослідження швидкодії розробленого засобу у симуляторі Electronics Workbench реалізовано основні вузли, а у симуляторі Xilinx 10.1.03 спроектовано на мові VHDL сам засіб та експериментально досліджено його часові параметри для програмованої логічної матриці Spartan-3 Starter Kit обсягом 200000 логічних елементів. Залежно від кількості комірок, які описують функції належності входів (32...128), час оброблення нечітких даних складає від 1 до 4,2 мкс, що підтверджує працездатність даного засобу та можливість його застосування у комп’ютерних системах з метою розподілу доступу до інформаційних ресурсів.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу наукову задачу – підвищення стійкості до часового аналізу підсистем розподілу доступу комп'ютерних систем в реальному часі з врахуванням наявних ресурсів самої системи на основі оптимального вибору методу модулярного експоненціювання.

Вирішення цієї задачі дає змогу зробити наступні висновки:

1. Аналіз сучасних атак на криптопристрої показав, що найпоширенішими є атаки на реалізацію, а особливо небезпечною є пасивна часова атака, яку важко виявити в процесі роботи підсистеми захисту інформації комп'ютерної системи.
2. Аналіз відомих методів доступу до інформації, що зберігається на сервері, показав, що необхідно враховувати стійкість каналу передачі даних до атак. Основними параметрами розподілу доступу в комп'ютерних системах є продуктивність, допустимі затрати пам'яті та стійкість до часового аналізу.
3. На основі визначених параметрів розподілу доступу та з врахуванням нечітких даних про клієнта запропоновано для побудови засобу розподілу доступу в комп'ютерних системах використати нечітку логіку, яка забезпечує достовірний результат в реальному часі.
4. У застосовуваних на сьогодні асиметричних алгоритмах шифрування основною операцією є модулярне експоненціювання. Проаналізовано найпоширеніші методи модулярного експоненціювання – бінарний, β-арний та метод ковзаючого вікна, що дозволило дослідити їх основні характеристики: продуктивність, затрати пам'яті та стійкість до атак.
5. Розроблено метод визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу, що базується на залежності часу виконання алгоритму модулярного експоненціювання від ваги Хемінга двійкового представлення ключа шифрування інформації, який може застосовуватись для аналізу стійкості будь-якого методу модулярного експоненціювання до часового аналізу.
6. Досліджено продуктивність, затрати пам'яті та нормовану стійкість до часового аналізу алгоритмів модулярного експоненціювання, в результаті чого визначено, що найкращими для застосування є β-арний метод та метод ковзаючого вікна модулярного експоненціювання зі зчитуванням бітів експоненти «зліва направо».
7. Розроблено метод оптимального вибору алгоритму модулярного експоненціювання, який базується на методі визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу та механізмі нечіткого висновку Мамдані, що дало змогу забезпечити зменшення часу реакції системи захисту інформації на зміну вхідних параметрів в реальному часі.
8. Розроблено метод оброблення нечітких даних для налаштування сервера шляхом попередньої обробки функцій належності входів, в результаті чого зменшено часову складність нечіткого висновку Мамдані на $O(n^2)$, що зменшує час реагування системи захисту інформації в 4 рази.
9. Вдосконалено структуру засобу розподілу доступу в комп'ютерних

системах, яка, на основі розробленого методу оброблення нечітких даних, адаптивно, з врахуванням наявних ресурсів комп'ютерної системи, вибирає оптимальний метод модулярного експоненціювання та в реальному часі змінює його при зміні середовища експлуатації.

10. Проведені дослідження в середовищі MatLab (засоби Fuzzy Logic Toolbox та Simulink) програмної версії засобу розподілу доступу в комп'ютерній системі показали, що відхилення результатів тестування пропонованого нечіткого контролера від нечіткого контролера, базованого на класичному механізмі Мамдані, в середньому становить 0,055, що цілком допустимо.

11. Розроблено структурну схему засобу визначення методу модулярного експоненціювання для сервера обміну даними за заданим каналом зв'язку та експериментально досліджено його швидкодію у симуляторі Electronics Workbench та середовищі ISO 10.3 проектування фірми Xilinx. Залежно від кількості комірок, які описують функції належності входів (від 32 до 128), час оброблення нечітких даних становить від 1 до 4,2 мкс, що підтверджує працездатність розробленого засобу.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Широчин В.П. Підвищення лінійної складності генераторів псевдовипадкових чисел, побудованих на основі регістрів зсуву / В.П.Широчин, І.В.Васильцов, Б.З.Карпінський, Л.О.Васильків // Всеукраинский межведомственный научно-технический сборник "Радиотехника". Тематический выпуск "Информационная безопасность" – 2003. - № 134. - С.181-184.

2. Васильцов І.В. Структура програмно-методичного комплексу «Спецкрипт-1.0» / І.В.Васильцов, Н.М.Васильків, Л.О.Васильків // Вісник Національного університету «Львівська політехніка». Комп'ютерні системи проектування. Теорія і практика. – 2003. - №471. – С.136-139.

3. Васильцов І.В. Стійкість сучасних алгоритмів модулярного експоненціювання до часового аналізу / І.В.Васильцов, Л.О.Васильків // Захист інформації. – 2005. - №1. - С. 54-69.

4. Карпінський М. Оцінка ризику витоку конфіденційної інформації внаслідок часового аналізу алгоритмів модулярного експоненціювання / М.Карпінський, І.Васильцов, Л.Васильків // Вісник Тернопільського державного технічного університету. – 2006. - №4. – С.135-144.

5. Васильцов І.В. Методи захисту проти атак спеціального виду / І.В.Васильцов, Л.О.Дубчак // Вісник Хмельницького національного університету. Технічні науки. – 2007. - №5. – С.174-182.

6. Васильцов І.В. Класифікація сучасних атак спеціального виду на реалізацію / І.В.Васильцов, Л.О.Дубчак // Захист інформації. – 2007. - №4. – С.10-21.

7. Карпінський М.П. Система для проведення криптоаналізу / М.П.Карпінський, Л.О.Дубчак, В.М.Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2008. - №9(127), Ч.2. – С.95-98.

8.Дубчак Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації / Л.О.Дубчак, Л.М.Тимошенко, Т.О.Яремчук //Інформаційна безпека. –2011. -№1(5). – С.112-116.

9.Дубчак Л.О. Модель апаратного засобу вибору методу модулярного експоненціювання / Л.О.Дубчак // Науковий вісник Чернівецького національного університету імені Юрія Федьковича. Серія: Комп'ютерні системи та компоненти. – 2011. - Т. 2, вип. 4. – С.44-48.

10.Дубчак Л.О. Спосіб обробки нечіткої інформації / Л.О.Дубчак // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. - № 8(179), Ч.1. – С. 306-309.

11.Дубчак Л.О. Метод обробки нечітких даних на основі механізму Мамдані /Л.О.Дубчак //Системи обробки інформації.– 2012. - №7(105). – С.131-134.

12.Karpinski M. Bezpieczenstwo informacji / M.Karpinski, T.Korkiszko, I.Wasylcow, L. Dubczak, U.Jacykowska, J.Kinach, A.Chominczuk, W.Karpinski, B.Karpinski, M.Aleksander, G.Litawa, L.Korkiszko. – Warszawa (PL): Wydawnictwo PAK, 2012. – 275 s. / Rozdz. 1, 4.

13.Карпінський М.П. Захист інформації на основі нечіткої системи / М.П.Карпінський, Л.О.Дубчак, Н.М.Васильків // Інформатика та математичні методи в моделюванні – 2011. - №3, Т.1. – С.236-242.

14.I.Vasyltsov. The Structure of the Program and Methodical Complex "Speccrypt-1.0" / I.Vasyltsov, N.Vasylkiv, L.Vasylkiv, J.Chajkivska // The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM 2003): VII–th International Conf., February 18-22, 2003: Proceedings. – Lviv-Slavske, Ukraine, 2003. – P.256.

15.Vasyltsov I. Investigation of Modern Exponentiation Algorithms / I.Vasyltsov, L.Vasylkiv, N.Vasylkiv, M.Chyrka // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2004): International Conf., 24-28 February, 2004: Proceedings. - Lviv-Slavsko, Ukraine, 2004. – P.291-293.

16.Vasyltsov I. Information Leakage Risk Estimation during Timing Analysis of Binary Method Modular Exponentiation / I.Vasyltsov, L.Vasylkiv, N.Vasylkiv, M.Chyrka // The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2005): VIII–th International Conf., February 23 – 26, 2005: Proceedings. - Lviv-Polyana, Ukraine, 2005. - P.124-126.

17.Karpinskyy M. Estimation of the Secret Information Leakage Risk during Timing Analysis of Binary Modular Exponentiation Method/ M.Karpinskyy, I.Vasyltsov, L.Vasylkiv // Advanced Computer Systems and Networks: Design and Application (ACSN-2005): 2-nd International Conf., September 21-23, 2005: Proceedings. - Lviv, Ukraine, 2005. - P.132-135.

18.Karpinskyy M. Comparative Analysis of Secret Information Leakage Risk during Timing Analysis of General Modular Exponentiation Methods / M.Karpinskyy, I.Vasyltsov, L.Vasylkiv // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2006): International Conf., February 28 - March 4, 2006: Proceedings. - Lviv-Slavske, Ukraine, 2006. – P.347-350.

19.Karpinskyy M. Secret Key Leakage caused by Hamming-weight Timing Analysis on Modular Exponentiation / M.Karpinskyy, L.Vasylkiv, M.Gizycki // Security & Management (SAM'06): 2006 International Conference, June 26-29, 2006: Proceedings. - Las Vegas, Nevada, USA, 2006. - P.179-185.

20.Карпінський М.П. Дослідження часової реалізації алгоритму електронного цифрового підпису RSA / М.П.Карпінський, Л.О.Дубчак, У.О.Яциковська // Актуальные проблемы научных исследований – 2007: III междунар. науч.-практ. конф., 15-30 июня 2007г.: материалы. - Днепропетровск, 2007. - Т.7. - С.42-48.

21.Гіжицкі М. Аналіз безпеки протоколів керування комп'ютерною мережею / М.Гіжицкі, Л.Дубчак, Т.Строньскі // Дванадцята наукова конференція Тернопільського державного технічного університету імені Івана Пулюя, 14-15 травня 2008р.: матеріали. – Тернопіль, 2008. - С.88.

22.Чайківська Ю.М. Аналіз стійкості алгоритмів Монтгомері до атак спеціального виду / Ю.М.Чайківська, Л.О.Дубчак, Л.М.Тимошенко // Методи та засоби кодування, захисту й ущільнення інформації: Друга міжнар. наук.-практ. конф., 22-24 квітня, 2009р.: тези доп. – Вінниця, 2009. - С.110-111.

23.Дубчак Л.О. Спосіб вибору методу модулярного експоненціювання для забезпечення стійкості комп'ютерної системи до часового аналізу / Л.О.Дубчак, М.П.Карпінський //Проблеми впровадження інформаційних технологій в економіці: VIII-а міжнар. конф., 28-30 березня 2012 р.: матеріали. - К., 2012. – С.289-291.

24.Дубчак Л.О. База правил нечіткої системи вибору методу модулярного експоненціювання / Л.О.Дубчак // Сучасні комп'ютерні інформаційні технології (АСІТ'2012): II Всеукраїнська школа-семінар молодих вчених і студентів , 4-5 травня, 2012р.: матеріали – Тернопіль, 2012. - С.202.

АНОТАЦІЯ

Дубчак Л.О. Методи та засоби розподілу доступу в комп'ютерних системах на основі нечіткої логіки. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Тернопільський національний економічний університет, Тернопіль, 2013.

Дисертація присвячена розробці методів та засобів для здійснення розподілу доступу в комп'ютерних системах з метою захисту інформації від часового аналізу в реальному часі.

У роботі досліджено методи розподілу доступу до інформації, що зберігається на сервері, сучасні атаки на реалізацію криптопристроїв та методи їх протидії. Це дало змогу ідентифікувати найбільш небезпечну пасивну атаку на системи захисту інформації, а саме, часовий аналіз. Визначено найпоширеніші методи модулярного експоненціювання, які є основною операцією сучасних асиметричних криптосистем. Запропоновано метод визначення нормованої стійкості до часового аналізу кожного з цих методів, що базується на залежності часу виконання алгоритму від ваги Хемінга. Досліджено продуктивність, затрати пам'яті та стійкість методів модулярного експоненціювання до часового аналізу, що є

основними параметрами розподілу доступу в комп'ютерних системах. Розроблено метод оптимального вибору алгоритму модулярного експоненціювання для розподілу доступу в комп'ютерних системах на основі механізму нечіткого висновку Мамдані. Розроблено метод оброблення нечітких даних для налаштування сервера, що має нижчу складність, ніж класичний механізм нечіткого висновку Мамдані, чим пришвидшує роботу підсистеми захисту інформації комп'ютерної системи в 4 рази. Здійснено моделювання та дослідження засобу розподілу доступу в комп'ютерних системах на основі розробленого методу оброблення нечітких даних, що підтверджують його працездатність та можливість застосування у комп'ютерних системах з метою розподілу доступу до інформаційних ресурсів.

Ключові слова: комп'ютерна система, розподіл доступу, часова атака, асиметрична криптосистема, нечіткі дані, засіб розподілу доступу.

АННОТАЦИЯ

Дубчак Л.О. Методы и средства распределения доступа в компьютерных системах на основе нечеткой логики. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Тернопольский национальный экономический университет, Тернополь, 2013.

Диссертация посвящена разработке методов и средств для осуществления распределения доступа в компьютерных системах с целью защиты информации от временного анализа в реальном времени.

В работе исследованы методы распределения доступа к информации, хранящейся на сервере, современные атаки на реализацию криптосредств и методы их противодействия. Это позволило идентифицировать наиболее опасную пассивную атаку на системы защиты информации, а именно, временной анализ.

Определены самые распространенные методы модулярного экспоненциирования, которые являются основной операцией современных асимметрических криптосистем, а именно бинарный, β-арный и метод скользного окна. Предложен метод определения нормируемой устойчивости к временному анализу каждого из этих методов, основанный на зависимости времени выполнения алгоритма от веса Хемминга. Исследованы производительность, объём используемой памяти и устойчивость методов модулярного экспоненциирования к временному анализу, являющиеся основными параметрами распределения доступа в компьютерных системах. Определено, что для обеспечения эффективной работы системы и её устойчивости к временному анализу можно использовать β-арный и метод скользного окна со считыванием бит экспоненты «слева направо».

Разработан метод оптимального выбора алгоритма модулярного экспоненциирования для распределения доступа в компьютерных системах на основе механизма нечеткого вывода Мамдани. Разработан метод обработки нечетких данных для настройки сервера, имеющий низшую сложность, чем классический механизм нечеткого вывода Мамдани, за счёт разделения на этапы обучения и эксплуатации процесса нечёткого вывода, чем ускоряет работу

подсистемы защиты информации компьютерной системы в 4 раза.

Осуществлено моделирование и исследование средства распределения доступа в компьютерных системах на основе разработанного метода обработки нечетких данных, подтверждающие его работоспособность и возможность применения в компьютерных системах с целью распределения доступа к информационным ресурсам.

Ключевые слова: компьютерная система, распределение доступа, временная атака, асимметрическая криптосистема, нечёткие данные, средство распределения доступа.

ANNOTATION

Dubchak L.O. Methods and means for distribution of access to computer systems based on fuzzy logic. – Manuscript.

Thesis for the Ph.D. degree of technical sciences by specialty 05.13.05 – Computer Systems and Components. – Ternopil National Economical University, Ternopil, 2013.

The thesis is devoted to development of methods and means for the distribution of access to computer systems to protect information from timing analysis in real time.

In this work, the methods of distribution of access to information, stored on a server, modern attacks on the implementation of crypto devices and methods of resisting those attacks were researched. This made it possible to identify the most dangerous passive attack on the information protection systems, which is timing analysis. The most common methods of modular exponentiation determined, which are the basic operations of modern asymmetric cryptosystems. The method of determination of the normalized resistance to timing analysis of each of these methods was proposed, based on the dependence of the algorithm execution time on the Hamming weight. Performance was explored, memory consumption and resistance of methods of modular exponentiation to timing analysis, which are the main parameters of the access distribution in computer systems. A method of selecting an optimal algorithm for modular exponentiation for access distribution in computer systems based on the mechanism of Mamdani fuzzy conclusion was developed. A method of processing fuzzy data for server configuration was developed, which has lower complexity than the classical mechanism of Mamdani fuzzy conclusion, thus accelerating up to 4 times the work of information protection subsystem of computer system. Modeling and analysis of access distribution tool in computer systems on the basis of the developed method of processing fuzzy data was made, proving its efficiency and applicability in computer systems for sharing access to information resources.

Keywords: computer system, distribution of access, timing attack, asymmetrical cryptosystem, fuzzy datas, means of distribution access.