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

На правах рукопису

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

Дисертація на здобуття наукового ступеня кандидата технічних наук

Науковий керівник
Карпінський Микола Петрович
д.т.н., професор

Тернопіль − 2012

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КС – комп’ютерна система;

ЕМ – електромагнітне;

RSA – абревіатура прізвищ Rivest, Shamir та Adleman;

IP – Internet Protocol;

ЛОМ – локальна обчислювальна мережа;

ТЗОІ – технічний засіб обробки інформації;

ЕОМ – електронно-обчислювальна машина;

PIN – Personal Identification Number;

ПЛІС – програмована логічна інтегральна схема;

DES - Data Encryption Standard;

SPA – Simple Power Analysis;

ЕЦП - електронний цифровий підпис.

ВСТУП

Актуальність теми. Сучасні 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 [1-3].

Комп'ютерні системи функціонують в жорстких умовах експлуатації, тому необхідно враховувати на етапах їх розробки та впровадження не тільки швидкодію, мінімізацію фінансових витрат, але й стійкість до атак. Отже, виникає необхідність моделювання процесу експлуатації комп'ютерної системи ще 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.

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 [4].

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" (англ. мовою side-channel attacks, covert-channel attacks) [5,6,7].

Проблемі захисту комп'ютерних систем та мереж передачі інформації від атак на реалізацію присвячені дослідження відомих науковців, зокрема Е.Біхама, А.Шаміра, Ж.-Ж.Кеске, В.О.Хорошка, А.О.Чекаткова, В.П.Широчина та ін.

Для безпечної експлуатації комп'ютерних систем необхідно застосовувати програмно-апаратні засоби протидії пасивним типам атак з врахуванням обчислювальних ресурсів самих систем. Крім того, інформація, що зберігається на сервері, може мати різні рівні таємності, отже виникає

необхідність розподілу доступу.

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. Дана 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 різного рівня конфіденційності в комп'ютерних системах 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.

В результаті виконаного дисертаційного дослідження:

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 мережі.

2) розроблені методи за рахунок їх комбінованого використання 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) розроблена і реалізована оригінальна структура засобу розподілу доступу в комп'ютерних системах, 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 "Захист інформації в комп'ютерних системах", «Комп'ютерна криптографія», «Моделювання комп'ютерних систем».

Особистий внесок здобувача. Усі основні результати, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих у співавторстві, здобувачу належать: визначення залежності часу виконання алгоритмів сучасних методів модулярного експоненціювання від ваги Хемінга, метод визначення нормованої стійкості методів модулярного експоненціювання до часового аналізу, імовірнісна оцінка ризику витоку інформації під час проведення часового аналізу, формулювання рекомендацій щодо побудови криптосистем, стійких до часового аналізу, визначення основних параметрів комп'ютерної системи захисту інформації та розподілу доступу, побудова нечіткої системи вибору методу модулярного експоненціювання на основі механізму Мамдані, метод вибору алгоритму модулярного експоненціювання на основі класичного механізму нечіткого висновку Мамдані з розподілом процесу на етапи навчання та експлуатації, розробка засобу обробки нечіткої інформації для реалізації розподілу доступу в комп'ютерній системі.

Апробація результатів дисертації. Основні результати дисертації були висвітлені та обговорені на науково-технічних конференціях: VII міжнародній науково-технічній конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" (CADSM'2003) (Львів-Славське, 2003); міжнародній науково-технічній конференції "Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії" (TCSET'2004) (Львів-Славське, 2004); VIII міжнародній науково-технічній конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" (CADSM'2005) (Львів-Поляна, 2005); 2-ій міжнародній науково-технічній конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN-2005) (м.Львів, 2005); міжнародній науково-технічній конференції "Сучасні проблеми радіоінженерії, телекомунікацій та комп'ютерних наук" (TCSET'2006) (Львів-Славсько, 2006); міжнародній конференції "Безпека та менеджмент" (SAM'06) (Лас Вегас, США, 2006); III міжнародній науково-практичній конференції "Актуальные проблемы научных исследований - 2007" (м.Дніпропетровськ, 2007); дванадцятій науковій

конференції Тернопільського державного технічного університету імені Івана Пулюя (м.Тернопіль, 2008); другій міжнародній науково-практичній конференції «Методи та засоби кодування, захисту й ущільнення інформації» (м.Вінниця, 2009); 8-ій 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. Всього за темою дисертаційної роботи опубліковано 24 наукові праці, які містять 1 монографію (1, 4 розділи), 12 статей, з них 11 - у фахових виданнях, що входять до переліку, затвердженому ВАК України, 11 праць у збірниках наукових конференцій.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КС – комп’ютерна система;

ЕМ – електромагнітне;

RSA – абревіатура прізвищ Rivest, Shamir та Adleman;

IP – Internet Protocol;

ЛОМ – локальна обчислювальна мережа;

ТЗОІ – технічний засіб обробки інформації;

ЕОМ – електронно-обчислювальна машина;

PIN – Personal Identification Number;

ПЛІС – програмована логічна інтегральна схема;

DES - Data Encryption Standard;

SPA – Simple Power Analysis;

ЕЦП - електронний цифровий підпис.

ВСТУП

Актуальність теми. Сучасні 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 [1-3].

Комп’ютерні системи функціонують в жорстких умовах експлуатації, тому необхідно враховувати на етапах їх розробки та впровадження не тільки швидкодію, мінімізацію фінансових витрат, але й стійкість до атак. Отже, виникає необхідність моделювання процесу експлуатації комп’ютерної системи ще 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.

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 [4].

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” (англ. мовою side-channel attacks, covert-channel attacks) [5,6,7].

Проблемі захисту комп’ютерних систем та мереж передачі інформації від атак на реалізацію присвячені дослідження відомих науковців, зокрема Е.Біхама, А.Шаміра, Ж.-Ж.Кеске, В.О.Хорошка, А.О.Чекаткова, В.П.Широчина та ін.

Для безпечної експлуатації комп’ютерних систем необхідно застосовувати програмно-апаратні засоби протидії пасивним типам атак з врахуванням обчислювальних ресурсів самих систем. Крім того, інформація, що зберігається на сервері, може мати різні рівні таємності, отже виникає необхідність розподілу доступу.

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. Дана 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 різного рівня конфіденційності в комп'ютерних системах 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:

5. 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.

6. 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.

7. 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.

8. 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.

В результаті виконаного дисертаційного дослідження:

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 мережі.

2) розроблені методи за рахунок їх комбінованого використання 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) розроблена і реалізована оригінальна структура засобу розподілу доступу в комп'ютерних системах, 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 "Захист інформації в комп'ютерних системах", «Комп'ютерна криптографія», «Моделювання комп'ютерних систем».

Особистий внесок здобувача. Усі основні результати, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих у співавторстві, здобувачу належать: визначення залежності часу виконання алгоритмів сучасних методів модулярного експоненціювання від ваги Хемінга, метод визначення нормованої стійкості методів модулярного експоненціювання до часового аналізу, імовірнісна оцінка ризику витоку інформації під час проведення часового аналізу, формулювання рекомендацій щодо побудови криптосистем, стійких до часового аналізу, визначення основних параметрів комп'ютерної системи захисту інформації та розподілу доступу, побудова нечіткої системи вибору методу модулярного експоненціювання на основі механізму

Мамдані, метод вибору алгоритму модулярного експоненціювання на основі класичного механізму нечіткого висновку Мамдані з розподілом процесу на етапи навчання та експлуатації, розробка засобу обробки нечіткої інформації для реалізації розподілу доступу в комп'ютерній системі.

Апробація результатів дисертації. Основні результати дисертації були висвітлені та обговорені на науково-технічних конференціях: VII міжнародній науково-технічній конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" (CADSM'2003) (Львів-Славське, 2003); міжнародній науково-технічній конференції "Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії" (TCSET'2004) (Львів-Славське, 2004); VIII міжнародній науково-технічній конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" (CADSM'2005) (Львів-Поляна, 2005); 2-ій міжнародній науково-технічній конференції "Сучасні комп'ютерні системи та мережі: розробка та використання" (ACSN-2005) (м.Львів, 2005); міжнародній науково-технічній конференції "Сучасні проблеми радіоінженерії, телекомунікацій та комп'ютерних наук" (TCSET'2006) (Львів-Славсько, 2006); міжнародній конференції "Безпека та менеджмент" (SAM'06) (Лас Вегас, США, 2006); III міжнародній науково-практичній конференції "Актуальные проблемы научных исследований - 2007" (м.Дніпропетровськ, 2007); дванадцятій науковій конференції Тернопільського державного технічного університету імені Івана Пулюя (м.Тернопіль, 2008); другій міжнародній науково-практичній конференції «Методи та засоби кодування, захисту й ущільнення інформації» (м.Вінниця, 2009); 8-ій міжнародній конференції «Проблеми впровадження інформаційних технологій в економіці» (м.Ірпінь, 2012); II Всеукраїнській школі-семінарі «Сучасні комп'ютерні інформаційні технології» (ACIT'2012) (м.Тернопіль, 2012).

Публікації. Всього за темою дисертаційної роботи опубліковано 24 наукові праці, які містять 1 монографію (1, 4 розділи), 12 статей, з них 11 - у фахових виданнях, що входять до переліку, затвердженому ВАК України, 11 праць у збірниках наукових конференцій.

РОЗДІЛ 1
СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ РОЗПОДІЛУ ДОСТУПУ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Особливості розподілу доступу та загроз в комп'ютерній системі

Згідно міжнародної конвенції про кіберзлочинність, комп'ютерна система (КС) – це будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичну обробку даних [1].

Розподілені комп'ютерні системи реалізуються на основі обчислювальних мереж та віддалених процесорів-сателітів, які обслуговуються та інформаційно взаємодіють з одним або багатьма системними серверами [2].

Архітектура клієнт-сервер є однією з найпопулярніших концепцій при створенні комп'ютерних інформаційних систем. В цій архітектурі передбачені наступні компоненти:

– серверна частина (збереження і обробка інформації);

– клієнтська частина (робочий інструмент користувача);

– мережа, яка забезпечує взаємодію (обмін інформацією) між клієнтом і сервером.

Саме на цій архітектурі і базуються більшість веб-орієнтованих систем.

Такі системи можуть бути надзвичайно різноманітними і розгалуженими. Перевагами веб-орієнтованих систем, базованих на клієнт-серверній архітектурі, є [3, 5]: мінімум затрат на обслуговування бізнес-процесів, максимальна оперативність при оперуванні даними, зручність в обслуговуванні, мінімум затрат на комунікації між підрозділами компанії, зв'язок з системою можна здійснювати з будь-якого комп'ютера, що приєднаний до Інтернету.

Кожен клієнт комп'ютерної мережі ідентифікується своєю IP-адресою,

а також має свою «історію» користування системою обробки та передачі інформації відносно наявності збоїв чи втрати інформації під час передачі шифротексту. Така інформація зберігається на сервері, який присвоює клієнту свій рівень доступу до інформації (рисунок 1.1).

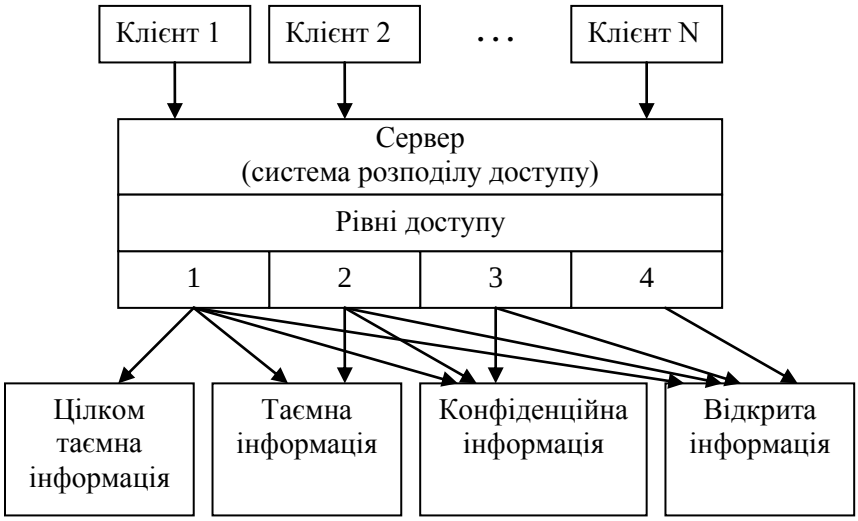


Рисунок 1.1 - Рівні доступу клієнтів комп'ютерної системи до інформації

Проте, коли зловмисник здійснює часову атаку чи підміну IP-адреси, неможливо однозначно забезпечити стійкість криптосистеми [1, 3].

Ефективність взаємодії комп'ютерів у рамках локальної комп'ютерної мережі значною мірою визначається використовуваним правилом доступу до сервера. Правило, згідно з яким організовується доступ робочих станцій до концентратора, називається методом доступу. Різноманіття локальних мереж і вимог до них перешкоджає у визначенні універсального, найефективнішого у всіх випадках методу доступу [8-10]. Існує два основних типи доступу в мережі – детермінований та випадковий доступ [5].

Детермінований доступ припускає наявність певного алгоритму, на підставі якого робочим станціям надається доступ до інформації на сервері. Алгоритм надання права передачі інформації може бути доволі гнучким і враховувати пріоритет запитів на передачу та їх інтенсивність. Для нормального функціонування мережі необхідно, щоб вона не знаходилася в

режимі насичення, тобто навантаження на мережу не повинні перевищувати її пропускну здатність. Загалом, методи детермінованого доступу дозволяють враховувати особливості топології мережі та характер інформації, що передається, забезпечуючи найбільш ефективне використання передавального середовища.

Другу групу методів доступу складають методи випадкового доступу, які дозволяють кожній робочій станції довільним чином, незалежно від інших систем, звертатись до сервера. Випадкові методи доступу передбачають можливість захоплення загального поділюваного середовища передачі даних будь-яким вузлом мережі у довільний випадковий момент часу. Через це не виключена можливість одночасного захоплення середовища двома або більше станціями мережі, що призводить до помилок передачі даних. Таке явище називається колізією.

Детерміновані методи, навпаки, передбачають можливість надання загального середовища в розпорядження вузла мережі за чітко визначеним (детермінованим) порядком в реальному часі. При використанні детермінованих методів колізії неможливі, але ці методи є більш складними в реалізації і збільшують вартість мережевого обладнання. Тому врахування поточних параметрів сервера в момент доступу робочої станції є важливою задачею.

Оскільки доступ до інформації в більшості КС здійснюється віддалено через Інтернет, то необхідно забезпечити захист інформації від несанкціонованого доступу.

Загрози для комп’ютерних систем можуть класифікуватися за дев’ятьма ознаками [4]:

1. За метою реалізації загрози: порушення конфіденційності інформації; порушення цілісності інформації; порушення працездатності комп’ютерних систем.

2. За принципом впливу на КС:

– з використанням доступу суб’єкта системи (користувача, процесу) до

об’єкта (файла даних, каналу зв’язку тощо);

–з використанням прихованих каналів (шляхів передачі інформації, які дають змогу двом взаємодіючим процесам обмінюватися інформацією таким способом, що порушує системну політику безпеки).

Втручання, засновані на першому принципі, простіші, більш інформаційні та від них легше захиститись. Втручання на основі другого принципу відрізняється важкістю організації, меншою інформаційністю, складністю виявлення і усунення.

3. За характером впливу на КС:

–активна загроза, що веде до зміни стану системи і може здійснюватися або з використанням доступу, або як з використанням доступу, так і з використанням прихованих каналів;

–пасивна загроза, що здійснюється шляхом спостереження користувачем будь-яких побічних ефектів та їх аналізу. Прикладом пасивного впливу може бути прослуховування лінії зв’язку між двома вузлами мережі. Пасивний вплив не веде до зміни стану системи. Він завжди пов’язаний тільки з порушенням конфіденційності інформації в КС.

4. За причиною використовуваної помилки захисту, яка може бути зумовлена однією з наступних причин:

–невідповідністю політики безпеки реальній КС;

–помилками адміністративного управління, під якими розуміють некоректну реалізацію або підтримку прийнятої політики безпеки КС;

–помилками в алгоритмах, у зв’язках між ними тощо, які виникають на етапі проектування програми або комплексу програм, у зв’язку з чим їх можна використовувати зовсім не так, як це описано в документації;

–помилками реалізації алгоритмів (помилками кодування), зв’язками між ними тощо, які виникають на етапі реалізації або відлагодження і які також можуть бути джерелом недокументованості.

5. За способом впливу на об’єкт атаки (при активному впливі):

–безпосередній вплив на об’єкт атаки (таким діям звичайно легко

запобігти з допомогою засобів контролю доступу);

–вплив на систему дозволу (в тому числі загарбання привілеїв);

–опосередкований вплив (через інших користувачів);

–“маскарад”, у цьому разі користувач присвоює собі повноваження іншого користувача, видаючи себе за нього;

–“користувач наосліп” – коли один користувач змушує іншого виконувати необхідні дії, причому останній про них може і не підозрювати; для цього може використовуватися вірус (він виконує необхідні дії та повідомляє тому, хто його впровадив, про результат).

6. За способом впливу на КС: в інтерактивному режимі та в пакетному режимі.

7. За об’єктом атаки:

–КС в цілому (проникнення в систему), для цього, як правило, використовують метод “маскараду”, перехоплення або підробки пароля, “злом” та доступ до КС через мережу;

–об’єкти КС — дані або програми, самі пристрої системи, канали передачі даних;

–суб’єкти КС — процеси і підпроцеси користувачів, частим випадком такого впливу є введення зловмисником віруса в середовище іншого процесу і його виконання від імені цього процесу;

–канали передачі даних — пакети даних, які передаються каналами зв’язку, і власне канали, прослуховування каналу і аналіз трафіка (потоку повідомлень, підміна або модифікація повідомлень у каналах зв’язку і на вузлах-ретрансляторах, зміна топології та характеристик мережі).

8. За використовуваними засобами атаки (використовується або стандартне програмне забезпечення, або спеціально розроблені програми).

9. За станом об’єкта атаки. Об’єкт атаки може знаходитись в одному із трьох станів:

–збереження — вплив на об’єкт, як правило, здійснюється з використанням доступу;

–передачі — вплив передбачає або доступ до фрагментів інформації, що передається, або просто прослуховування з використанням прихованих каналів;

–обробки — об’єктом атаки є процес користувача.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації в комп’ютерній системі [3, 11]:

– контроль доступу (перевірка IP-адреси кожного одержаного пакету, обмеження доступу за допомогою паролів, застосування програмних засобів);

– розширення парольного захисту (відповідь на віддалений виклик, тобто перевірка паролю «передзвонюванням», безупинне квитирування зв’язку – система, при якій сервер постійно опитує клієнтський комп’ютер протягом усього сеансу підключення);

– шифрування (найпопулярнішою асиметричною системою захисту інформації є RSA-шифрування, яке дозволяє створювати стійкий цифровий підпис);

– використання брандмауерів (комбінація апаратного і програмного забезпечення для запобігання доступу з Інтернету до інформації).

Проте ці підходи не забезпечують повну стійкість системи, оскільки зловмисник може підмінити IP-адресу, перехопити пакети даних, що передаються по каналу зв’язку, і таким чином дізнатися пароль. Тому для забезпечення стійкості комп’ютерної системи, яка використовує мережу типу клієнт-сервер для передачі даних, необхідно враховувати найнебезпечніші атаки, що можуть здійснюватися по побічних каналах витоку інформації.

1.2 Сучасні атаки спеціального виду на канали передачі даних в комп’ютерних системах

Кількість зареєстрованих мережевих вторгнень за рік становить сотні тисяч. Проте вважається, що 80% комп'ютерних злочинів не попадає в офіційну статистику, оскільки жертви бояться розголосу, який може підірвати довіру до них партнерів і клієнтів [12].

За підсумками 2011 року Україна на 8 щаблів - з 31 на 23 - піднялася у світовому рейтингу країн за найбільшою кількістю кібер-загроз і вперше увійшла до десятки країн з найбільшою кількістю мережевих атак [13].

Сучасні системи обробки інформації являють собою складні програмно-апаратні комплекси, які володіють специфічними каналами витоку інформації, що супроводжують штатний процес обробки інформаційних ресурсів.

Таким чином, комп'ютерні системи піддаються широкому спектру потенційних загроз, що обумовлює необхідність передбачити великий перелік функцій та підсистем захисту. В першу чергу необхідно забезпечити захист найбільш інформативних каналів витоку інформації.

Проблема перекриття цих каналів ускладнюється тим, що процедури захисту даних не повинні приводити до помітного зниження продуктивності КС [6].

На рисунку 1.2 зображено модель типового процесу передачі інформації по незахищених каналах зв'язку із врахуванням нестандартних каналів витоку інформації від адресата *A* до адресата *B* [4].

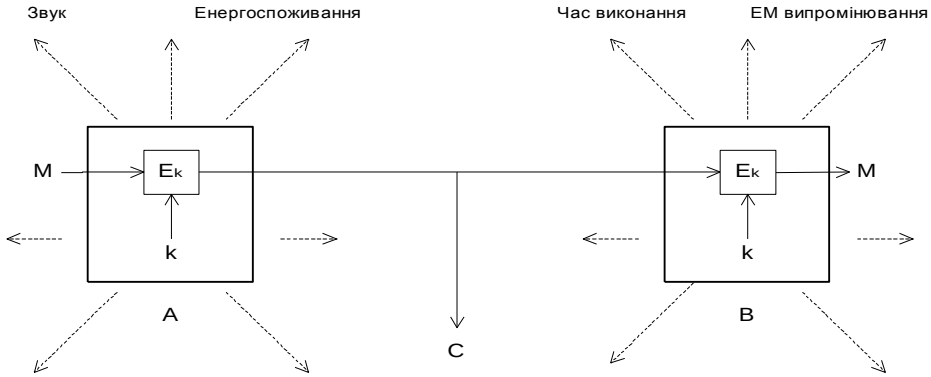


Рисунок 1.2 - Модель типового процесу передачі інформації по незахищених каналах зв'язку

З рисунку 1.2 видно, що окрім каналу, по якому передається шифротекст *C* (який традиційно утворюється шляхом криптографічного перетворення *E* вхідного повідомлення *M* за умови використання ключа *k* та може бути доступним зловмиснику в умовах виконання пасивної атаки прослуховування), існує також інша додаткова інформація, що може бути використана криптоаналітиком для ефективної реалізації атаки на систему захисту інформації: звук, енергоспоживання, час виконання, електромагнітне (ЕМ) випромінювання і т.п. У [7, 11] показано, що така додаткова інформація дозволяє різко підвищити ймовірність успішного виконання атаки за рахунок зменшення її складності.

Відповідно до способів перехоплення інформації, до фізичної природи каналів передачі даних, а також до середовища розповсюдження, канали витоку та перехоплення інформації можна розділити на електромагнітні, електричні, акустичні, кабелі локальних обчислювальних мереж (ЛОМ), візуальні, індукційні, параметричні, закладки та віруси [4, 14-23].

Для електромагнітних каналів характерним є побічне випромінювання елементів і високочастотних генераторів технічних засобів обробки інформації (ТЗОІ) та самозбудження підсилювачів низької частоти ТЗОІ [4, 16, 24].

Середовищем акустичних каналів витоку та перехоплення інформації можуть бути повітря, конструкції будівель, труби водопостачання та опалення, а також інші тверді тіла [15-18]. Слід зауважити, що акустичні канали можуть бути джерелом витоку не лише мовної інформації, але й інформації з механічних замків, ключів, інформації з принтера чи клавіатури ЕОМ тощо.

Кабелі ЛОМ виділені в окрему групу, оскільки сучасні системи обробки інформації побудовані на базі локальних комп’ютерних мереж і, як правило, таке кабельне господарство являє собою розвинуту мережу провідників різного типу. Кабельна система не містить в собі активних чи

нелінійних елементів, тому сама по собі не може бути джерелом “побічних” випромінювань, проте пов’язує між собою всі елементи комп’ютерної мережі. По ній передаються мережеві дані, але також вона є і приймачем усіх паразитних наведень і середовищем для перенесення побічних ЕМ випромінювань [15].

Візуальні канали витоку інформації широко використовувалися в епоху докомп’ютерного захисту інформації та продовжують застосовуватися і тепер [25, 26]. Для цього використовують спеціальні технічні засоби оптичного, теплового та іншого випромінювання.

Хімічна комбінаторна атака - це спеціальний вид атаки на клавіатуру [18], яка полягає у нанесенні на кожну клавішу клавіатури невеликої кількості (кілька іонів) різних солей солі (наприклад, NaCl, KCl, LiCl, $SrCl_2$ і т.д.). В процесі натискання користувачем PIN-коду солі змішуються, що дає змогу використати таку інформацію для атаки.

Звукова атака - класичний спосіб атаки на криптосистему з механічними та електричними замками, кодовими клавіатурами і т.п., які під час виконання різних операцій (наприклад, набір PIN-коду банкомата) видають звуки [27].

Окремою категорією виділено атаки на реалізацію, найпоширенішими з яких є [28]:

1) фізична атака полягає у дослідженні особливостей реалізації пристрою в мікросхемі, щоб отримати інформацію про алгоритми чи визначити секретні ключі шляхом дослідження області всередині кристалу ПЛІС [16];

2) оптична атака апаратних помилок (відноситься до фізичних напівруйнівних атак) полягає у генеруванні збоїв у пристрої та подальшому застосуванні диференційного криптоаналізу помилок [29];

3) зчитування ЕМ випромінювання – кожен компонент криптопристрою виділяє різні типи ЕМ випромінювань, вони дозволяють отримати різні “описи” подій, що відбуваються протягом кожного

синхроімпульсу (в цьому полягає відмінність від атаки аналізу енергоспоживання, в якій в кожен момент часу доступний лише один “опис” зміни потоку струму, і пояснення, чому даний вид атаки є ефективнішим). Детальніший опис атаки такого виду можна знайти у [30];

4) атака апаратних помилок – порушник має доступ до апаратури захисту інформації і може проводити штатні операції стосовно криптографічного перетворення вхідних даних, а також спеціальним чином впливати на процес обробки інформації, щоб спричинити некоректну роботу засобів захисту інформації, а відтак отримати спотворений шифротекст. Подальша робота полягає в аналізі криптотексту, отриманого у нормальному режимі роботи та у режимі виникнення помилок. Незважаючи на очікувану велику складність такого процесу, Е.Біхам та А.Шамір теоретично довели, що в загальному випадку достатньо від 50 до 200 пар незалежних криптотекстів для зламу найпоширенішого симетричного алгоритму DES (Data Encryption Standard) [31-33];

5) атака на час виконання окремих операцій (часова атака). Час виконання криптографічних операцій залежить не лише від ефективності реалізації конкретного алгоритму, але й також (інколи суттєво) від вхідних даних [34-38]. Особливо сильно така кореляція проявляється для алгоритмів модулярного експоненціювання асиметричних криптосистем та алгоритмів додавання (множення) точок на еліптичній кривій [39, 40]. Як правило, ці вказані криптографічні операції є обчислювально складними, і для підвищення продуктивності виконання процедури шифрування повідомлення чи формування цифрового підпису використовують спеціальні алгоритми, які базуються на оцінці бітової інформації ключа шифрування. Така оцінка в алгоритмах дозволяє пришвидшити виконання криптографічних операцій за рахунок обходу виконання деяких операцій алгоритму при нульових бітах ключа. Звідси очевидно, що завжди можна виявити певну кореляцію між кількістю одиничних бітів ключа та часом виконання такого алгоритму. Саме така інформація дозволяє зловмиснику висунути гіпотезу щодо кількості

одиничних та нульових бітів у секретному ключі, кількісним еквівалентом якої може бути вага Хемінга, а на основі такої оцінки здійснити атаку повного перебору в певному піддіапазоні ключового простору, що потребує значно менших обчислювальних ресурсів [39]. Таким чином, оцінка кореляції часу виконання криптографічних операцій та ваги Хемінга ключової інформації дозволяє зловмиснику зменшити складність атаки на систему захисту інформаційних ресурсів;

6) атака енергоспоживання. Електронні пристрої споживають струм з джерела струму протягом виконання операцій. Струм споживання змінюється в залежності від типів операцій, які ці пристрої виконують. Джерела струму більшості пристроїв надають константне значення енергії, тому зрозуміло, що енергія, яку споживає пристрій в процесі роботи, є пропорційною до споживаного струму. Для здійснення атаки зловмисник може використовувати або аналіз особливостей асиметрії, або ж аналіз імпульсів, що виникають в колі джерела живлення [41-48].

Атакам сторонніми каналами витоку інформації властива менша потужність, ніж традиційним атакам, основаним на математичному аналізі криптографічного алгоритму, але разом з тим вони суттєво дієвіші. Їх дослідження висвітлені у [30, 33, 34, 49]. Найнебезпечнішою атакою такого типу для комп'ютерної системи є часова атака [50, 51], тому розробка методів протидії сучасним атакам сторонніми каналами витоку інформації є актуальною задачею.

Існує велика кількість різноманітних підходів і методів, що дозволяють захистити криптографічні пристрої від різних атак спеціального виду [4, 52-77], описаних вище.

Одним із відомих традиційних та універсальних методів захисту є метод дворазового обчислення та перевірки [4]. Суть методу полягає у проведенні двох паралельних обчислень з одними і тими ж вхідними даними та перевірці результатів на ідентичність. При послідовному виконанні цих операцій за умови існування довготривалих збоїв в апаратній частині

криптосистеми існує ймовірність проведення успішної атаки, проте алгоритм може бути легко модифікований для усунення цієї проблеми шляхом застосування інверсних операцій.

До переваг такого методу слід віднести його універсальність (такий метод може використовуватися як для симетричних, так і асиметричних систем) та простоту реалізації, а недоліком є дублювання обчислювальних ресурсів, в результаті чого значно знижується продуктивність системи та зростають апаратні затрати.

Існує узагальнена класифікація способів захисту проти атак спеціального виду на криптопристрої, побудована на основі виділення ряду ознак, що детальніше розглянуті нижче [4].

За типом імплементації – дана ознака визначає, як саме повинен реалізуватися метод та які підходи лежать в його основі. Розрізняють такі типи засобів захисту: апаратні, програмні, конструктивні, піротехнічні та топологічні. Наприклад, для досягнення високого рівня швидкодії та високого ступеня захисту метод повністю може бути реалізований апаратно. Для боротьби з атаками, що базуються на аналізі енергоспоживання, інколи використовують спеціальні конструкції зчитувачів (наприклад, в банкоматах), які унеможливлюють використання емуляторів смарт-карток, наприклад, шляхом використання механічних різців, що обтинають будь-які проводи та шини, які виходять за межі зчитувача. Піротехнічні методи полягають у використанні спеціальних порохових мікрозапалів в пристрої, призначених для його самознищення в разі несанкціонованого доступу чи спробі виявити особливості його реалізації.

За прикладним використанням – дана ознака визначає міру захисту даного методу від певного класу атак. Наприклад, маскування таємного ключа в асиметричних криптосистемах чи на основі еліптичних кривих дозволяє одночасно захистити пристрій від атак аналізу енергоспоживання. Тому такий метод, що дозволяє здійснити одночасно захист від декількох атак певного типу, можна назвати універсальним. З іншого боку, існують

методи, здатні захистити пристрій лише від однієї з типових атак. Прикладом може бути алгоритм “double-and-add always”, який дозволяє здійснити захист лише від атаки SPA (Simple Power Attack – проста атака аналізу енергоспоживання) на еліптичні криві, але як в полі простих чисел, так і двійкових [48]. Такі методи можна назвати комплексними. Окрім того, існують досить вузькі методи захисту, що використовують певну специфіку конкретного алгоритму шифрування і дозволяють здійснити захист лише від однієї конкретної атаки. Такі методи називають частковими.

За типом доведення методу – дана ознака визначає спосіб доведення дієвості методу захисту. Розрізняють методи, побудовані на основі формального доведення, які є повними та, як правило, універсальними, але таке формальне доведення не завжди може бути легко реалізованим. Інший клас методів захисту доводить дієвість методу на основі експериментальних даних. Такі методи легше будувати, але використовувати їх небезпечніше, оскільки навіть незначна модифікація атаки чи імплементації пристрою може привести до його компрометації.

За досконалістю захисту – дана ознака визначає, наскільки повно даний метод захисту дозволяє нейтралізувати певну атаку. Розрізняють методи з повним захистом (як правило, формально доведеним), що означає неспроможність успішної реалізації атаки навіть при збільшенні обчислювальних потужностей та накопичених статистичних даних криптоаналітика. З іншого боку, якщо збільшення інформаційних ресурсів дозволяє успішно атакувати криптопристрій, то такі методи захисту є частковими, а їх теоретична основа базується на збільшенні обчислювальної (або статистичної) складності атаки, що в багатьох прикладних випадках є достатнім.

За об’єктом системи – дана ознака визначає об’єкт системи захисту, який є ключовим для побудови методу захисту. Наприклад, при використанні методів рандомізації чи маскування можна модифікувати таємний ключ, вхідне повідомлення тощо. Також для захисту від атак апаратних помилок

можуть використовуватися різні схеми виявлення помилок, що використовують інформацію про названі та інші об’єкти системи захисту. Тому можна виділити такі об’єкти системи: ключ, повідомлення, алгоритм, загальносистемні параметри (наприклад, параметри поля, в якому проводять обчислення).

За мірою деталізації. Захист системи можна будувати на різних рівнях її реалізації, починаючи від протоколів та цілої системи і аж до рівня імплементації елементарних операцій. Тому при розробці методу захисту доцільно виявити необхідні та достатні рівні для його імплементації. Розрізняють рівні вузлів, блоків, модулів, операцій, ітерацій, алгоритмів, протоколів та систем.

За типом надлишковості – дана ознака є найцікавішою і визначає, який механізм боротьби з атакою покладено в основу захисту. Очевидно, що набути нових ознак (стійкість до певних атак) система може лише за рахунок зміни властивостей інших ознак (продуктивність, використана площа кристалу тощо). Можна виділити такі типи надлишковості: архітектурна, часова, алгоритмічна та інформаційна.

Архітектурна надлишковість передбачає використання спеціальних компонентів для реалізації захисту, таких, як реконфігуративні систолічні архітектури, схеми контролю, асинхронна логіка, мажоритарні пристрої, генератори шумів, спеціальні давачі, вбудовані джерела живлення, лічильники кількості операцій та резервування [63].

Часова надлишковість передбачає використання додаткових або повторних обчислень для боротьби з атаками і, як правило, приводить до зниження продуктивності роботи пристроїв.

Алгоритмічна надлишковість передбачає модифікацію традиційного алгоритму для боротьби з певним видом атак. Як правило, імплементація такої модифікації приводить до зменшення продуктивності роботи пристрою або ж до додаткових апаратних затрат.

Інформаційна надлишковість передбачає використання додаткових

інформаційних бітів в представленні даних, які дозволяють проводити виявлення наявності, а інколи й виправлення помилок [64]. Ці методи захисту базуються на традиційних методах антизбійного кодування, а саме: перевірка на парність, аутентифікація ключів за хеш-функцією та спеціальне кодування.

Таким чином, перелічені в даному підрозділі методи застосовуються до сучасних криптосистем, які базуються на асиметричній криптографії [78-83]. Асиметричні криптоалгоритми використовують два ключі, один з яких є таємним, що забезпечує високу стійкість системи передачі даних в цілому. Проте ці методи здійснюють протидію, в основному, активним атакам на реалізацію і вимагають великих продуктивних та обчислювальних затрат системи. Тому необхідним є розробка методу захисту від найнебезпечнішої на даний час пасивної атаки – часового аналізу, який враховує поточний стан системи. Зловмисник, здійснюючи атаку на асиметричні криптосистеми, аналізує в основному модулярне експоненціювання, що містить таємний ключ. Вибір оптимального методу піднесення до степеня за модулем забезпечує найкращий захист від розкриття ключа шифрування.

1.3 Методи модулярного експоненціювання, які застосовуються для захисту інформації в комп’ютерних системах

Під час розробки стійких комп’ютерних систем захисту інформації необхідно забезпечити заборону функціонування системи в обхід підсистем захисту та розмежування доступу. Високим рівнем захисту інформації володіють криптосистеми на основі еліптичних кривих, проте на практиці вони широко не використовуються через складність практичної реалізації [40].

Система асиметричної криптографії дозволяє реалізувати строгу

аутентифікацію сторін, накладання та перевірку електронного цифрового підпису (ЕЦП), а також видачу та перевірку сертифікатів відкритих ключів [54].

Політикою безпеки системи має бути обумовлено, що уповноважений орган повинен видавати сертифікат відкритого ключа лише за умови, що ключ надано організацією або особою, яка буде цей ключ використовувати (або уповноваженою особою). Для цього мають бути розроблені певні організаційні вимоги.

В сучасній криптосистемі, як правило, використовуються стандартні алгоритми RSA (назва системи утворена з перших літер імен її винахідників – R. Rivest, A. Shamir, L.Adleman) з довжиною ключа 1024 біт [8, 83].

Запропонована у 1977 році система RSA є чи не найпопулярнішою системою захисту інформації з відкритим ключем.

Ключі в схемі RSA генеруються наступним чином [39, 53, 54]: знаходяться два великі прості числа p і q, для їх добутку $N = p \cdot q$ використовуються значення функції Ейлера:

$$\phi(N) = (p-1)(q-1). \qquad (1.1)$$

Вибирається випадкове число e, що не перевищує $\phi(N)$ і взаємно просте з ним. Обчислюється обернений до e елемент за модулем $\phi(N)$. Таким чином, відкритим ключем буде (N, e), а таємним – (N, d). Зрозуміло, що вибір між d і e в якості таємного ключа досить умовний, тому вважається, що випадковим з певними характеристиками обирається таємний ключ – число d, а відкритий ключ обчислюється. Параметри p і q використовуються лише для обчислення оберненого елемента в $Z^*_{\phi(N)}$ і після генерації ключа знищуються.

Однією з важливих задач при генерації пари ключів є генерація великих простих чисел.

Багато криптосистем з відкритим ключем використовують функцію дискретного піднесення до степеня [40, 53, 84]

$$f(n) = x^n (\mathrm{mod}\, m), \tag{1.2}$$

де n – ціле число $(1 \le n \le m-1)$,

m – велике число,

x – ціле число $(1 \le x \le m)$.

Оскільки для забезпечення стійкості двоключових систем необхідно використовувати досить великі значення x та p, то виникла потреба у використанні спеціальних методів для спрощення і прискорення процесу обчислення цієї функції. На даний час найвживанішими є бінарний, β-арний методи, метод ковзаючого вікна, а також методи з фіксованим показником, з фіксованою основою та з використанням особливостей модулів [53].

Бінарний метод використовує двійкове (бінарне) зображення числа $n = (n_{k-1} \ldots n_0)_2$. Цей метод виконується у двох напрямах (додаток А). При зчитуванні "зліва направо" x^n записується як [55]:

$$x^n = x^{(n_{k-1} \ldots n_0)_2} = \left(\ldots \left(\left(x^{n_{k-1}} \right)^2 x^{n_{k-2}} \right)^2 \ldots \right) x^{n_1} \Bigg)^2 x^{n_0}. \tag{1.3}$$

У бінарному методі на основі зчитування "справа наліво" використовується запис [55]:

$$x^n = x^{(n_{k-1} \ldots n_0)_2} = \left(x^{2^0} \right)^{n_0} \left(x^{2^1} \right)^{n_1} \ldots \left(x^{2^{k-1}} \right)^{n_{k-1}} = \prod_{\{i | n_i = 1\}} x^{2^i}. \tag{1.4}$$

Ці алгоритми потребують $\lceil \log n \rceil$ піднесень до квадрата та $H(n)$ (вага Хемінга, яка дорівнює кількості одиниць в двійковому зображенні числа n) і,

отже, $2\lceil \log n \rceil$ множень у найгіршому випадку та $\frac{3\lceil \log n \rceil}{2}$ множень у середньому [55].

β-арний метод ґрунтується на зображенні показника степеня за основою β, тобто $n = (n_{k-1} \ldots n_0)_\beta$. Цей метод також виконується у двох напрямах (додаток А). При зчитуванні “зліва направо” [55]:

$$x^n = x^{(n_{k-1} \ldots n_0)_\beta} = \left(\ldots \left(\left(x^{n_{k-1}} \right)^\beta x^{n_{k-2}} \right)^\beta \ldots \right) x^{n_1} \Bigg)^\beta x^{n_0} \ . \qquad (1.5)$$

Якщо β є степенем двійки, тобто $\beta = 2^w$ для будь-якого цілого додатного w, то піднесення y^β потребує w піднесень до квадрата. Тоді потрібне лише двійкове зображення числа n, w бітів якого обробляються за одну ітерацію, рухаючись зліва направо. При $w = 1$ отримуємо бінарний метод “зліва направо”.

Для $\beta = 2^w$ потрібно виконати в алгоритмі реалізації даного методу $2^w - 1 + \frac{\lceil \log n \rceil}{w}$ множень та $\frac{\lceil \log n \rceil}{w}$ піднесень до степеня. Отже, кількість множень щонайбільше становить $2^w - 1 + \frac{2}{w}\lceil \log n \rceil$ [55].

При зчитуванні “справа наліво” [55]:

$$x^n = x^{(n_{k-1} \ldots n_0)_\beta} = \left(x^{\beta^0} \right)^{n_0} \left(x^{\beta^1} \right)^{n_1} \ldots \left(x^{\beta^{k-1}} \right)^{n_{k-1}} = \prod_{w=1}^{\beta-1} \left(\prod_{\{i | n_i = w\}} x^\beta \right)^w \ . \qquad (1.6)$$

Для обчислення цього добутку необхідно виконати $2\beta - 2$ множень. Тому в даному алгоритмі “справа наліво” в загальному випадку при $\beta = 2^w$

виконується $2\beta - 2 + \frac{2}{w}\lceil \log n \rceil$ піднесень до степеня.

Вираз

$$y = \prod_{w=1}^{\beta-1} y_w^w \bmod m = y_{\beta-1}\left(y_{\beta-1} \cdot y_{\beta-2}\right)\ldots\left(y_{\beta-1} \cdot y_{\beta-2} \cdot \ldots \cdot y_1\right) \qquad (1.7)$$

у алгоритмі даного методу (див. додаток А) реалізується наступним чином:

Input: $\beta, y_1, y_2, \ldots, y_{\beta-1}, m$;

Output: $y = \prod_{w=1}^{\beta-1} y_w^w \bmod m$;

begin

$y = 1$;

$z = 1$;

for $w = \beta - 1$ downto 1 do

begin

$z = z \cdot y_w \bmod m$;

$y = y \cdot z \bmod m$;

end;

end.

Метод ковзаючого вікна ґрунтується на довільному розбитті на блоки (вікна) бінарного зображення показника степеня, тобто $n = [w_{i-1}, \ldots, w_0]_2$. У даному методі вікна не повинні мати однаковий розмір.

У [55] розглянуто два типи вікон: нульові вікна, які утворюються лише бітом 0, та непарні вікна довжиною щонайбільше *w*, які починаються та закінчуються бітом 1.

При зчитуванні “зліва направо” бінарного зображення числа *n* [55]

$$x^n = \left(\left(\ldots \left(\left(x^{(w_{i-1})_2} \right)^{2^{|w_{i-2}|}} \cdot x^{(w_{i-2})_2} \right)^{2^{|w_{i-3}|}} \ldots \right)^{2^{|w_1|}} \cdot x^{(w_1)_2} \right)^{2^{|w_0|}} \cdot x^{(w_0)_2}. \quad (1.8)$$

У алгоритмі реалізації методу ковзаючого вікна “зліва направо” (додаток А) виконується $2^w - 1 + |w_i|$ множень, де $|w_i|$ – довжина непарного w_i вікна, та $\lceil log\, n \rceil$ піднесень до квадрату.

При зчитуванні “справа наліво” [55]

$$x^n = \prod_{i=0}^{l-1} x^{(w_i)_2 \cdot 2^{l_i}} = \prod_{w \in \{1,3,\ldots,2^w-1\}} \left(\prod_{\{i | (w_i)_2 = w\}} x^{2^{l_i}} \right)^w, \quad (1.9)$$

де $l_i = \sum_{j=0}^{i-1} |w_j|$, для будь-якого $1 \le i \le l-1$, $l_0 = 0$.

У загальному випадку в алгоритмі “справа наліво” необхідно виконати $2^w - 2 + |w_i|$ множень ($|w_i|$ – довжина непарного w_i вікна) та $2^{w-1} - 1 + \lceil \log n \rceil$ піднесень до квадрату.

Вираз

$$\begin{aligned} &\textstyle\prod_{\omega \in \{1,3,\ldots,2^w-1\}} y_\omega^\omega \bmod m = \\ &= \left(y_{2^w-1}\right)^2 \cdot \left(y_{2^w-1} \cdot y_{2^w-3}\right)^2 \ldots \left(y_{2^w-1} \cdots y_3\right)^2 \cdot \left(y_{2^w-1} \cdots y_1\right)^2 \end{aligned} \quad (1.10)$$

у алгоритмі реалізації даного методу модулярного експоненціювання (див. додаток А) здійснюється наступним чином [55]:

Input: $w \ge 1$, y_1, y_3, …, y_{2^w-1}, m;

Output: $y = \prod_{\omega \in \{1,3,\ldots,2^w-1\}} y_\omega^\omega \bmod m$;

Begin

for $\omega = 2^w - 1$ downto 3 step 2 do

begin

$y_{\omega-2} = y_{\omega-2} \cdot y_{\omega} \, mod \, m$;

$y_1 = y_1 \cdot (y_{\omega})^2 \, mod \, m$;

end;

$y = y_1$;

end.

Аналіз операцій, які виконуються під час реалізації наведених вище алгоритмів модулярного екпоненціювання, дозволяє дослідити основні характеристики асиметричних криптосистем в цілому. Варто зазначити, що час виконання найпоширеніших алгоритмів піднесення до степеня за модулем залежить в основному від довжини ключа шифрування.

Стійкість алгоритму захисту інформації RSA забезпечується складністю задачі факторизації, тобто розкладу складного числа на прості множники. Проте, ця проблема для ключа довжиною до 1024 біт розв'язується за допомогою методу решета в полі чисел спеціального виду. Тому необхідно забезпечити додатковий захист криптосистем типу RSA.

На даний час відомо три основні підходи до здійснення криптоаналізу асиметричних криптосистем типу RSA [53, 78]:

1) простий перебір, який полягає у перевірці всіх можливих ключів. Захистом від цього методу служить рекомендована довжина ключа від 1024 біт;

2) математичний аналіз, який здійснює розв'язок задачі факторизації (розкладу числа на прості множники). Стійкість системи RSA до даного типу криптоаналізу забезпечується довжиною ключа від 1024 до 4096 біт;

3) метод аналізу часових затрат, який лежить в основі часової атаки. Атаки такого типу небезпечні з двох причин: вони ведуться з будь-якого комп'ютера мережі і передбачають лише аналіз шифрованого повідомлення.

Крім того, довжина ключа не впливає на успішність проведення атаки так відчутно, як у двох попередніх типах атак.

Лабораторія RSA Data Security пропонує наступні заходи підвищення стійкості до такого типу атак [11]:

1) забезпечення постійного часу виконання всіх піднесень до степеня, проте в такому випадку знижується продуктивність системи захисту;

2) внесення в алгоритм додаткових затримок, але при цьому, якщо затримок додати замало, то зловмисник зможе за допомогою додаткових вимірювань все-таки здійснити криптоаналіз;

3) маскування, тобто множення шифрованого тексту на випадкове число до здійснення піднесення до степеня. Такий метод протидії часовій атаці знижує продуктивність системи захисту інформації на 2-10 %.

Отже, є потреба у розробці нового підходу захисту асиметричних криптосистем від аналізу часової реалізації без втрат продуктивності.

Таким чином, з аналізу асиметричних криптоалгоритмів, проведеного в даному підрозділі, випливає, що їх стійкість та швидкодія залежить, в основному, від реалізації операції модулярного експоненціювання. Тому виникає необхідність розробки методів та засобів оптимального вибору методу піднесення до степеня за модулем при розподілі доступу клієнта до інформаційних ресурсів комп’ютерної системи.

1.4 Шляхи вдосконалення розподілу доступу в комп’ютерних системах

Згідно ДСТУ 3396.0-96, заходи захисту інформації повинні бути відповідними загрозам, розроблятися з урахуванням можливої шкоди від їх реалізації та вартості захисних заходів та обмежень, що вносяться ними, і забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення

загроз [82].

Останні дослідження [40, 50, 51] показали, що сучасні атаки на реалізацію, особливо пасивна атака часового аналізу, є найнебезпечнішим типом незаконних дій зловмисника. Тому сучасні комп'ютерні системи захисту повинні забезпечувати високу стійкість саме до часового аналізу, не поступаючись продуктивністю та затратами пам'яті.

Як зазначалося вище, основною операцією, яка впливає на стійкість та продуктивність асиметричної криптосистеми, є модулярне експоненціювання. Вибір методу піднесення до степеня за модулем, який є стійким до часового аналізу і забезпечує високу продуктивність системи є першочерговою задачею. У [51] зазначено, що застосування алгоритму Монтгомері при піднесенні до степеня за модулем підвищує стійкість системи до часового аналізу. Проте, враховуючи принцип Кочера [39], згідно якого зловмисник знає все про алгоритм шифрування, окрім ключа, а також сам процес здійснення часового аналізу, що не вимагає розв'язання задачі факторизації, здійснення модулярного експоненціювання варто проводити за допомогою індивідуального для кожного клієнта методу.

В загальному схема вибору методу модулярного експоненціювання зображена на рисунку 1.3. В даному випадку в якості критеріїв вибору виступають основні параметри комп'ютерної системи захисту інформації, а підсистемою вибору є система обробки нечіткої інформації. Виходом такої системи є один з методів модулярного експоненціювання, відповідний

вхідним критеріям вибору і застосовуючи який комп'ютерна система забезпечить свою оптимальну роботу.

Рисунок 1.3 - Загальна схема оптимального вибору методу

модулярного експоненціювання для розподілу доступу клієнтів комп’ютерної системи

Так як при розподілі доступу клієнтів необхідно врахувати поточні параметри системи, такі як продуктивність [85], допустимі затрати пам’яті та необхідний рівень стійкості до часового аналізу, а також нечіткі відомості про клієнтів, то для вирішення цієї задачі варто застосувати апарат нечіткої логіки [86-98].

Математична теорія нечітких множин (fuzzy sets) і нечітка логіка (fuzzy logic) є узагальненнями класичної теорії множин і класичної формальної логіки. Дані поняття були вперше запропоновані американським ученим Лотфі Заде (Lotfi Zadeh) у 1965 р. [87]. Основною причиною появи цієї теорії стала наявність нечітких і наближених міркувань при описі людиною процесів, систем, об’єктів.

Основними перевагами нечітких систем у порівнянні з іншими є [87, 88]:

– можливість оперувати вхідними даними, заданими нечітко, наприклад, значеннями, що невпинно змінюються в часі (динамічні задачі);

– можливість нечіткої формалізації критеріїв оцінки і порівняння;

– можливість проведення якісних оцінок як вхідних даних, так і виведених результатів, оскільки система оперує не тільки власне значеннями даних, а й їх ступенем вірогідності та її розподілом;

– можливість проведення швидкого моделювання складних динамічних систем та їх порівняльний аналіз із заданим ступенем точності.

Перевагу нечіткої системи над класичними підходами можна проілюструвати на прикладі порівняння класичного ПІ та нечіткого регулятора, поданих в [90]. На рисунку 1.4 зображено перехідні процеси нечіткої і типової системи автоматизованого регулювання, що демонструє переваги нечіткого контролера, який має чіткий затухаючий вигляд.

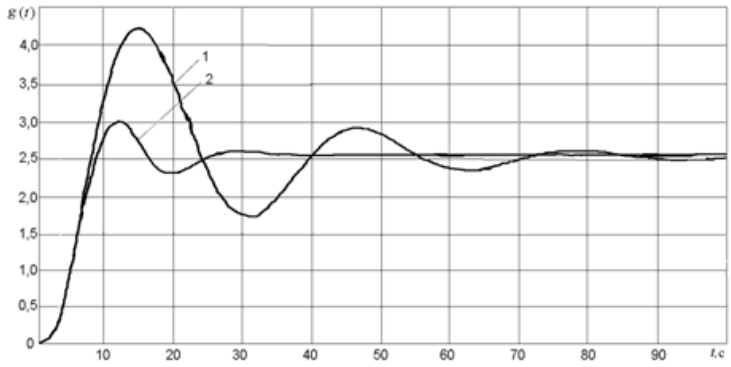


Рисунок 1.4 - Перехідні процеси нечіткої та класичної автоматизованої системи регулювання: 1 – ПІ-регулятор, 2 – нечіткий регулятор

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [87, 97]. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій [99]:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій належності $MF_i(x)$ для лівих частин кожного *i*-го правила (передумов);

2) нечіткий висновок. Спочатку визначаються мінімальний рівень "відсічення" для лівої частини кожного з правил $A_i = \min(MF_i(x))$, а потім знаходяться "усічені" функції належності висновку $B_i = \min(A_i, B_i)$;

3) композиція або об’єднання отриманих "усічених" функцій, для чого використовується максимальна композиція нечітких множин $MF(y) = \max(B_i(y))$;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод. Геометричний зміст такого значення – центр ваги для кривої функції належності отриманого виходу.

Застосування апарату нечіткої логіки при створенні апаратно-програмного засобу для здійснення розподілу доступу в комп’ютерній системі шляхом вибору оптимального методу модулярного експоненціювання для кожного окремого клієнта та врахування поточних параметрів самої КС дозволить забезпечити стійкість криптосистеми до

часового аналізу в режимі реального часу.

Для вирішення цього завдання необхідно:

1) дослідити основні параметри методів модулярного експоненціювання, що найчастіше застосовуються в сучасних системах захисту інформації та визначити стійкість кожного з них до часового аналізу;

2) розробити метод обробки нечіткої інформації під час розподілу доступу в комп’ютерних системах, застосовуючи досліджені параметри методів піднесення до степеня за модулем;

3) розробити структуру засобу реалізації розробленого методу та дослідити його основні характеристики.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. Проаналізовано особливості розподілу доступу до інформації в комп’ютерній системі, а також можливі атаки, що можуть реалізовуватись через комп’ютерну мережу зловмисником.

2. На основі огляду відомих сучасних атак на реалізацію встановлено, що найнебезпечнішою атакою на комп’ютерну систему захисту інформації є пасивна часова атака, оскільки її неможливо помітити в мережі і, відповідно, вчасно застосувати методи протидії. Обґрунтовано, що вибір оптимального методу піднесення до степеня за модулем може забезпечити найкращий захист від розкриття ключа шифрування при здійсненні часового аналізу.

3. Аналіз асиметричних криптоалгоритмів показав, що їх стійкість та швидкодія залежать, в основному, від реалізації операції модулярного експоненціювання, тому виникає необхідність розробки методів та засобів оптимального вибору методу піднесення до степеня за модулем при розподілі доступу клієнта до інформаційних ресурсів комп’ютерної системи.

4. Визначено, що засіб розподілу доступу найкраще побудувати за допомогою методів нечіткої логіки, які дозволять реконфігурувати комп’ютерну систему в реальному часі, та здійснено постановку задачі дослідження.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ОСНОВНИХ ПАРАМЕТРІВ МЕТОДІВ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ

2.1 Оцінка часу виконання та затрат пам’яті

Існують різні параметри аналізу роботи комп’ютерної системи в цілому, але основним критерієм оцінки її підсистеми захисту інформації є стійкість до атак. Для забезпечення безвідмовної та результативної роботи цієї підсистеми, яка працює за криптоалгоритмом RSA, необхідно дослідити основні параметри алгоритмів виконання модулярного експоненціювання.

Традиційно прийнято оцінювати ступінь складності алгоритму за обсягом використовуваних ним основних ресурсів комп’ютера: процесорного часу та оперативної пам’яті. У зв’язку з цим розглядаються такі поняття, як часова складність та об’ємна складність алгоритму [100, 101].

Об’ємна складність алгоритму – це об’єм пам’яті, який займає процесор під час виконання цього алгоритму. Цей параметр є дуже важливим, оскільки він впливає на продуктивність комп’ютерної системи в цілому.

Параметр часова складність є особливо важливим для задач, що передбачають інтерактивний режим роботи програми, або для задач управління в режимі реального часу.

На виконання кожного з описаних у п. 1.3 алгоритмів необхідно затратити певний час. Виконання однієї операції залежить від швидкодії процесора, тому можна вважати, що в загальному кожен окремий крок алгоритму виконується за деякий час. Основні операції алгоритмів модулярного експоненціювання та затрати часу на виконання кожної з них можна подати у вигляді таблиці 2.1 [102, 103]:

Таблиця 2.1 - Час виконання основних операцій алгоритмів модулярного експоненціювання

Операція	Зміст операції	Час виконання операції, в тактах
$a = b$	Просте присвоєння	c
$z = x \bmod m$	Присвоєння за модулем	b
$\text{FIND}(\max\{n_i \ldots n_j\} \mid i - j + 1 \le w, n_j = 1)$	Знаходження найдовшої послідовності бітів, такої, що $i - j + 1 \le w$ та $n_j = 1$	q
$n = (n_{k-1} \ldots n_0)_2$	Зображення числа у двійковій системі числення	t
$y = x \cdot x \bmod m$	Піднесення до квадрату за модулем	r
$z = x \cdot y \bmod m$	Множення за модулем	s
$z = y^{\beta} \bmod m$	Піднесення до степеня за модулем	d

Аналізуючи швидкодію сучасних процесорів, в загальному, можна прийняти, що співвідношення між значеннями затрат часу на виконання основних операцій алгоритмів модулярного експоненціювання, які представлені в таблиці 2.1, є таким [104-108]:

$$c \le b \le q \le t \le r \le s \le d . \qquad (2.1)$$

Виходячи з таблиці 2.1, можна побудувати математичну модель обчислення часу, затраченого на виконання кожного з алгоритмів реалізації методів модулярного експоненціювання, описаних у п.1.3. При цьому,

оскільки змінна n опрацьовується у бінарному вигляді, то через $\lceil \log n \rceil$ представляється довжина цієї бінарної послідовності.

На виконання бінарного методу затрачається час [102]:

– при зчитуванні “зліва направо”:

$$T1(n) = t + c + \sum_{i=k-1}^{0} r_i + \sum_{i=k-1|n_i=1}^{0} s_i = t + c + \lceil \log n \rceil \cdot r + H(n) \cdot s, \qquad (2.2)$$

– при зчитуванні “справа наліво”:

$$T2(n) = t + c + b + \sum_{i=0|n_i=1}^{k-1} s_i + \sum_{i=0}^{k-1} r_i = t + c + b + H(n) \cdot s + \lceil \log n \rceil \cdot r. \qquad (2.3)$$

Через $H(n)$ позначено вагу Хемінга, тобто кількість одиниць у бінарному представленні n.

На виконання β-арного методу затрачається час [102]:

– при зчитуванні “зліва направо”:

$$\begin{aligned} T3(n,w) &= t + c + \sum_{i=1}^{\beta-1} s_i + c + \sum_{i=k-1}^{0} (d_i + s_i) = \\ &= t + 2c + \left(\frac{\lceil \log n \rceil}{w} + 2^w - 1 \right) \cdot s + \frac{\lceil \log n \rceil}{w} \cdot d \end{aligned} \qquad (2.4)$$

– при зчитуванні “справа наліво”:

$$\begin{aligned} T4(n,w) &= t + b + \sum_{w=1}^{\beta-1} c_w + \sum_{0}^{k-1} \left(d_{\{i|n_i=0\}} + s_{\{i|n_i=1\}} + d_{\{i|n_i=1\}} \right) + 2c + \sum_{w=\beta-1}^{1} 2s_w = \\ &= t + \left(2^w + 1\right)c + b + \frac{\lceil \log n \rceil}{w} \cdot d + \left(\frac{\lceil \log n \rceil}{w} - W_0(n) + 2^{w+1} - 2 \right) \cdot s \end{aligned} \qquad ,(2.5)$$

де $W_0(n)$ – кількість нульових бітів у зображенні числа n за основою β, w – показник степеня двійки в $\beta = 2^w$.

Очевидно, що в бінарному зображенні числа n є $\lceil \log n \rceil - H(n)$ нульових бітів. Для переведення числа в β-арну систему числення бінарне зображення n розбивають на вікна довжиною w. Звідси випливає, що верхня оцінка $W_0(n)$ [109-111]:

$$W_0{}^{\max}(n) = \left\lfloor \frac{\lceil \log n \rceil - H(n)}{w} \right\rfloor. \tag{2.6}$$

З іншого боку, нижня оцінка легко може бути визначена як

$$W_0{}^{\min}(n) = \left\lfloor \frac{(\lceil \log n \rceil - H(n)) \cdot w}{(w-1) \cdot \lceil \log n \rceil} \right\rfloor. \tag{2.7}$$

На виконання методу ковзаючого вікна затрачається час [102]:

– при зчитуванні “зліва направо”:

$$\begin{aligned} T5(n,|w_i|) &= b + s + \sum_{j=1}^{2^{|w_i|}-1} s_j + t + 2c + \\ &\quad + \sum_{i=0}^{k-1} \left((r+c)_{\{i|n_i=0\}} + (q+s+c+r)_{\{i|n_i=1\}} \right) = \\ &= b + s + \left(2^{|w_i|} - 1\right)s + t + 2c + \\ &\quad + (k - H(n))(r+c) + p(q+s+c) + r(|w_o| + \ldots + |w_i|) = \\ &= t + b + 2c + kr + 2^{|w_i|}s + p(q+s+c) + (k - H(n))c = \\ &= t + b + (2 + p + \lceil \log n \rceil - H(n))c + \lceil \log n \rceil r + \left(2^{|w_i|} + p\right)s + pq \end{aligned} \tag{2.8}$$

– при зчитуванні “справа наліво”:

$$
\begin{aligned}
T6(n,|w_i|) &= t+b+\sum_{\{j=1,3,\ldots,2^{|w_i|}-1\}} c_j + c + \\
&\quad + \sum_{i=k-1}^{0} \left((r+c)_{\{i|n_i=0\}} + (q+s+c+d)_{\{i|n_i=1\}} \right) + \\
&\quad + \sum_{\{v=2^{|w_i|}-1,\ldots,5,3\}} (2s_v) + c = \\
&= t+b+\left(2^{2|w_i|-2}+1\right)c + (k-H(n))(r+c) + \\
&\quad + p(q+s+c+d) + 2^{2|w_i|-1}s + c = \\
&= t+b+\left(2^{2|w_i|-2}+2+\lceil \log n \rceil - H(n) + p\right)c + \\
&\quad + (\lceil \log n \rceil - H(n))r + \left(2^{2|w_i|-1}+p\right)s + pq + pd
\end{aligned}, \quad (2.9)
$$

де p – кількість вікон,

$(|w_0|+\ldots+|w_i|)$ – сума всіх непарних вікон (рівна вазі Хемінга, оскільки ці вікна складаються лише з одиничних бітів).

Очевидно, що $p_{\max} = \left\lceil \frac{\log n}{2} \right\rceil$, а $p_{\min} = \left\lceil \frac{H(n)}{|w_i|} \right\rceil$. Тому в загальному для дослідження часу виконання цього алгоритму можна розглядати середнє значення [111]

$$
p = \frac{\left\lceil \frac{H(n)}{|w_i|} \right\rceil + \left\lceil \frac{\log n}{2} \right\rceil}{2}. \quad (2.10)
$$

Очевидно, що для підвищення продуктивності асиметричних криптосистем виникає необхідність визначення найпродуктивнішого з усіх відомих алгоритмів модулярного експоненціювання, які в них використовуються.

Шлях розв’язання цієї задачі розглянемо на прикладі описаних вище бінарного, β-арного методів та методу ковзаючого вікна.

Як зазначалося у п.1.3, загальний час виконання алгоритму бінарного

методу залежить лише від довжини двійкового зображення числа n. Час виконання алгоритму β-арного методу залежить не тільки від довжини бінарного зображення числа n, а й від значення β (тобто від числа w). Час, який займає виконання алгоритму методу ковзаючого вікна, залежить від довжини двійкового зображення числа n та ширини непарного вікна $|w_i|$. Враховуючи це, можна дослідити залежність часу виконання алгоритму $T_i(n, w, |w_i|)$ від довжини двійкового зображення числа n [112].

На рисунку 2.1 зображено цю залежність при усереднених значеннях ваги Хемінга ($H(n)$) та кількості нулів у β-арному зображенні числа n ($W_0(n)$), а також при різних значеннях w та ширини непарного вікна [113]. У подальших дослідженнях приймаються значення $c=1$, $b=1.5$, $q=1.6$, $t=1.6$, $r=15$, $s=16$, $d=19$, що відповідають кількості тактів, які затрачає процесор Intel 80386 на виконання відповідних до таблиці 2.1 операцій [108].

У даному випадку на рисунку 2.1 через $T1(n)$ та $T2(n)$ позначено час виконання бінарного методу «зліва направо» та «справа наліво», відповідно, а $T3(n,2)$ і $T3(n,4)$ - час виконання алгоритму β-арного методу модулярного експоненціювання «зліва направо» при $w=2$ та $w=4$, відповідно. $T4(n,2)$ і $T4(n,4)$ - це час виконання алгоритму β-арного методу модулярного експоненціювання «справа наліво» при $w=2$ та $w=4$, відповідно. $T5(n,3)$ і $T6(n,3)$ - час виконання методу ковзаючого вікна «зліва направо» та «справа наліво» при довжині вікна $|w_i|=3$.

Аналіз рисунку 2.1 показує, що час виконання алгоритмів модулярного експоненціювання має лінійний характер. Крім того, найпродуктивнішими є алгоритми β-арного методу “зліва направо” та “справа наліво”, а найбільше часу займає виконання алгоритму бінарного методу.

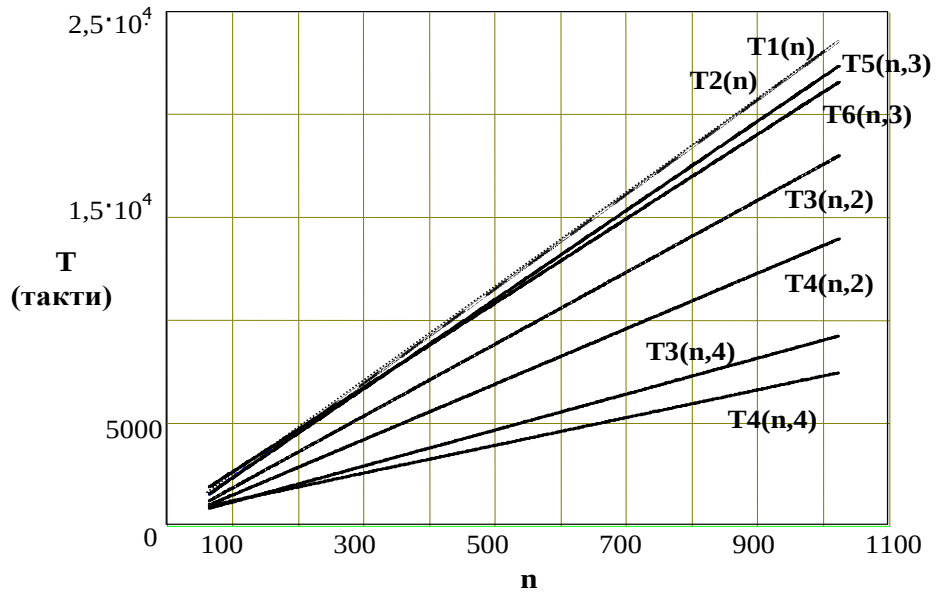


Рисунок 2.1 - Оцінка часових характеристик досліджуваних алгоритмів

На рисунку 2.2 та рисунку 2.3 [113] 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 та 4096 біт) та при усередненому значенні ваги Хемінга.

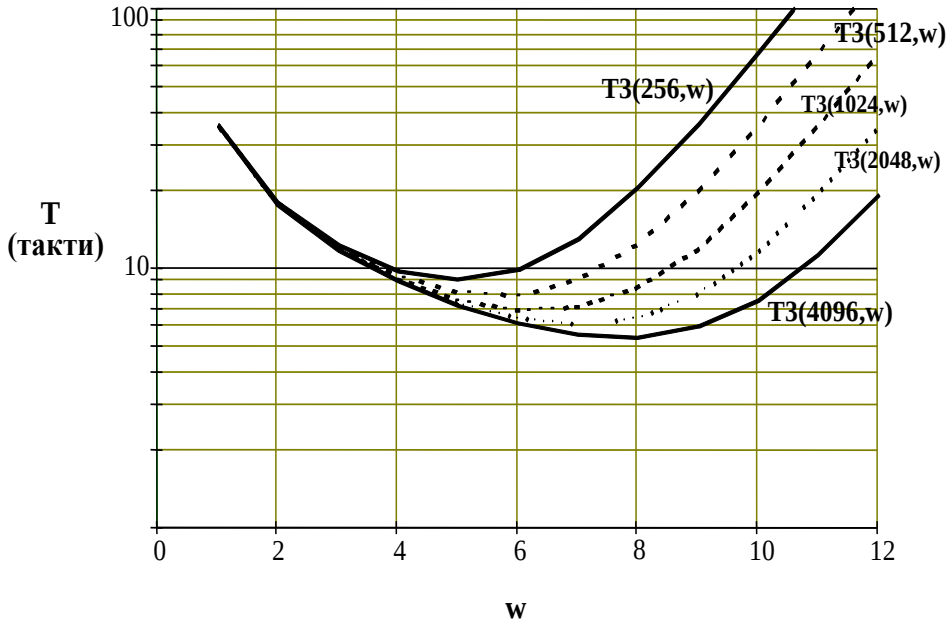


Рисунок 2.2 - Залежність швидкодії алгоритму β-арного методу “зліва направо” від значення степеня основи w

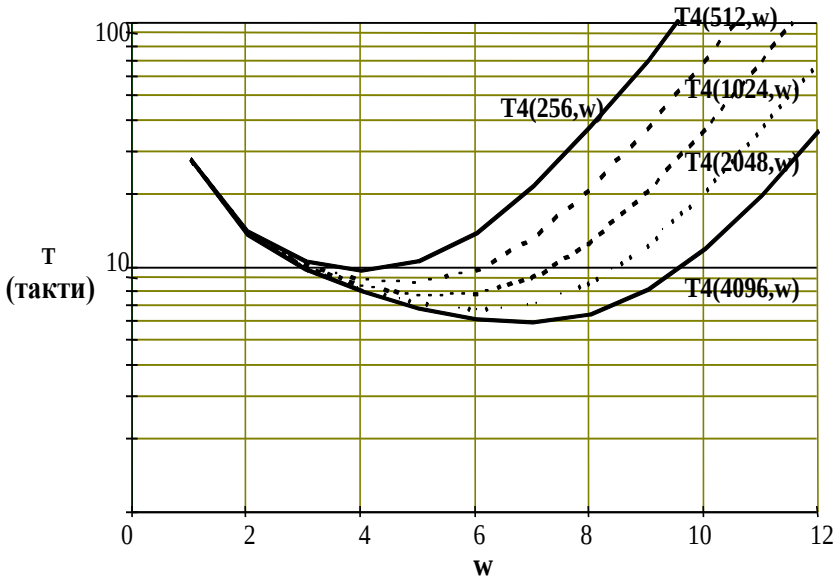


Рисунок 2.3 - Залежність швидкодії алгоритму β-арного методу “справа наліво” від значення степеня основи w

За даними рисунків 2.2 та 2.3 можна визначити оптимальну основу w, при якій здійснюється найменша затримка роботи алгоритму, тобто мінімальні $T3$ та $T4$, відповідно, а отже, забезпечується його максимальна продуктивність при заданих значеннях експоненти n. Для алгоритмів β-арного методу найкращими будуть значення w, подані в таблиці 2.2 [113].

Таблиця 2.2 - Оптимальні значення степеня основи β-арного методу при різній довжині ключа n.

Довжина ключа n	Значення степеня двійки в β-арному представленні, w	
	β-арний метод “зліва направо”	β-арний метод “справа наліво”
4096	8	7
2048	7	6
1024	6	5
512	6	5
256	5	4

Об’ємна складність алгоритму модулярного експоненціювання, тобто затрати пам’яті комп’ютера на його виконання, стає критичною, коли обсяг опрацьовуваних даних виявляється на межі обсягу оперативної пам’яті. В

сучасних комп'ютерних системах гострота цієї проблеми знижується завдяки зростанню обсягу оперативних запам'ятовуючих пристроїв (ОЗП) комп'ютера та ефективного використання багаторівневої системи запам'ятовуючих пристроїв. Програмі, що реалізує алгоритм піднесення до степеня за модулем, виявляється доступною дуже велика, практично необмежена область пам'яті (віртуальна пам'ять), а нестача основної пам'яті призводить лише до деякого уповільнення роботи через обмін даними з диском. Для мінімізації втрати часу при такому обміні використовується кеш-пам'ять та апаратний перегляд команд програми на необхідне число ходів вперед, що дозволяє завчасно переносити з диска в основну пам'ять потрібні значення [101].

Під час виконання розглянутих алгоритмів модулярного експоненціювання в пам'яті комп'ютера використовується, подана в таблиці 2.3, максимальна кількість регістрів.

Таблиця 2.3 - Максимальна кількість комірок пам'яті, зайнятих під час виконання алгоритмів модулярного експоненціювання

Алгоритм модулярного експоненціювання	Кількість комірок пам'яті
Бінарний	2
β-арний	2^w
Ковзаючого вікна	$2^{\lvert w_i \rvert}$

Аналіз таблиці 2.3 показує, що найбільшими є затрати пам'яті у випадку виконання алгоритму ковзаючого вікна, оскільки довжина найбільшого вікна w_i може дорівнювати половині довжини ключа. У випадку застосування алгоритму β-арного методу модулярного експоненціювання затрати пам'яті залежать від обраної системи числення, тобто від значення w.

Проведені дослідження показали, що найвищу швидкодію має

алгоритм β-арного методу модулярного експоненціювання і на його виконання затрачається найменша кількість регістрів пам'яті [102]. Тобто в криптосистемах типу RSA можна рекомендувати використання β-арного методу піднесення до степеня за модулем у випадку необхідності високої продуктивності системи при невеликих затратах пам'яті.

2.2 Вага Хемінга як критерій оцінки чутливості до часової атаки

Оскільки в асиметричних криптосистемах основною операцією, що використовується в процесі шифрування та дешифрування, є модулярне експоненціювання, то використовувана криптосистема, яка базується на такій операції, повинна задовільняти певні умови, зокрема, мати високу швидкодію та захищеність від атак зловмисників. Перша проблема вирішується вибором найоптимальнішого методу піднесення числа до степеня за модулем. Друга проблема набагато серйозніша і вимагає гарантованого забезпечення стійкості цього методу до атак спеціального виду.

Виявлення певної кореляції між кількістю одиничних бітів ключа та часом виконання відповідного алгоритму дозволяє зловмиснику висунути гіпотезу щодо цієї кількості одиничних (нульових) бітів, кількісним еквівалентом якої є вага Хемінга. Тобто, знаючи вагу Хемінга, можна значно швидше та точно визначити таємний ключ криптосистеми RSA.

Тому для дослідження стійкості алгоритмів, описаних у п. 1.3, необхідно встановити залежність часу виконання відповідного алгоритму від ваги Хемінга.

На рисунку 2.4 [112, 113] зображено залежність часу виконання алгоритмів бінарного методу "зліва направо" $T1(n, H(n))$ та "справа наліво" $T2(n, H(n))$, відповідно, від ваги Хемінга при довжині n - $\lceil \log n \rceil = 1024$ біти,

яка задовільняє сучасні вимоги до довжини ключа криптосистеми. Варто зазначити, що зображення залежності $T1(n, H(n))$ та $T2(n, H(n))$ від ваги Хемінга співпадають. Аналіз цього графіка показує, що продуктивність даних алгоритмів суттєво залежить від ваги Хемінга, а також є можливість визначення мінімальної та максимальної швидкодії, математичного сподівання і т.п. Крім того, очевидно, що стійкість цих методів до часового аналізу буде мінімальною, тобто зловмисник, вимірявши час виконання алгоритму, може легко оцінити кількість одиниць у двійковому зображенні числа n, а отже, і визначити таємний ключ шляхом перебору у звуженому ключовому просторі.

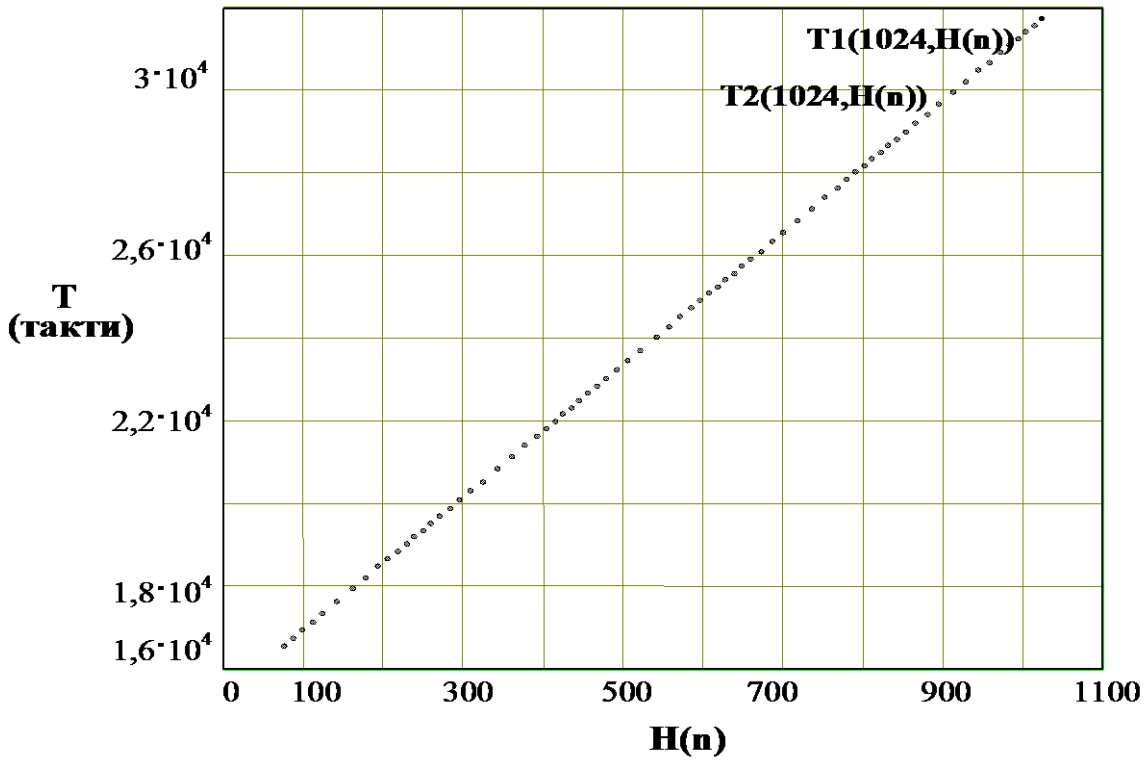


Рисунок 2.4 - Залежність часу виконання алгоритму бінарного методу від ваги Хемінга

Аналіз графіка залежності швидкодії алгоритму β-арного методу "зліва направо" $T3(n, \beta, H(n))$ від ваги Хемінга (рисунок 2.5) [112, 113] показує, що, на відміну від бінарного методу (див. рисунок 2.4), час

виконання цього алгоритму залежить лише від значення β. Тобто цей алгоритм є абсолютно стійкий до часової атаки.

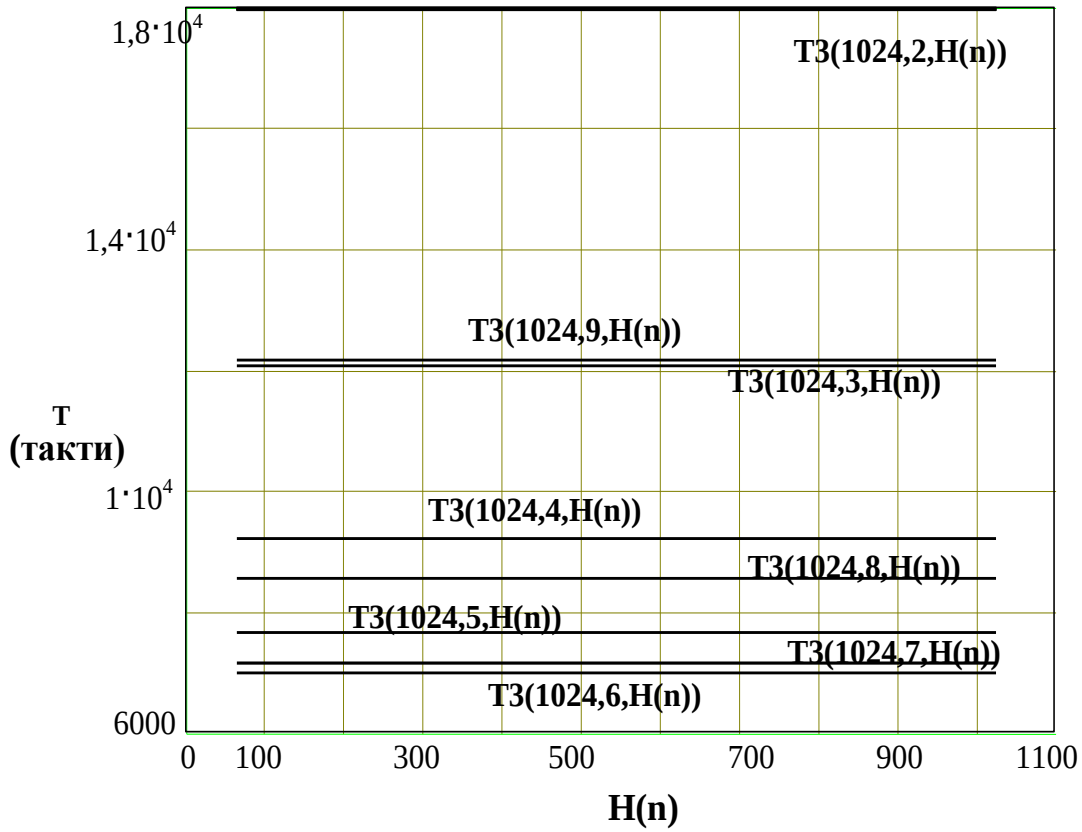


Рисунок 2.5 - Залежність часу виконання алгоритму β-арного методу “зліва направо” від ваги Хемінга

Дослідження залежності часу виконання алгоритму β-арного методу “справа наліво” $T4(n,\beta,H(n))$ від ваги Хемінга (рисунок 2.6) показує [111], що на відміну від попереднього (див. рисунок 2.5), він залежить від кількості одиниць у двійковому зображенні числа n. Тобто при різних значеннях його параметрів отримуються різні характеристики швидкодії та стійкості до часового аналізу. Проте в окремих випадках можна знайти таке значення β, при якому можливе отримання практичної стійкості, близьке до абсолютної, наприклад, при $\beta = 9$.

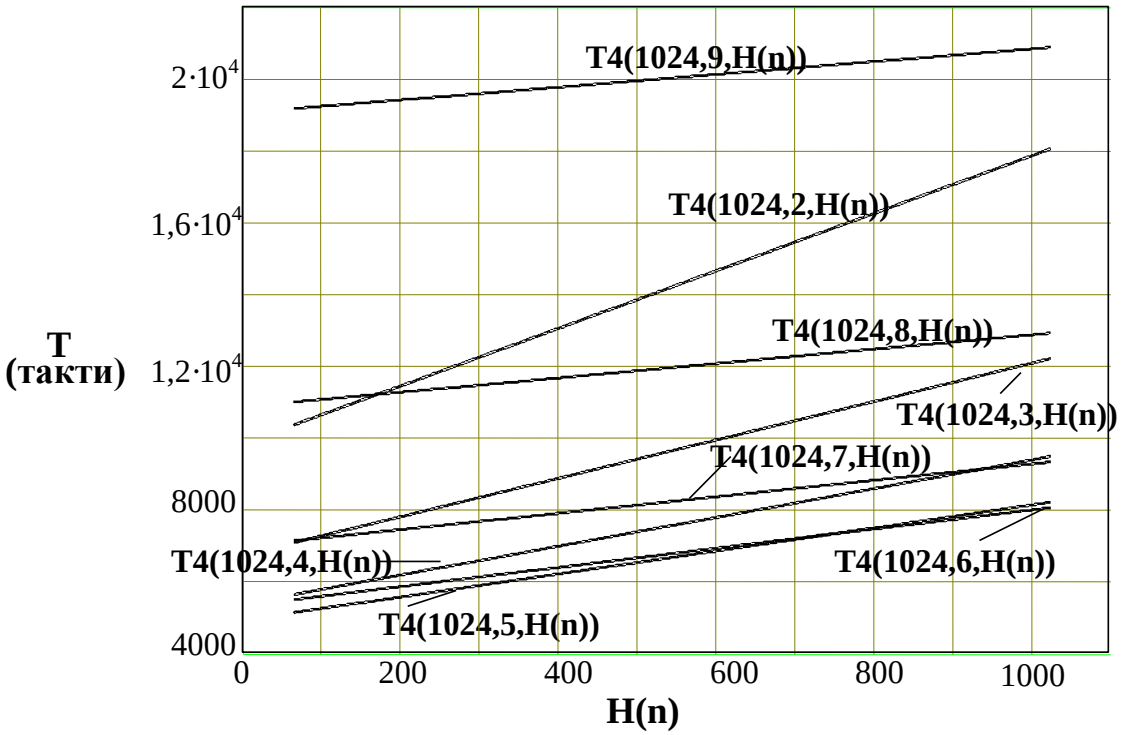


Рисунок 2.6 - Залежність швидкодії алгоритму β-арного методу “справа наліво” від ваги Хемінга

З аналітичного представлення (2.8) та (2.9) випливає, що існує обернена залежність часу виконання алгоритмів методу ковзаючого вікна при зчитуванні “зліва направо” $T5(n,|w_i|,H(n))$ та “справа наліво” $T6(n,|w_i|,H(n))$, відповідно, від ваги Хемінга. Проте, оскільки ця залежність є невеликою, то можна вважати, що для певного класу прикладних задач можна успішно використовувати вказані алгоритми, оскільки їх стійкість до часового аналізу є вищою в порівнянні з іншими методами.

Таким чином, проведені дослідження показали, що β-арний метод модулярного експоненціювання є стійким до пасивних атак, в яких проводиться аналіз ваги Хемінга, зокрема до найнебезпечнішої – атаки часового аналізу.

На рисунках 2.7 та 2.8 зображено залежність часу виконання цих алгоритмів від ваги Хемінга, при $W_0(n)=W_0^{\max}(n)$, що є найсприятливішою умовою для криптоаналізу [113].

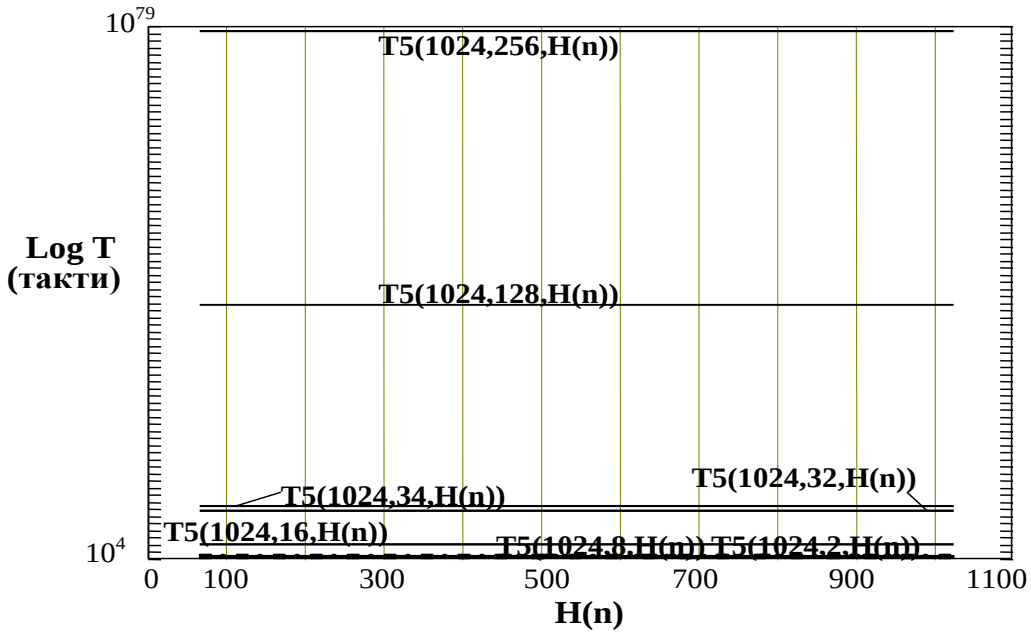


Рисунок 2.7 - Залежність швидкодії алгоритму методу ковзаючого вікна при зчитуванні “зліва направо” від ваги Хемінга

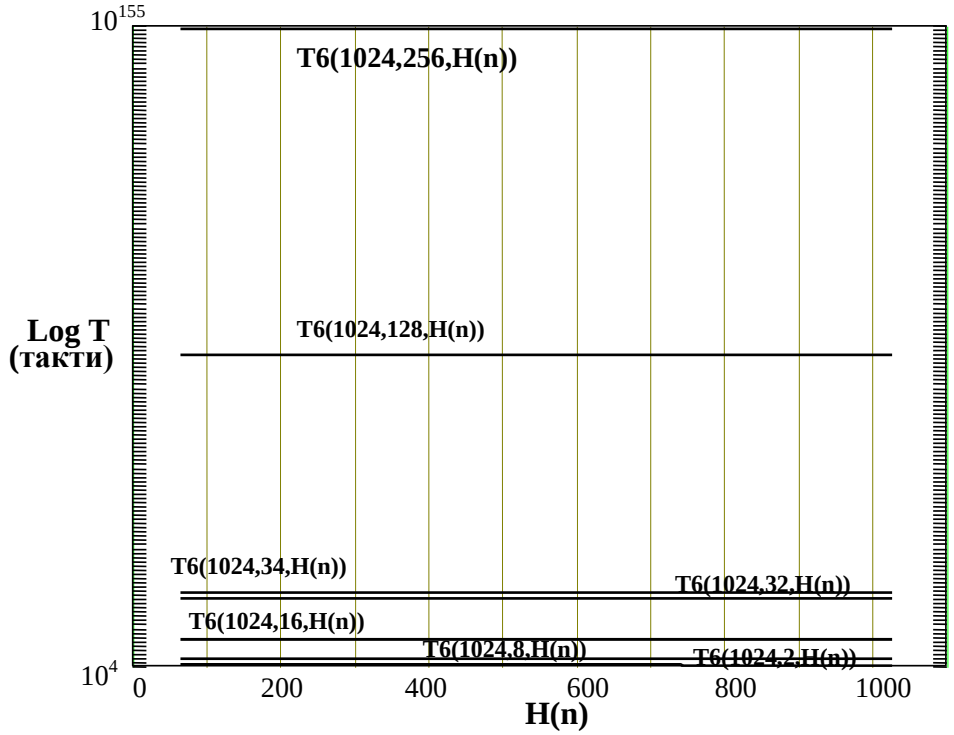


Рисунок 2.8 - Залежність швидкодії алгоритму методу ковзаючого вікна при зчитуванні “справа наліво” від ваги Хемінга

Таким чином, для оцінки стійкості інших методів піднесення до степеня необхідно ввести критерій стійкості до часового аналізу, який

відображає залежність часу виконання відповідних алгоритмів від ваги Хемінга.

2.3 Метод визначення нормованої стійкості до часового аналізу

З аналізу графіків залежності часу виконання алгоритмів модулярного експоненціювання від ваги Хемінга (див. рисунки 2.5 – 2.8) випливає, що, по перше, абсолютно стійким є той алгоритм, час виконання якого є сталим, тобто пряма зображення якого паралельна до осі абсцис, і, по друге, чим більший кут нахилу прямої, тим легше зловмиснику визначити вагу Хемінга за обчисленим 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°.

Як відомо, якщо функція $y = f(x)$ зображена своїм графіком – кривою в декартових координатах, то $f'(x) = tg\alpha$, де α – кут між віссю OX і дотичною до кривої в даній її точці [114].

Звідси випливає, що $\frac{dT_i}{dH(n)} = tg\alpha_i$, де α_i – кут нахилу прямої $T_i(n, w, |w_i|)$ до осі OX.

Як відомо, $\cos 0^\circ = 1$ [114]. Тому нормовану стійкість алгоритму модулярного експоненціювання до часової атаки можна оцінити наступним чином [103, 113]:

$$S = \cos\left(arctg \frac{dT_i}{dH(n)} \right). \qquad (2.11)$$

Продиференціювавши математичні моделі часу виконання кожного алгоритму за основою $H(n)$, отримаємо [103]:

- для бінарного методу модулярного експоненціювання «зліва направо»

$$\frac{dT1}{dH(n)} = \frac{d\left(t + c + \lceil \log n \rceil \cdot r + H(n) \cdot s\right)}{dH(n)} = s, \qquad (2.12)$$

- для бінарного методу модулярного експоненціювання «справа наліво»

$$\frac{dT2}{dH(n)} = \frac{d\left(t + c + b + \lceil \log n \rceil \cdot r + H(n) \cdot s\right)}{dH(n)} = s, \qquad (2.13)$$

- для β-арного методу «зліва направо», час виконання якого не залежить від ваги Хемінга:

$$\frac{dT3}{dH(n)} = \frac{d\left(t + 2c + \frac{\lceil \log n \rceil}{w} \cdot d + \left(2^w - 1 + \frac{\lceil \log n \rceil}{w}\right) \cdot s\right)}{dH(n)} = 0, \qquad (2.14)$$

- для β-арного методу модулярного експоненціювання «справа наліво», враховуючи (2.6)

$$\frac{dT4}{dH(n)} = \frac{d\left(t + \left(2^w + 1\right) \cdot c + b + \frac{\lceil \log n \rceil}{w} \cdot d + \left(2^{w+1} - 2 - W_0(n) + \frac{\lceil \log n \rceil}{w}\right) \cdot s\right)}{dH(n)} = \qquad (2.15)$$

$$= \frac{-d\left(W_0(n) \cdot s\right)}{dH(n)} = \frac{-d\left(\left\lfloor \frac{\lceil \log n \rceil - H(n)}{w} \right\rfloor \cdot s\right)}{dH(n)} = \frac{s}{w}$$

- для методу ковзаючого вікна «зліва направо» та «справа наліво», враховуючи (2.10) та спрощення, подані у додатку Б:

$$\frac{dT5}{dH(n)} = \left(\left|\frac{1}{2w_i}\right| - 1\right)\cdot c + \left|\frac{1}{2w_i}\right|\cdot s + \left|\frac{1}{2w_i}\right|\cdot q = \left|\frac{1}{2w_i}\right|\cdot(c+s+q) - c \qquad (2.16)$$

$$\frac{dT6}{dH(n)} = \left|\frac{1}{2w_i}\right|\cdot(c+s+q+d) - c - r \qquad (2.17)$$

Аналізуючи вирази (2.12) – (2.17), можна зробити висновок, що найвищу стійкість до часового аналізу забезпечує алгоритм β-арного методу "зліва направо", а $\frac{dT5}{dH(n)}$ та $\frac{dT6}{dH(n)}$ залежать лише від довжини вікна $|w_i|$ [103].

У таблиці 2.3 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 [113].

Аналіз таблиці 2.3 показує, що абсолютно стійким до часової атаки (як і випливало з (2.14)) є β-арний метод "зліва направо". Наступним за стійкістю є метод ковзаючого вікна "зліва направо". Найменшу стійкість до часового аналізу має бінарний метод.

При заданих параметрах найшвидшим алгоритмом модулярного експоненціювання є β-арний метод "справа наліво", який виконується за 3956 тактів при $\lceil \log n \rceil = 512$, а при довжині $\lceil \log n \rceil = 4096$ біт – за 28150 тактів.

Отже, для побудови сучасних ефективних систем захисту інформації на основі асиметричних криптоалгоритмів найкраще застосовувати алгоритм β-арного методу "зліва направо" чи "справа наліво".

Таблиця 2.3 - Результати досліджень часу виконання та нормованої стійкості алгоритмів модулярного експоненціювання

Алгоритм	Довжина n, Біт	Час виконання, такти	Нормована стійкість до часового аналізу S
Бінарний метод “зліва направо”	512	11780	0.062
	1024	23550	
	2048	47110	
	4096	94210	
Бінарний метод “справа наліво”	512	11780	0.062
	1024	23560	
	2048	47110	
	4096	94210	
β -арний метод “зліва направо”	512	4724	1
	1024	9204	
	2048	18160	
	4096	36080	
β -арний метод “справа наліво”	512	3956	0.243
	1024	7412	
	2048	14320	
	4096	28150	
Метод ковзаючого вікна “зліва направо ”	512	10970	0.430
	1024	22350	
	2048	44570	
	4096	89020	
Метод ковзаючого вікна “справа наліво”	512	12290	0.114
	1024	21560	
	2048	42590	
	4096	84640	

Таким чином, запропонований в даному підрозділі метод визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу, який базується на залежності часу виконання алгоритму від ваги Хемінга, дозволяє аналітично визначити стійкість будь-якого методу піднесення до степеня за модулем до часового аналізу [115, 116].

2.4 Оцінка стійкості методів модулярного експоненціювання на основі ймовірнісних наближень

Для підтвердження (2.11) необхідно провести імітаційне моделювання здійснення зловмисником часового аналізу.

Відповідно до математичних моделей (2.12) − (2.17), біти експоненти впливають на значення часу t_i (переведення числа n у двійкову, β-арну форму чи представлення у вигляді послідовності нульових та непарних вікон), d_i (час виконання операції $y^{\beta} \bmod m$) та s_i (час виконання операції множення за модулем).

Оскільки прийнято вважати, що зловмисник може виміряти час здійснення шифрування повідомлення, то час виконання алгоритму будь-якого методу модулярного експоненціювання в загальному записується з урахуванням впливу помилки вимірювання часу шифрування та відстані передачі.

Для реалізації часової атаки криптоаналітик на ідентичному комп'ютері проводить аналогічне до реального експоненціювання і обчислює часи $\hat{T}_{i,k-1,0}$ і $\hat{T}_{i,k-1,1}$ (для кожного методу «зліва направо») чи $\hat{T}_{i,0,0}$ та $\hat{T}_{i,0,1}$ (для кожного методу «справа наліво», відповідно) для експонент 0 та 1 (i – номер проведеного обчислення) [33, 34]. Після цього він може побудувати таблицю різниць між реальним та отриманим часами (таблиця 2.4) [117].

Таблиця 2.4 - Різниці реального та отриманого часів під час здійснення часового аналізу.

Значення поточного біта рівне 0	Значення поточного біта рівне 1
$T_1 - \hat{T}_{1,k-1,0}$	$T_1 - \hat{T}_{1,k-1,1}$
$T_2 - \hat{T}_{2,k-1,0}$	$T_2 - \hat{T}_{2,k-1,1}$
$T_3 - \hat{T}_{3,k-1,0}$	$T_3 - \hat{T}_{3,k-1,1}$
...	...

В даній таблиці стовпчик, де є найменша різниця часів ΔT, відповідає значенню біта експоненти, що аналізується. Тобто криптоаналітик може знайти значення n_{k-2} для кожного методу «зліва направо» чи n_1 при зчитуванні бітів «справа наліво».

Отримуючи аналогічні різниці часів, зловмисник може знайти послідовність бітів експоненти для будь-якого методу.

Нехай j_0 - деяке значення j (порядковий номер біта у представленні експоненти) у відповідному алгоритмі та $g = \begin{cases} 0, \text{для експоненти} 0 \\ 1, \text{для експоненти} 1 \end{cases}$.

Слід зазначити, що $\hat{s}_{i,j_0,g} > 0$ для β-арного методу «зліва направо», оскільки він не залежить від n_j, і $\hat{s}_{i,j_0,g} = \begin{cases} 0, g = 0 \\ > 0, g = 1 \end{cases}$ - час здійснення множення в β-арному методі «справа наліво», коли $n_j = 1$.

Позначимо через binLTR, binRTL – бінарний метод модулярного експоненціювання «зліва направо» та «справа наліво», відповідно, βLTR – β-арний метод зі зчитуванням біт «зліва направо», βRTL – β-арний метод «справа наліво», а *sw*LTR і *sw*RTL – метод ковзаючого вікна «зліва направо» і «справа наліво», відповідно.

Зловмисник може обчислити для бінарного, β-арного методів та методу ковзаючого вікна відповідні часи [118]:

$$\hat{T}_{i,j_0,g\ \text{binLTR}} = t_i + c_i + \sum_{j=k-1}^{j_0+1} (r_{i,j} + s_{i,j}) + (r_{i,j_0} + \hat{s}_{i,j_0,g}), \qquad (2.18)$$

$$\hat{T}_{i,j_0,g\ \text{binRTL}} = t_i + c_i + b_i + \sum_{j=0}^{j_0-1} (r_{i,j} + s_{i,j}) + (r_{i,j_0} + \hat{s}_{i,j_0,g}), \qquad (2.19)$$

$$\widehat{T}_{i,j_0,g_{\beta LTR}} = t_i + 2c_i + (\beta - 1)s_i + \sum_{\substack{j=k-1 \\ n_j=1}}^{j_0+1} (d_{i,j} + s_{i,j}) + (d_{i,j_0} + \widehat{s}_{i,j_0,g}), \quad (2.20)$$

$$\widehat{T}_{i,j_0,g_{\beta\, RTL}} = t_i + (\beta + 1)c_i + b_i + \sum_{\substack{j=0 \\ n_j=1}}^{j_0-1} d_{i,j} + \sum_{\substack{j=0 \\ n_j=1}}^{j_0-1} (d_{i,j} + s_{i,j}) + (d_{i,j_0} + \widehat{s}_{i,j_0,g}), \quad (2.21)$$

$$\hat{T}_{i,j_0,g\ \ SWLTR} = t_i + b_i + (2^{w-1} + p_{j_0})s_i + (p_{j_0} + 1)c_i + \\ + p_{j_0}q_i + \sum_{j=k-1}^{j_0} s_{i,j} + \sum_{\substack{j=k-1 \\ n_{ji}=0}}^{j_0+1} c_{i,j} + \hat{c}_{i,j_0,g}, \quad (2.22)$$

$$\hat{T}_{i,j_0,g\ \ SWRTL} = t_i + b_i + (2^{w-1} + 2 + p_{j_0})c_i + (3 \cdot 2^{w-1} + p_{j_0})s_i + \\ + p_{j_0}d_i + p_{j_0}q_i + \sum_{\substack{j=0 \\ n_j=0}}^{j_0-1} s_{i,j} + \hat{s}_{i,j_0,g}. \quad (2.23)$$

А звідси відповідно різниця виміряного та обчисленого часів $\Delta T = T_i - \hat{T}_i$ для кожного з досліджуваних методів модулярного експоненціювання із врахуванням часу e_i, затраченого на проходження сигналом по каналу зв'язку:

$$\Delta T_{i\,binLTR} = e_i + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (2.24)$$

$$\Delta T_{i\,binRTL} = e_i + \sum_{j=j_0+1}^{k-1} (r_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (2.25)$$

$$\Delta T_{i\beta_{LTR}} = e_i + \sum_{j=j_0-1}^{0} (d_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (2.26)$$

$$\Delta T_{i\beta_{RTL}} = e_i + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} d_{i,j} + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} s_{i,j} + (s_{i,j_0} - \hat{s}_{i,j_0,g}), \qquad (2.27)$$

$$\Delta T_{i\,SWLTR} = e_i + (p - p_{j_0})s_i + (p - p_{j_0})c_i + (p - p_{j_0})q_i + \\ + \sum_{\substack{j=j_0-1 \\ n_j=0}}^{0} s_{i,j} + \sum_{\substack{j=j_0-1 \\ n_j=0}}^{0} c_{i,j} + (c_{i,j_0} - \hat{c}_{i,j_0,g}) \quad , \qquad (2.28)$$

$$\Delta T_{i\,SWRTL} = e_i + (p - p_{j_0})c_i + (p - p_{j_0})s_i + (p - p_{j_0})d_i + \\ + (p - p_{j_0})q_i + \sum_{j=j_0+1}^{k-1} s_{i,j} + (s_{i,j_0} - \hat{s}_{i,j_0,g}) \quad . \qquad (2.29)$$

Якщо $\hat{s}_{i,j_0,g}$ визначене правильно, то $\hat{s}_{i,j_0,g} \equiv s_{i,j_0}$. Звідси випливає, що $\Delta T_{i\,\mathrm{binLTR}} = \mathrm{e_i} + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j})$, $\Delta T_{i\,\mathrm{binRTL}} = \mathrm{e_i} + \sum_{j=j_0+1}^{k-1} (r_{i,j} + s_{i,j})$ (для бінарного методу), $\Delta T_{i\beta_{LTR}} = e_i + \sum_{j=j_0-1}^{0} (d_{i,j} + s_{i,j})$ та $\Delta T_{i\,\beta RTL} = e_i + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} d_{i,j} + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} s_{i,j}$ (для β-арного методу).

Для методу ковзаючого вікна, якщо $c_{i,j_0} \equiv \hat{c}_{i,j_0,g}$, то $\Delta T_{iSWRTL} = e_i + (p - p_{j_0})(s_i + c_i + d_i + q_i) + \sum_{j=j_0+1}^{k-1} s_{i,j}$ (при зчитуванні біт «справа наліво») та $\Delta T_{iSWLTR} = e_i + (p - p_{j_0})(s_i + c_i + q_i) + \sum_{j=j_0-1}^{0} s_{i,j} + \sum_{\substack{j=j_0-1 \\ n_j=0}}^{0} c_{i,j}$ («зліва направо»).

Проте, на практиці $\hat{s}_{i,j_0,g} \neq s_{i,j_0}$ чи $c_{i,j_0} \neq \hat{c}_{i,j_0,g}$, а це означає, що правильно визначити $\hat{s}_{i,j_0,g}$ чи $\hat{c}_{i,j_0,g}$ дуже важко. Саме тому необхідно

оцінити ймовірність успіху атаки.

Застосовуючи методи теорії ймовірності [119-122], спочатку обчислимо дисперсію випадкової змінної $T - \hat{T}_{j_0,g}$ з наступними умовами:

1) g визначене правильно (тобто правильно знайдене n_j), тоді дисперсії для кожного з досліджуваних методів [118]:

$$\sigma^2(\Delta T)_{binLTR} = \sigma^2(e) + j_0\sigma^2(r) + \frac{1}{2} j_0\sigma^2(s), \tag{2.30}$$

$$\sigma^2(\Delta T)_{binRTL} = \sigma^2(e) + (k - j_0 - 1)\sigma^2(r) + \frac{1}{2}(k - j_0 - 1)\sigma^2(s), \tag{2.31}$$

$$\sigma^2(\Delta T)_{\beta LTR} = \sigma^2(e) + j_0\sigma^2(d) + j_0\sigma^2(s)\ , \tag{2.32}$$

$$\sigma^2(\Delta T)_{\beta RTL} = \sigma^2(e) + (k - j_0 - 1)\sigma^2(d) + \frac{1}{2}(k - j_0 - 1)\sigma^2(s), \tag{2.33}$$

$$\begin{aligned}\sigma^2(\Delta T)_{SWLTR} &= \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \\ &+ \sigma^2(c) + \sigma^2(q)) + j_0\sigma^2(s) + \frac{1}{2} j_0\sigma^2(c)\end{aligned}\ , \tag{2.34}$$

$$\begin{aligned}\sigma^2(\Delta T_i)_{SWRTL} &= \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \sigma^2(c) + \sigma^2(d) + \\ &+ \sigma^2(q)) + \frac{1}{2}(k - j_0 - 1)\sigma^2(s)\end{aligned}\ . \tag{2.35}$$

Якщо припустити, що операції піднесення до квадрату та множення еквівалентні (а в більшості прикладних імплементацій так воно і є), тобто $r = s$, а також, що час, затрачений на виконання операції $z = z^{\beta} \bmod m$, рівний $(\beta - 1)s$, то:

$$\sigma^2(\Delta T)_{binLTR} = \sigma^2(e) + \frac{3}{2} j_0 \sigma^2(s), \tag{2.36}$$

$$\sigma^2(\Delta T)_{binRTL} = \sigma^2(e) + \frac{3}{2}(k - j_0 - 1)\sigma^2(s), \tag{2.37}$$

$$\sigma^2(\Delta T)_{\beta\,LTR} = \sigma^2(e) + \beta j_0 \sigma^2(s), \tag{2.38}$$

$$\sigma^2(\Delta T)_{\beta RTL} = (k - j_0 - 1)(\beta - \frac{1}{2})\sigma^2(s). \tag{2.39}$$

2) g визначене неправильно, тоді можливі два випадки:

а) $\begin{cases} \hat{s}_{i,j_0,g} \neq 0 \\ s_{i,j_0} \neq 0 \end{cases}$ (для бінарного та β-арного методів)

чи $\begin{cases} c_{i,j_0} \neq 0 \\ \hat{c}_{i,j_0,g} \neq 0 \end{cases}$ (для методу ковзаючого вікна),

тоді [118]:

$$\sigma^2(\Delta T)_{binLTR} = \sigma^2(e) + \left(\frac{3}{2} j_0 + 2\right)\sigma^2(s), \tag{2.40}$$

$$\sigma^2(\Delta T)_{binRTL} = \sigma^2(e) + \left(\frac{3}{2}(k - j_0 - 1) + 2\right)\sigma^2(s), \tag{2.41}$$

$$\sigma^2(\Delta T)_{\beta\,LTR} = (\beta + 1)(j_0 + 2)\sigma^2(s), \tag{2.42}$$

$$\sigma^2(\Delta T)_{\beta RTL} = \sigma^2(e) + ((k - j_0 - 1)(\beta - \frac{1}{2}) + 2)\sigma^2(s), \tag{2.43}$$

$$\sigma^2(\Delta T)_{SW\ LTR} = \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \sigma^2(c) + \sigma^2(q)) + \\ + j_0\sigma^2(s) + (\frac{1}{2} j_0 + 2)\sigma^2(c), \tag{2.44}$$

$$\sigma^2(\Delta T)_{SW\ RTL} = \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \sigma^2(c) + \sigma^2(d) + \sigma^2(q)) + \\ + (\frac{1}{2}(k - j_0 - 1) + 2)\sigma^2(s). \tag{2.45}$$

б) $\left[\begin{cases} s_{i,j_0} \neq 0 \\ \hat{s}_{i,j_0,g} = 0 \end{cases}\right.$ (для бінарного методу та β-арного методу «справа наліво»)

чи $\left[\begin{cases} c_{i,j_0} = 0 \\ \hat{c}_{i,j_0,g} \neq 0 \end{cases}\right.$ (для методу ковзаючого вікна). Звідси:

$$\sigma^2(\Delta T)_{binLTR} = \sigma^2(e) + \left(\frac{3}{2} j_0 + 1\right)\sigma^2(s), \tag{2.46}$$

$$\sigma^2(\Delta T)_{binRTL} = \sigma^2(e) + \left(\frac{3}{2}(k - j_0 - 1) + 1\right)\sigma^2(s), \tag{2.47}$$

$$\sigma^2(\Delta T)_{\beta RTL} = \sigma^2(e) + ((\beta - \frac{1}{2})(k - j_0 - 1) + 1)\sigma^2(s), \tag{2.48}$$

$$\sigma^2(\Delta T)_{SWLTR} = \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \sigma^2(c) + \sigma^2(q)) + \\ + j_0\sigma^2(s) + (\frac{1}{2} j_0 + 1)\sigma^2(c), \tag{2.49}$$

$$\sigma^2(\Delta T)_{SWRTL} = \sigma^2(e) + (p - p_{j_0})(\sigma^2(s) + \sigma^2(c) + \sigma^2(d) + \\ + \sigma^2(q)) + (\frac{1}{2}(k - j_0 - 1) + 1)\sigma^2(s). \tag{2.50}$$

Дисперсія $\sigma^2(\Delta T)$ може бути використана як критерій правильності припущення бітів експоненти, оскільки стовпчик таблиці 2.4 різниць часів з правильним припущенням має розкид на $2\sigma^2(s)$ для β-арного методу «зліва направо», $\sigma^2(s)$ та $2\sigma^2(s)$ для бінарного методу та β-арного методу «справа наліво», $\sigma^2(c)$ для методу ковзаючого вікна «зліва направо» та на $2\sigma^2(c)$ для методу ковзаючого вікна «справа наліво» нижчий, ніж інші стовпчики значень. Тобто, рівень похибки вимірювання часу виконання алгоритму модулярного експоненціювання залежить від кількості вимірювань. Тому необхідно оцінити ризик витоку таємної інформації під час проведення часового аналізу розглянутих методів модулярного експоненціювання.

Нехай $N\left(\mu_r, \sigma_r^2\right)$ – розподіл r, а $N\left(\mu_c, \sigma_c^2\right)$, $N\left(\mu_d, \sigma^2{}_d\right)$, $N\left(\mu_q, \sigma_q^2\right)$, $N\left(\mu_s, \sigma_s^2\right)$ - розподіли змінних c, d, q та s, відповідно.

Крім того, нехай $N\left(\mu_0, \sigma_0^2\right)$ – розподіл очікуваного значення ΔT.

Відповідно до аналізу, проведеного в [112, 113, 117, 118], ризик витоку таємної інформації:

$$P\left(S_W^2 > S_V^2\right) \approx P\left(2\sigma_0\sqrt{K}Z + \sigma_s K > 0\right) = P\left(Z > -\frac{\sigma_s}{\sigma_0}\frac{\sqrt{K}}{2}\right) = \Phi\left(\frac{\sigma_s}{\sigma_0}\frac{\sqrt{K}}{2}\right), \quad (2.51)$$

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.

Звідси можна записати для бінарного, β-арного та методу ковзаючого вікна:

$$\frac{\sigma_s}{\sigma_{0\,binLTR}} = \sqrt{\frac{\sigma_s^2}{\frac{3}{2} j_0 \sigma_s^2}} = \sqrt{\frac{2}{3 j_0}}, \tag{2.52}$$

$$\frac{\sigma_s}{\sigma_{0\,binRTL}} = \sqrt{\frac{\sigma_s^2}{\frac{3}{2}(k - j_0 - 1)\sigma_s^2}} = \sqrt{\frac{2}{3(k - j_0 - 1)}}, \tag{2.53}$$

$$\frac{\sigma_s}{\sigma_{0\,\beta LTR}} = \sqrt{\frac{\sigma_s^2}{j_0(\sigma_d^2 + \sigma_s^2)}} = \sqrt{\frac{1}{\beta j_0}}, \tag{2.54}$$

$$\frac{\sigma_s}{\sigma_{0\,\beta RTL}} = \sqrt{\frac{\sigma_s^2}{(k - j_0 - 1)(\sigma_d^2 + \frac{1}{2}\sigma_s^2)}} = \sqrt{\frac{2}{(k - j_0 - 1)(\beta - \frac{1}{2})}}, \tag{2.55}$$

$$\frac{\sigma_c}{\sigma_{0\,SWLTR}} = \sqrt{\frac{1}{(p - p_{j_0})(\frac{\sigma_q^2}{\sigma_c^2} + \frac{\sigma_s^2}{\sigma_c^2} + 1) + j_0 \frac{\sigma_s^2}{\sigma_c^2} + \frac{1}{2} j_0}}, \tag{2.56}$$

$$\frac{\sigma_s}{\sigma_{0\,SWRTL}} = \sqrt{\frac{1}{(p - p_{j_0})(\frac{\sigma_c^2}{\sigma_s^2} + \frac{\sigma_d^2}{\sigma_s^2} + \frac{\sigma_q^2}{\sigma_s^2} + 1) + \frac{1}{2}(k - j_0 - 1)}}. \tag{2.57}$$

Ризик витоку таємної інформації для бінарного, β-арного методів та методу ковзаючого вікна, враховуючи (2.51), можна оцінити як [118]:

$$P_{binLTR}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{k}{6 j_0}}\right), \tag{2.58}$$

$$P_{binRTL}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{k}{6(k-j_0-1)}}\right), \quad (2.59)$$

$$P_{\beta LTR}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{K}{4\beta_{j_0}}}\right), \quad (2.60)$$

$$P_{\beta RTL}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{K}{(k-j_0-1)(2\beta-1)}}\right), \quad (2.61)$$

$$P_{SWLTR}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{K}{4((p-p_{j_0})(\frac{\sigma_q^2}{\sigma_c^2}+\frac{\sigma_s^2}{\sigma_c^2}+1)+j_0\frac{\sigma_s^2}{\sigma_c^2}+\frac{1}{2}j_0)}}\right), \quad (2.62)$$

$$P_{SWRTL}\left(S_W^2 > S_V^2\right) \approx P\left(Z > -\sqrt{\frac{K}{4((p-p_{j_0})(\frac{\sigma_c^2}{\sigma_s^2}+\frac{\sigma_d^2}{\sigma_s^2}+\frac{\sigma_q^2}{\sigma_s^2}+1)+\frac{1}{2}(k-j_0-1))}}\right). \quad (2.63)$$

Зі збільшенням K, ймовірність успіху атаки також збільшується. Очевидно також, що ризик витоку таємної інформації зростає у відповідності до кількості правильно визначених бітів, причому ентропія зменшується.

У [104-108] вказано наближені співвідношення між часами c, b, t, q, s та d (див. таблицю 2.1). Наступна оцінка враховує ці співвідношення.

Для порівняння аналізованих методів, приймемо, що $p_{j_0} = p \cdot \frac{j_0}{k}$. Тоді, з імовірнісних наближень, випливає, що $p - p_{j_0} = \frac{j_0}{3}$.

Залежності ризику витоку таємної інформації від j_0 для бінарного, β-

арного методів та методу ковзаючого вікна, де кількість експериментів рівна 100 і експонента має довжину 1024 біти, показані на рисунку 2.9 та рисунку 2.10, відповідно [113].

З рисунків 2.9 та 2.10 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 у п.2.2 та 2.3 дослідження.

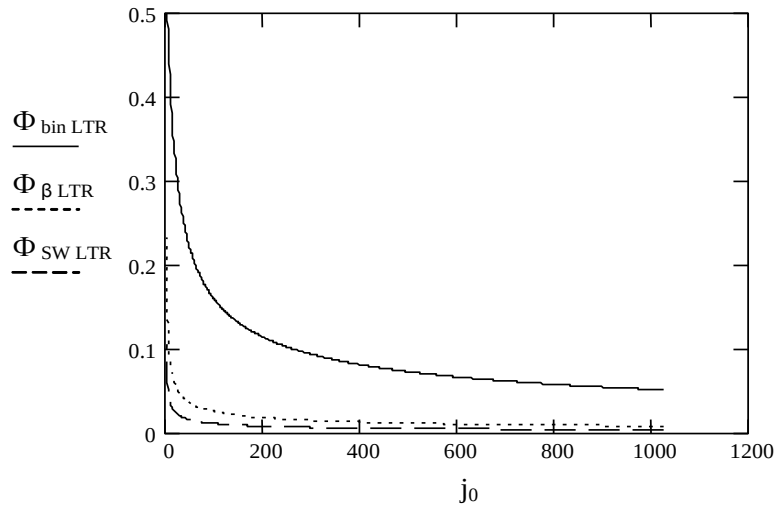


Рисунок 2.9 - Залежність ризику витоку таємної інформації від j_0 у випадку зчитування бітів експоненти «зліва направо».

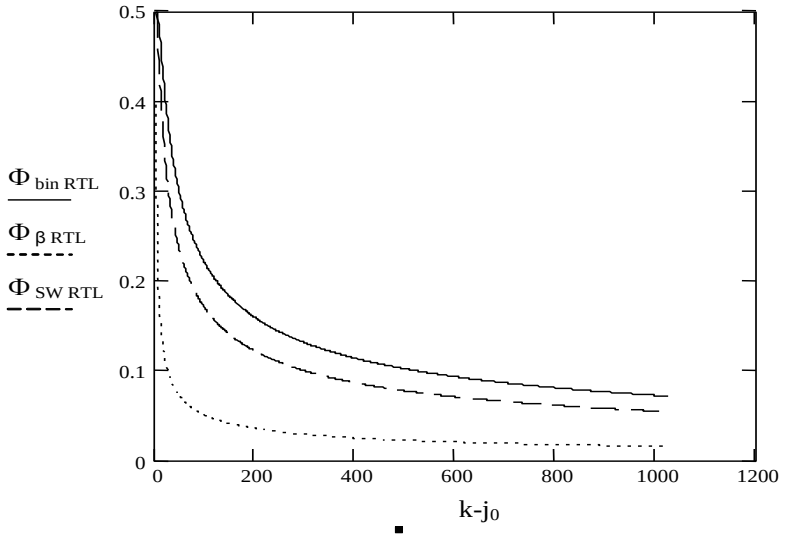


Рисунок 2.10 - Залежність ризику витоку таємної інформації від j_0 у випадку зчитування бітів експоненти «справа наліво»

Таким чином, для зменшення ризику витоку таємної інформації під час здійснення часового аналізу можна запропонувати такі шляхи:

1) збільшення помилки вимірювання шляхом внесення випадкових обчислень, щоб зменшити можливість правильного визначення біт таємного ключа;

2) зменшення кількості повідомлень, зашифрованих одним ключем, для зменшення ймовірності ризику витоку таємної інформації.

Досліджені в даному розділі параметри криптосистеми RSA, а саме продуктивність, об’ємна складність та стійкість до часового аналізу, є достатніми та необхідними при побудові сучасних комп’ютерних систем з розподілом доступу. Ще один важливий параметр криптосистеми, а саме довжину ключа, недоцільно виокремлювати, оскільки вона інтерпретується вагою Хемінга, що є основою для проведених досліджень.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Основними параметрами оцінки сучасних систем захисту інформації, які реалізують криптоалгоритм RSA, є продуктивність, затрати пам’яті та стійкість алгоритму використаного методу модулярного експоненціювання до атак на реалізацію, зокрема до часового аналізу. Досліджено, що найвищу продуктивність та прийнятні затрати пам’яті має алгоритм β-арного методу модулярного експоненціювання.

2. Досліджено залежність часу виконання алгоритмів модулярного експоненціювання від ваги Хемінга експоненти та встановлено, що β-арний метод модулярного експоненціювання має найвищу стійкість до пасивних атак, в яких проводиться аналіз ваги Хемінга, зокрема до найнебезпечнішої – атаки часового аналізу.

3. Запропоновано та досліджено метод визначення нормованої стійкості алгоритмів модулярного експоненціювання до часового аналізу, що базується на залежності часу виконання алгоритму модулярного експоненціювання від ваги Хемінга. Встановлено, що найкращими для застосування є алгоритм β-арного методу та методу «ковзаючого вікна» модулярного експоненціювання зі зчитуванням бітів експоненти «зліва направо».

4. Проведено оцінку стійкості методів модулярного експоненціювання до часового аналізу на основі ймовірнісних наближень і встановлено, 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».

РОЗДІЛ 3
НЕЧІТКА СИСТЕМА ВИБОРУ МЕТОДУ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ

3.1 Схема розподілу доступу до інформаційних ресурсів комп'ютерної системи

Основними критеріями працездатності комп'ютерної системи є висока продуктивність, оптимальні затрати пам'яті та стійкість до атак зловмисника.

Будь-яка комп'ютерна система може бути захищена від активних атак зловмисників, які можна виявити в процесі експлуатації завдяки відомим заходам політики безпеки [4]. Проте, існує також можливість виникнення пасивних атак (атака часового аналізу чи аналізу енергоспоживання), які можуть здійснюватись віддалено і тому їх важко виявити [50, 51].

Комп'ютерна система при передачі інформації використовує мережу для здійснення доступу клієнтів. Таку мережу передачі даних можна умовно розділити на захищену та незахищену частини (рисунок 3.1).

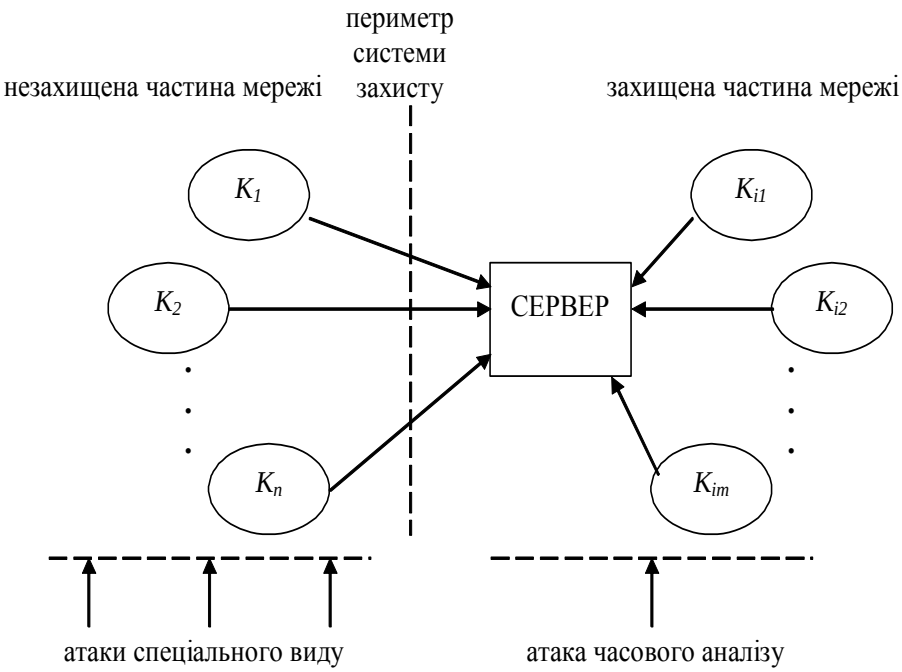


Рисунок 3.1 - Схема здійснення можливих атак на реалізацію при передачі даних в комп'ютерній системі

У незахищеній частині мережі клієнти $K_1, K_2, ..., K_n$ можуть бути випадковими, тому вони не є надійними для сервера з точки зору безпеки, тобто є велика ймовірність існування зловмисника. 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 (див. рисунок 3.1) 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 [50].

Сервер комп'ютерної системи складається з підсистеми ідентифікації клієнта, командної підсистеми та блоку оброблення інформації (рисунок 3.2).

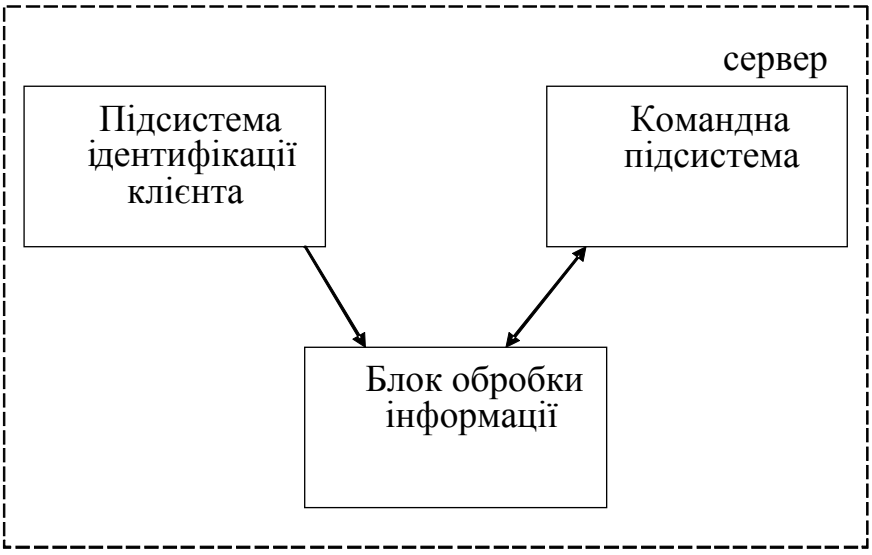


Рисунок 3.2 - Структура сервера комп'ютерної системи

Підсистема ідентифікації клієнта подає на блок оброблення інформації дані про необхідний рівень стійкості до часового аналізу, враховуючи усі дані про користувача.

Клієнти мережі відомі серверу по IP-адресі і, враховуючи «стаж»

користування мережею, мають свій рівень довіри, що можна задати ймовірністю збоїв при передачі пакетів інформації.

Отже, якщо клієнт є новим для даної системи або має рівень довіри дуже низький, то необхідний рівень стійкості до часового аналізу повинен бути максимальним, тобто рівним 1, згідно досліджень, проведених у п.2.3. І навпаки, для клієнта з дуже високим рівнем довіри значення стійкості може прямувати до 0, що забезпечить підвищення швидкодії системи.

Щодо незахищеної частини мережі, то можна застосувати рекомендації стосовно підвищення стійкості до часового аналізу, подані у п.2.4.

Командна підсистема сервера (див. рисунок 3.2) подає на блок оброблення інформацію про саму комп'ютерну систему, тобто допустимі затрати пам'яті та необхідний рівень продуктивності.

Для захисту інформації у мережі необхідно оптимально вибрати метод піднесення до степеня за модулем для здійснення шифрування інформації чи проведення аутентифікації клієнта за допомогою криптоалгоритму RSA. Це завдання вирішує блок оброблення інформації, побудований на основі нечіткої логіки, а саме, на механізмі нечіткого висновку Мамдані, описаному у п.1.4 [99]. Він опрацьовує вхідні значення продуктивності, затрат пам'яті та стійкості до часового аналізу і подає оптимальний у кожному випадку метод модулярного експоненціювання на командну підсистему, яка в свою чергу, застосовує його для шифрування інформації. Основною перевагою цього блоку є те, що він працює в режимі реального часу, що забезпечує вищу стійкість системи від атак зловмисника, оскільки він не буде достовірно знати алгоритму шифрування [123-130].

Загальну схему розподілу доступу в комп'ютерній системі подано на рисунку 3.3.

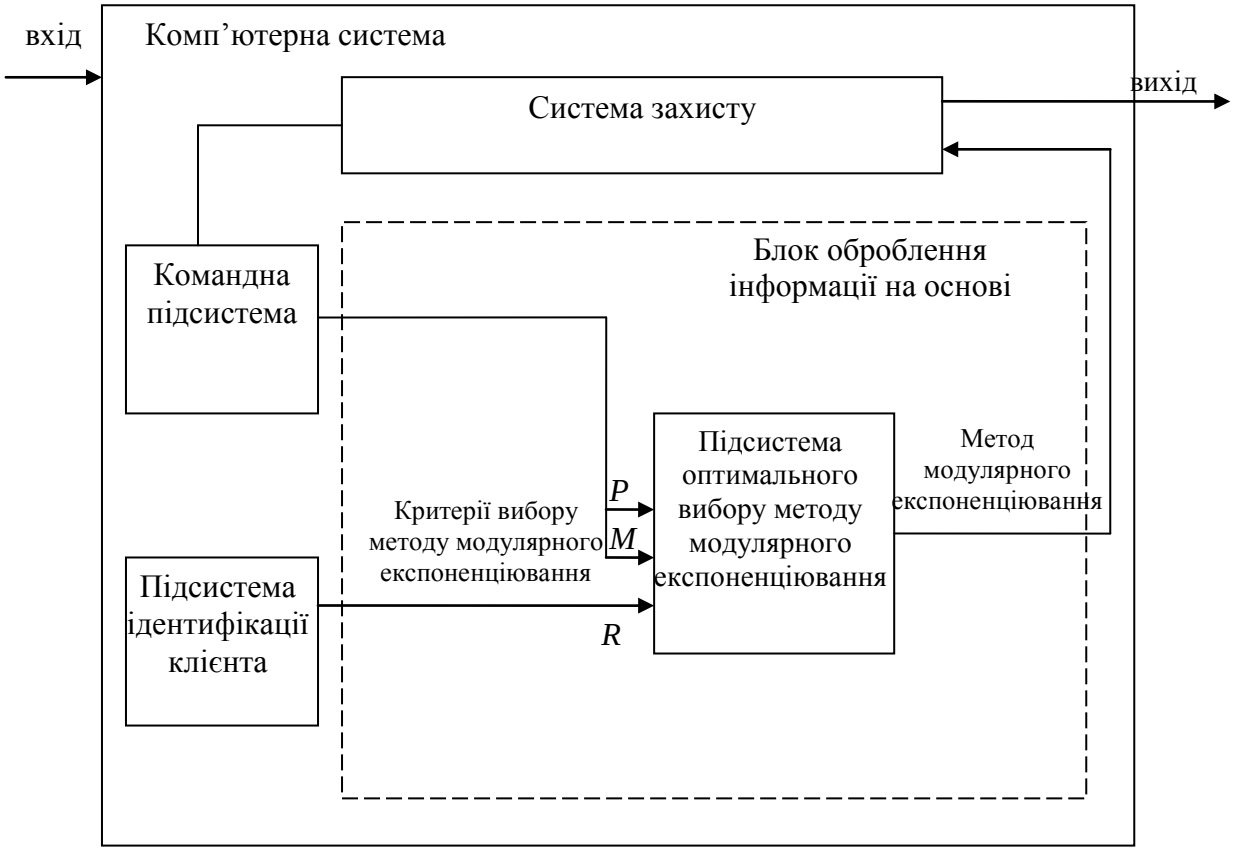


Рисунок 3.3 - Загальна схема розподілу доступу в комп'ютерній системі на основі нечіткої логіки:

P – продуктивність,

M – допустимі затрати пам'яті,

R – нормована стійкість до часового аналізу

Блок оброблення інформації на основі нечіткої логіки є основою системи захисту комп'ютерної системи. На його вхід поступають критерії вибору методу модулярного експоненціювання, серед яких необхідний рівень стійкості до часового аналізу *R*, продуктивності криптосистеми *P* та допустимі затрати пам'яті сервера *M*. Вхідні нечіткі дані опрацьовуються підсистемою оптимального вибору методу піднесення до степеня за модулем на основі механізму нечіткого висновку за механізмом Мамдані. Виходом блоку оброблення інформації є метод модулярного експоненціювання, що забезпечує оптимальну конфігурацію системи захисту відносно значень вхідних критеріїв вибору.

Таким чином, запропонована в даному підрозділі структура сервера комп’ютерної мережі дає можливість забезпечити оптимальну його роботу шляхом розподілу доступу до інформаційних ресурсів.

3.2 Метод оптимального вибору алгоритму модулярного експоненціювання

На блок оброблення інформації сервера системи захисту КС поступає нечітка інформація про необхідний рівень продуктивності та стійкості до часового аналізу, а також про допустимі затрати пам’яті.

В якості експертної оцінки вхідних даних відповідно до кожного з методів піднесення до степеня за модулем можна використати значення, подані у таблиці 2.3, та формули таблиці 2.4.

Застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB 7.7.0 (R2008b) [131], можна побудувати нечітку систему оптимального вибору методу модулярного експоненціювання (*method*) залежно від значень продуктивності (*performance*), стійкості до часового аналізу (*resistance*) та допустимих затрат пам’яті (*memory*) [132].

В якості бінарного методу можна використовувати бінарний метод з будь-яким напрямом зчитування бітів, оскільки, згідно з [113], вони мають ідентичну стійкість до атаки часового аналізу, а їх продуктивність практично однакова.

Значення функцій належності вхідних змінних *resistance* та *memory* задається трапецевидною функцією, що задається четвіркою чисел (*a*,*b*,*c*,*d*), які позначають абсциси вершин трапеції,

$$MF(x)=\begin{cases}\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ \dfrac{x-c}{d-c}, c\le x\le d\\ 0, \text{в інших випадках}\end{cases}, \qquad (3.1)$$

а вхідної змінної *performance* – дзвоноподібною функцією [99]

$$MF(x)=\frac{1}{1+\left|\dfrac{x-c}{a}\right|^{2b}}, \qquad (3.2)$$

яка задається трьома числами (*a*,*b*,*c*), що відповідають абсцисам крайніх точок та центру кривої.

Функція належності виходу *method* задається трикутною формою, яка залежить від трьох змінних (*a*,*b*,*c*) (абсциси вершин трикутника) [133]

$$MF(x)=\begin{cases}\dfrac{b-x}{b-a}, a\le x\le b\\ \dfrac{x-c}{c-b}, b\le x\le c\\ 0, \text{в інших випадках}\end{cases}, \qquad (3.3)$$

при чому в даному випадку має місце випадок симетричної трикутної функції належності, тобто (*b*-*a*)=(*c*-*b*).

Моделювання нечіткого висновку [134] здійснюється по типу Мамдані [99], описаному вище (див. п.1.4).

Функції належності для змінних *resistance*, *performance* та *memory*, подані на рисунках 3.4, 3.5 та рисунку 3.6, відповідно [135]. Вони поділені на три інтервали кожна для точного опису змінних, зокрема, для опису стійкості

до часового аналізу застосовується змінна $low \in [0,0.014]$, що позначає низький рівень стійкості, $middle \in [0.0145,0.72]$ - середній рівень та $high \in [0.56,1]$ - високий рівень.

Для задання продуктивності пропонуються змінні $high \in [0, 31000]$, $middle \in [27000, 75000]$ та $small \in [67000, 100000]$, що відповідають високому, середньому та низькому рівню (див.рисунок 3.5).

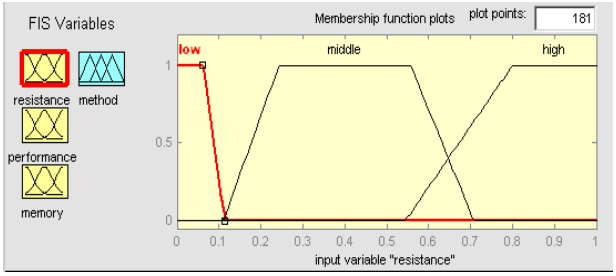


Рисунок 3.4 - Функції належності змінної *resistance*.

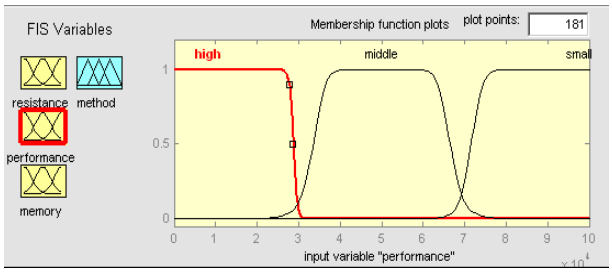


Рисунок 3.5 - Функції належності змінної *performance*.

Допустимі затрати пам'яті задаються значеннями $small \in [0, 9920]$, $middle \in [9921, 2.52 \cdot 10^5]$ і $big \in [2.49 \cdot 10^5, 5 \cdot 10^5]$, що відповідають малим, середнім та великим затратам, відповідно (див. рисунок 3.6).

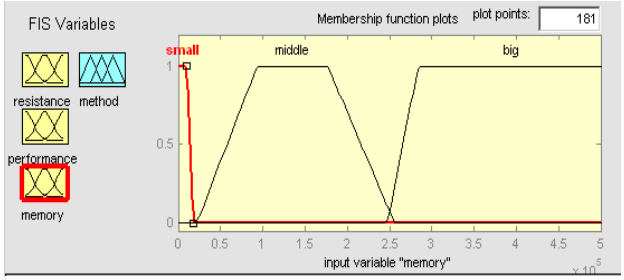


Рисунок 3.6 - Функції належності змінної *memory*.

Функції належності для вихідної змінної *method* зображено на рисунку 3.7. Вони позначаються однаковими інтервалами на осі ординат для точного визначення центру ваги, що позначає нечіткий висновок системи [99]. *Binary* позначає бінарний метод модулярного експоненціювання, *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».

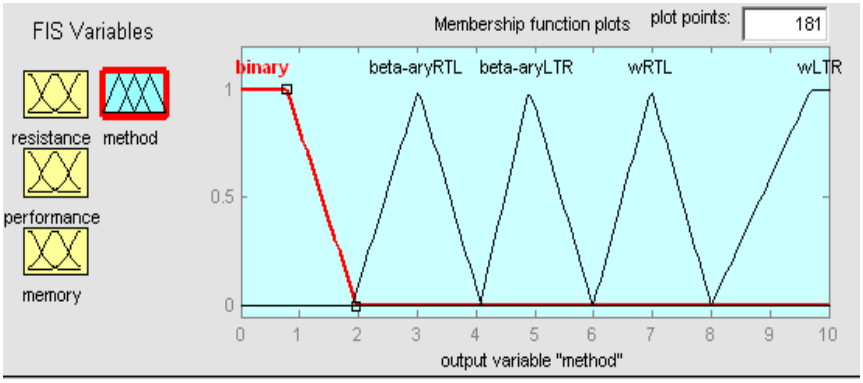


Рисунок 3.7 - Функції належності змінної *method*.

На рисунку 3.8 зображено логічний висновок за механізмом Мамдані на прикладі двох правил R1 та R2, в яких знаходяться мінімальні площі в зображеннях функцій належності трьох змінних, після чого здійснюється об'єднання усічених площ за максимальним законом і, нарешті, знаходиться центр ваги остаточної фігури, абсциса якого і є висновком нечіткої системи [136-138].

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то» [139], усі вхідні змінні мають по три нечітких стани і ще один стан *none*, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \cdot 4 \cdot 4 - 1 = 63$.

Система правил нечіткого висновку подана у додатку В.

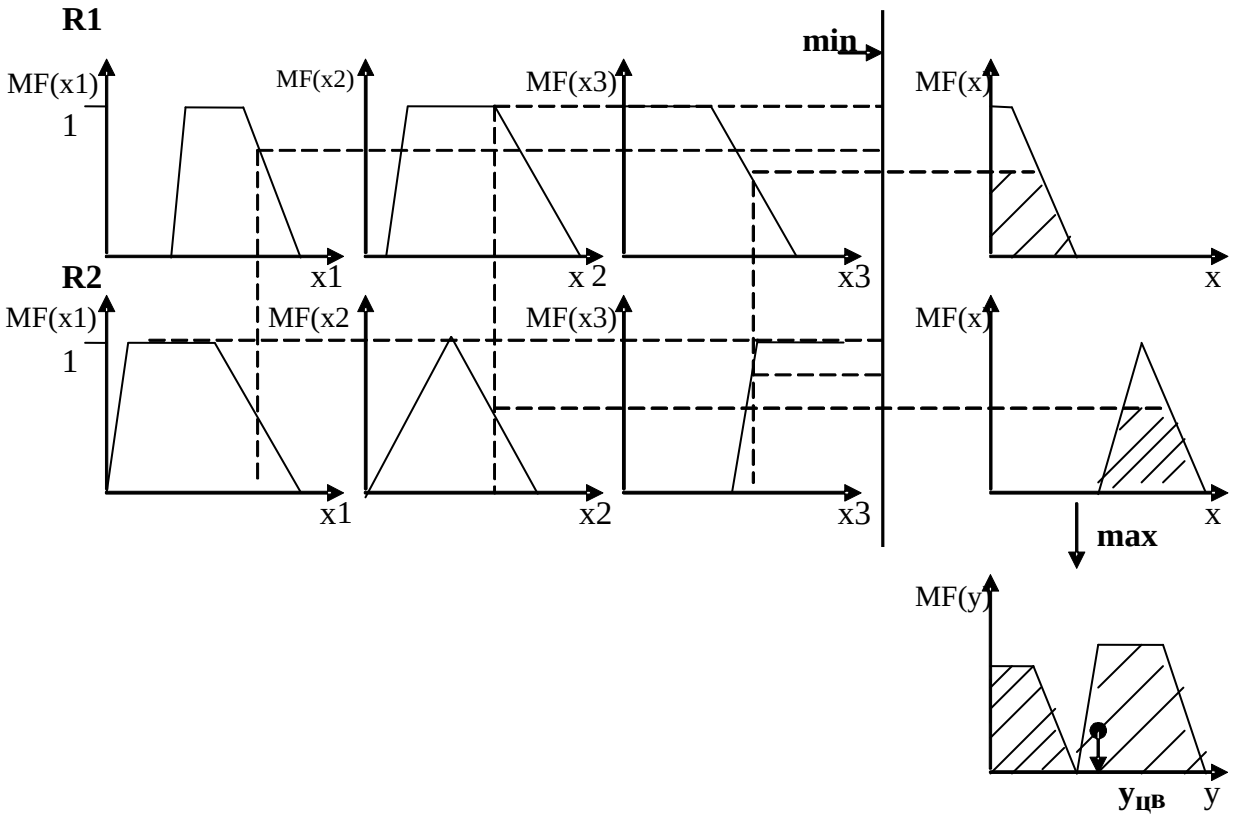


Рисунок 3.8 - Механізм нечіткого висновку Мамдані

Нечіткий висновок моделі вибору методу модулярного експоненціювання, побудованого на основі заданих 63 правил з поточними значеннями змінних *resistance*, *performance*, *memory* та *method*, має вигляд, представлений на рисунку 3.9 [139].

Лістинг побудованої моделі за класичним механізмом Мамдані, розроблений засобами MATLAB, поданий в додатку Г.

Поверхні значень нечіткої системи на основі механізму Мамдані подані на рисунку 3.10 [139]. Вони підтверджують правильність побудови бази правил нечіткого висновку.

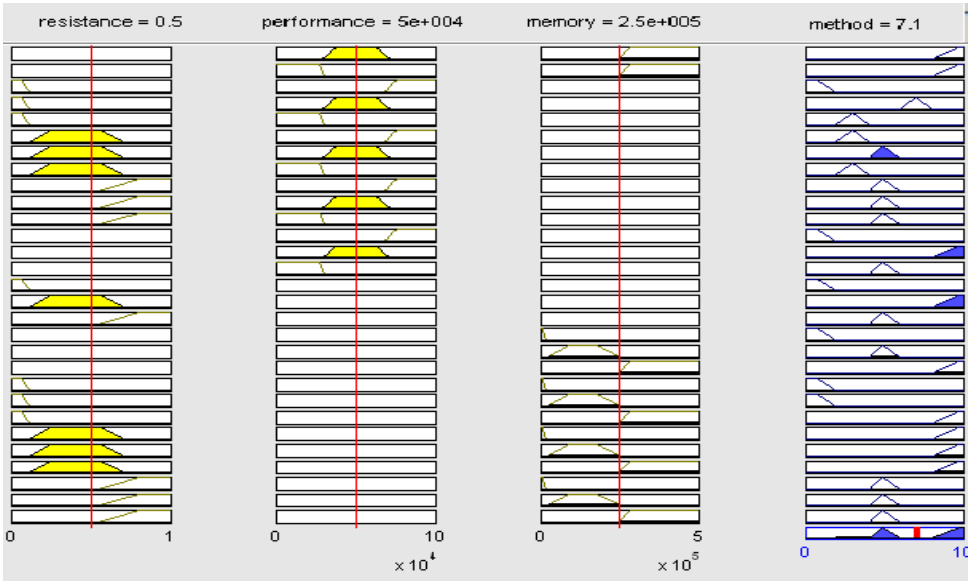
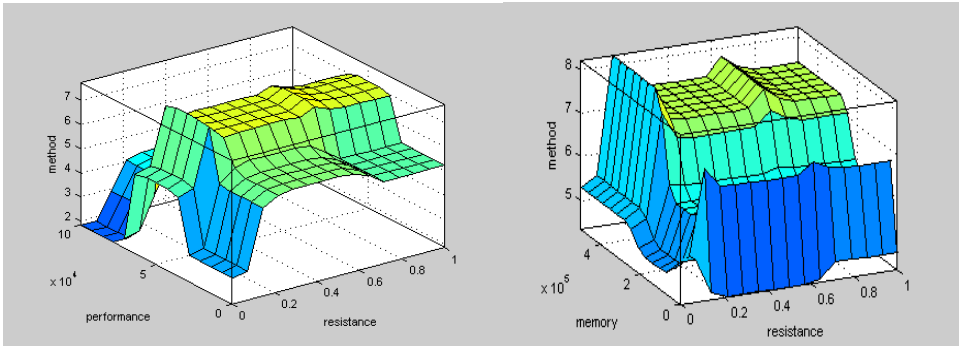
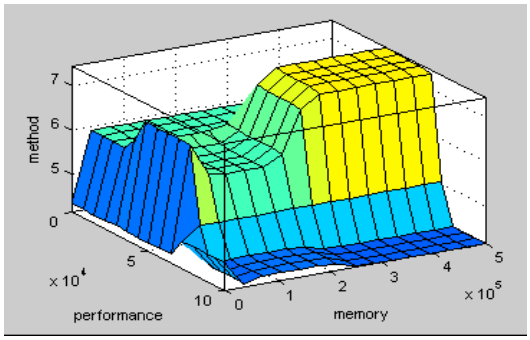


Рисунок 3.9 - Нечіткий висновок моделі вибору методу модулярного експоненціювання.



а) б)



в)

Рисунок 3.10 - Поверхня 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.

Основний недолік нечіткого висновку, побудованого на класичному механізмі Мамдані, полягає в тому, що для будь-яких вхідних даних необхідно опрацьовувати усю базу правил, тобто здійснювати три кроки (див. рисунок 3.8). Такий шлях оброблення нечітких даних знижує швидкодію системи та вимагає великих затрат пам’яті, тому варто вдосконалити метод вибору методу модулярного експоненціювання [134, 140], що базується на класичному методі Мамдані, який би задовольняв вимоги до швидкодії.

3.3 Метод оброблення нечітких даних для налаштування сервера

Суть пропонованого методу вибору методу піднесення до степеня за модулем полягає в тому, що процес оброблення вхідної нечіткої інформації розділено на етапи навчання та експлуатації.

Під час навчання засобу оброблення нечіткої інформації визначено області функцій належності виходу для кожного з правил.

Під час 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 [141, 142].

На рисунку 3.11 зображено схему алгоритму реалізації пропонованого методу оброблення нечітких даних.

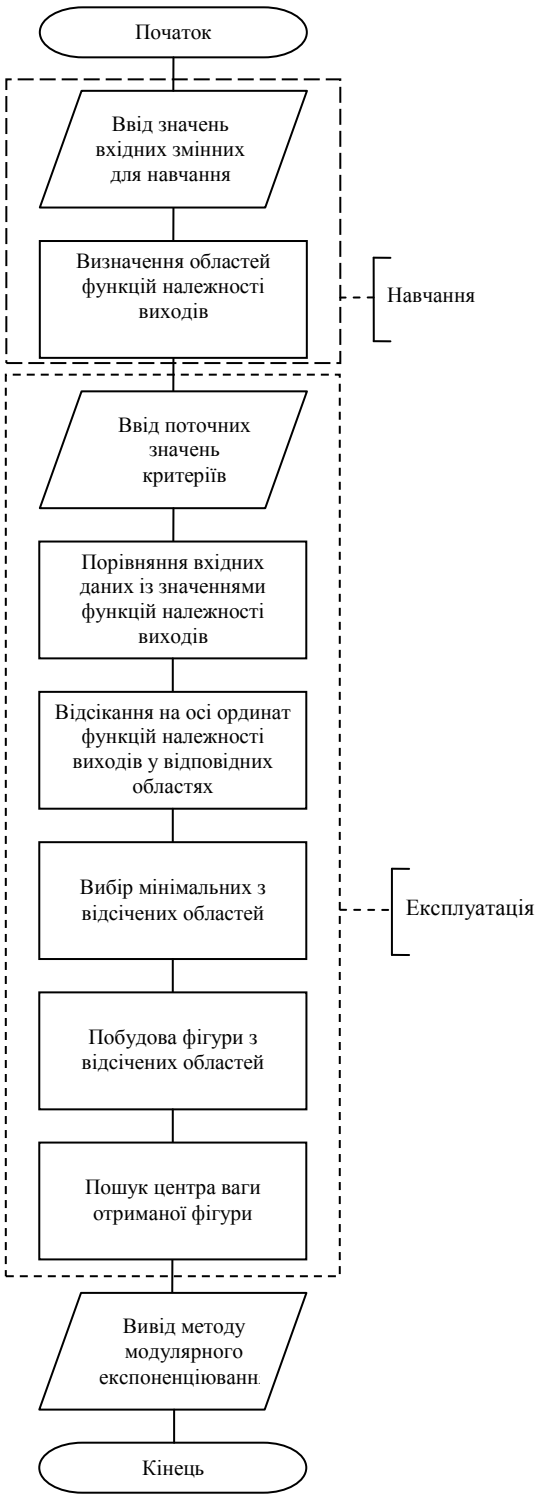


Рисунок 3.11 - Схема алгоритму реалізації пропонованого методу оброблення нечітких даних

Порівняння операцій пропонованого методу оброблення нечіткої інформації та класичного, поданого у [141], під час експлуатації приведено в таблиці 3.1 [142].

Таблиця 3.1 - Операції з оброблення нечіткої інформації

№ п/п	Операції нечіткого висновку за класичним механізмом Мамдані	Операції нечіткого висновку пропонованого методу	
		Співпадаючі операції пропонованого методу	Нові операції пропонованого методу
1	Порівняння вхідних даних зі значеннями функцій належності входів	–	Порівняння вхідних даних зі значеннями функцій належності виходів у відповідних областях ПЗП
2	Знаходження найменшого значення функцій належності входів щодо кожного з входів, які відповідають базі правил	–	–
3	Відсікання на осі ординат функцій належності виходу значень, які перевищують значення, знайдені в п. 2	–	Відсікання на осі ординат функцій належності виходу у всіх відповідних областях багатоканального блоку пам’яті значень, які перевищують значення, знайдені в п. 1
4	Знаходження серед відсічених функцій належності виходу тих, що мають максимальну амплітуду	–	Знаходження серед відсічених функцій належності виходу у всіх відповідних областях багатоканального блоку пам’яті тих, що мають мінімальну амплітуду
5	Знаходження суми знайдених в п. 4 значень відсічених функції належності виходу, що утворює кінцеву фігуру	Знаходження суми знайдених в п. 4 значень відсічених функції належності виходу, що утворює кінцеву фігуру	–
6	Знаходження центра ваги отриманої в п. 5 фігури	Знаходження центра ваги отриманої в п. 5 фігури	–

Як видно з таблиці 3.1, всі операції пропонованого методу близькі до операцій класичного механізму Мамдані і за складністю не перевищують їх. Однак кількість операцій у пропонованому методі менша, що спричиняє зростання його швидкодії. Зменшення кількості операцій зумовлено тим, що на етапі навчання (який передує етапу експлуатації) визначено області функцій належності виходу для кожного з правил. Результати записано у відповідні області багатоканального блоку пам'яті, звідки вони вибираються при виконанні операцій пп. 3, 4 таблиці 3.1. Така попередня підготовка власне й дозволяє уникнути операції, передбаченої в п. 2 методу Мамдані.

Так як часова складність є основним критерієм оцінки алгоритму, то розглядаючи операції нечіткого висновку пропонованого методу та механізму Мамдані, описані в таблиці 3.1, для порівняння складності цих алгоритмів варто розглянути лише неспівпадаючі операції. В таблиці 3.2 подано часові складності кожної операції розглянутих методів нечіткого висновку, враховуючи обчислення складності, проведені у [143-147].

Аналіз таблиці 3.2 показує, що часова складність пропонованого методу оброблення нечіткої інформації є на $O(n^2)$ менша, ніж складність механізму нечіткого висновку Мамдані.

Таким чином, пропонований метод, згідно значень часової складності, поданих у [143], має швидкодію вчетверо вищу, ніж класичний (при використанні аналогічної апаратної бази). Зменшити кількість операцій у пропонованому методі та виконувати їх саме таким чином, як це вказано у таблиці 3.1, вдається лише за рахунок попередньої оброблення на етапі навчання. Тому перелічені у таблиці 3.1 операції пропонованого методу є необхідними для досягнення мети (підвищення швидкодії), а їх достатність буде показана під час опису засобу, який реалізує запропонований метод [141].

Таблиця 3.2 - Часова складність неспівпадаючих операцій нечіткого висновку за механізмом Мамдані та пропонованого методу

Операції нечіткого висновку за класичним механізмом Мамдані	Часова складність операцій нечіткого висновку за механізмом Мамдані	Операції нечіткого висновку пропонованого методу	Часова складність операцій нечіткого висновку пропонованого методу
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	$O(n)$

На етапі навчання засобу реалізації пропонованого методу оброблення нечітких даних, відповідно до областей функцій належностей входів та вхідних даних (продуктивності – p, стійкості до часового аналізу – r та допустимих затрат пам’яті – m), однозначно визначаються області функцій належності виходу (тобто відповідних до цих функцій належності виходу методів модулярного експоненціювання) згідно бази правил нечіткого висновку Мамдані. Отримані значення, які відповідають ординатам визначених функцій належності виходу, записуються у відповідних областях багатоканального блоку пам’яті.

На етапі експлуатації засобу (рисунок 3.12), коли задані значення вхідних даних, опрацьовуються лише ті області функцій належності виходу, які відповідають записаним областям функцій належностей входів згідно бази правил нечіткого висновку.

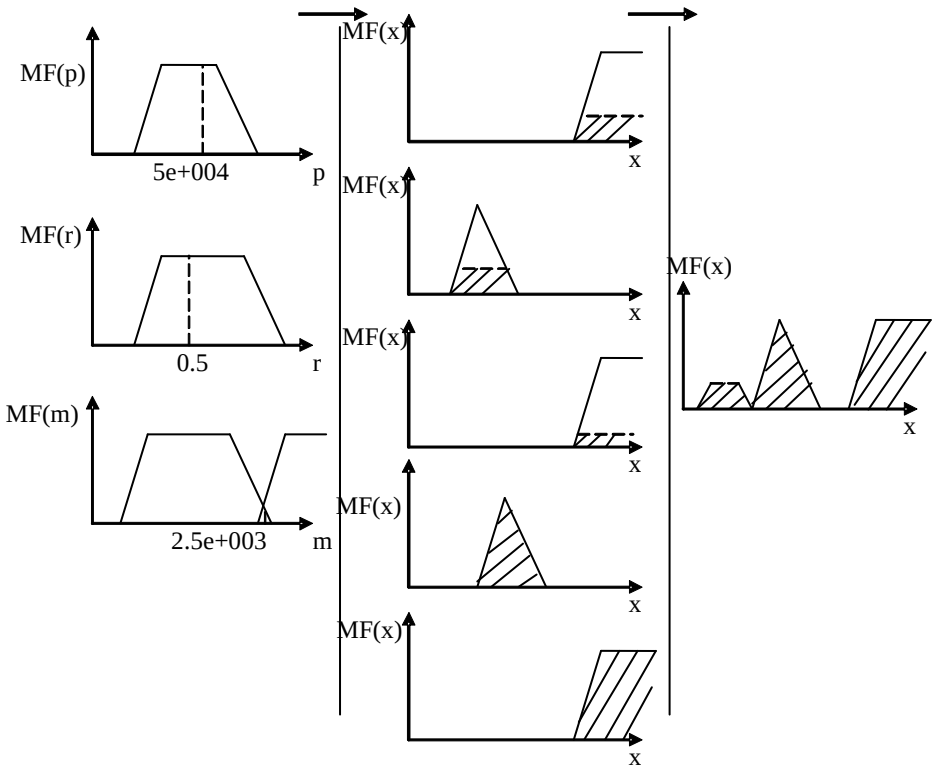


Рисунок 3.12 - Реалізація пропонованого методу нечіткого висновку під час експлуатації

На рисунку 3.13 подано ці області, встановлені в процесі дослідження бази правил нечіткої системи, засобами MATLAB 7.7.0 (R2008b) [131, 141].

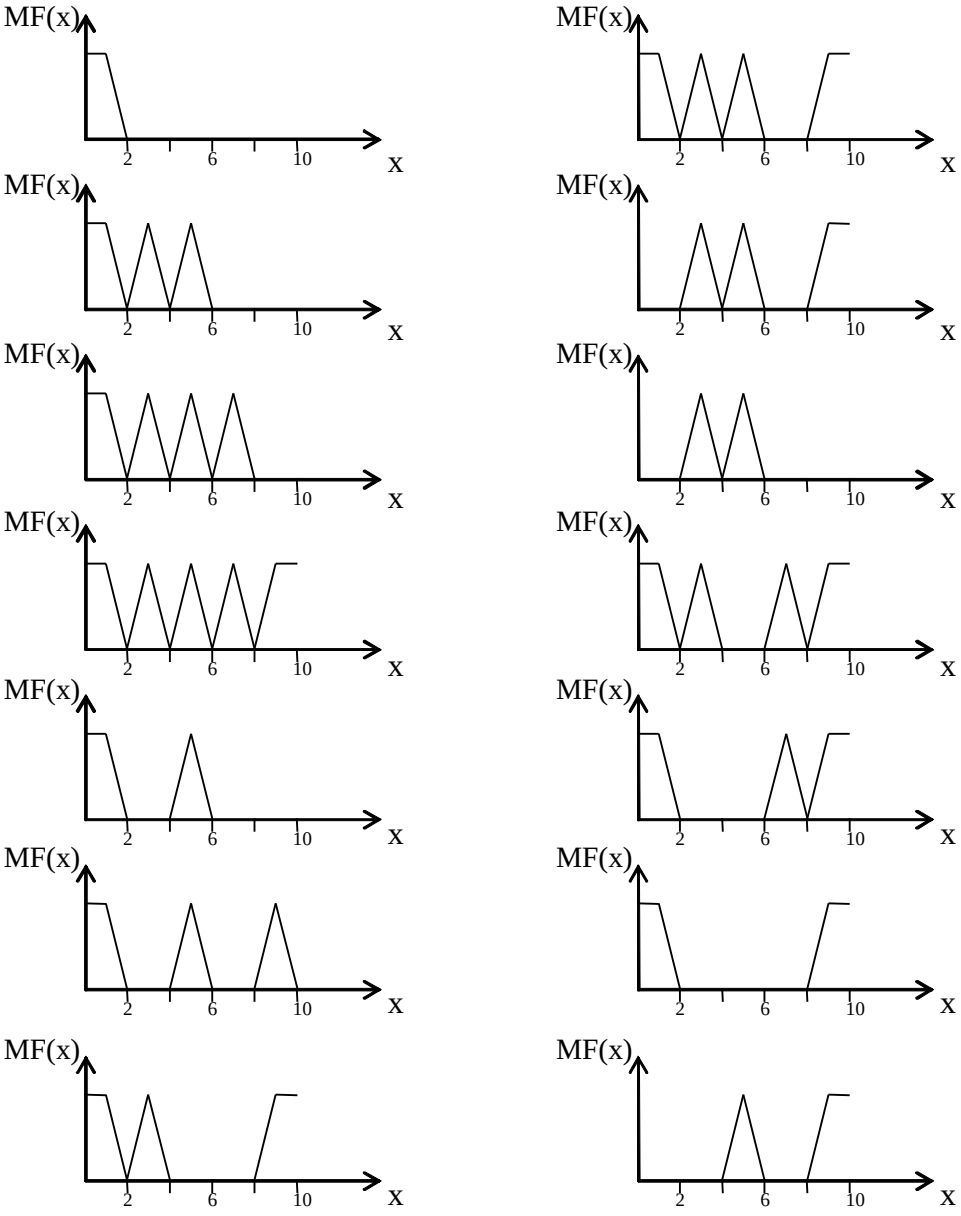


Рисунок 3.13 - Області функцій належності виходу запропонованого методу оброблення нечітких даних

Аналіз рисунку 3.13 показує, що кількість областей рівна 14, тобто зменшилась в 4,5 рази, порівняно з базою 63 правил, що використовується в класичній нечіткій системі на основі механізму Мамдані. Це, в свою чергу, прискорює процес опрацювання нечіткої інформації. При цьому області

виходу пропонованої нечіткої системи повністю відображають області виходу за класичним механізмом нечіткого висновку Мамдані, що підтверджує достатність операцій, поданих в таблиці 3.1.

Таким чином, запропонований в даному підрозділі метод оброблення нечітких даних для налаштування сервера комп'ютерної системи забезпечує його вищу швидкодію, ніж класичний механізм нечіткого висновку Мамдані.

3.4 Моделювання та дослідження засобу розподілу доступу в комп'ютерній системі на основі нечіткої логіки

Побудову моделі засобу оптимального вибору методу піднесення до степеня за модулем для забезпечення стійкості сервера комп'ютерної системи можна здійснити засобами Simulink. Дана модель нечіткого висновку за класичним механізмом Мамдані, описаним у 3.2, подана на рисунку 3.14 [142].

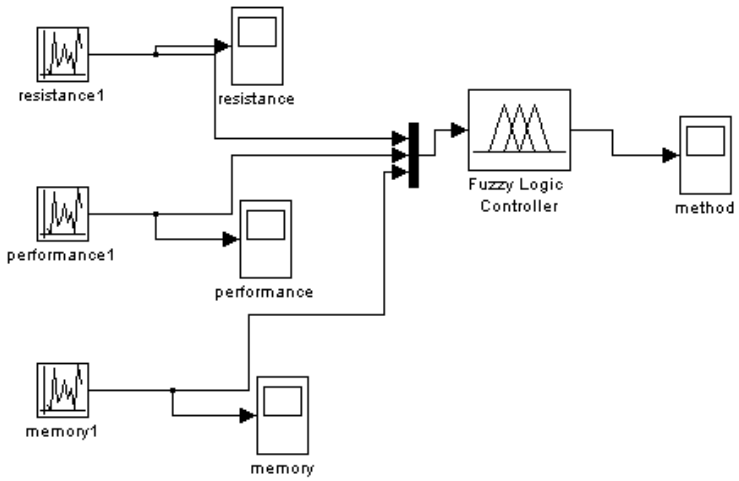


Рисунок 3.14 - Модель розробленого засобу

Входами нечіткого контролера (Fuzzy Logic Controller), який працює за механізмом Мамдані є значення стійкості (resistance), продуктивності (performance) та затрат пам'яті (memory), а виходом – значення центра ваги,

описаного в табл.3.1, який інтерпретує метод модулярного експоненціювання (method) (рисунок 3.15). Загальна схема нечіткого контролера 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).

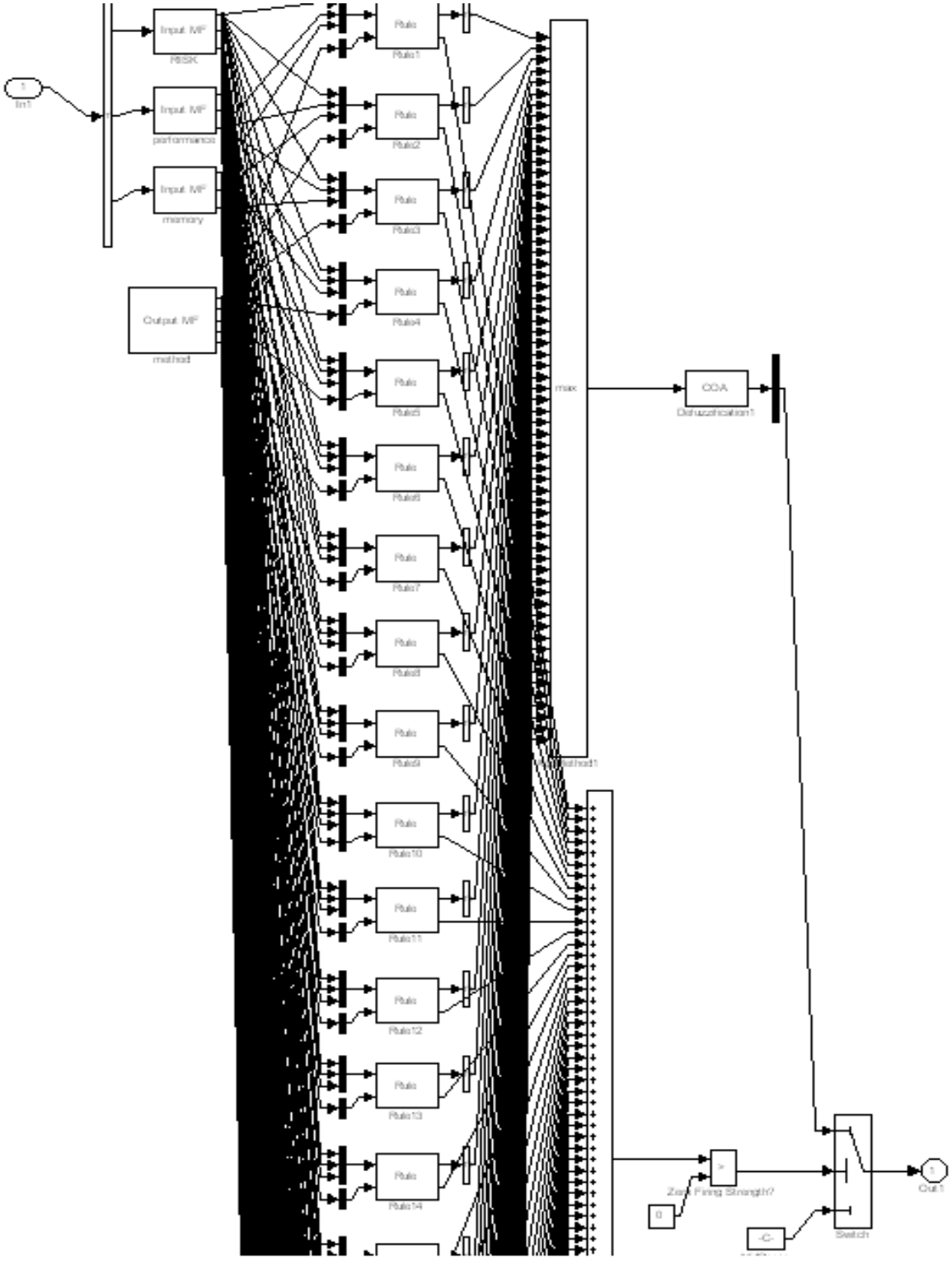
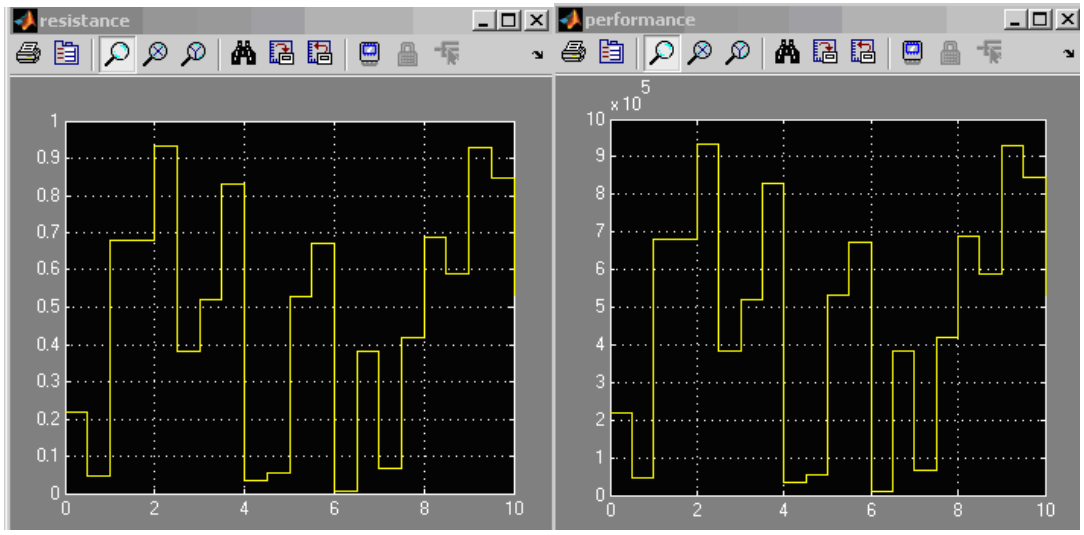
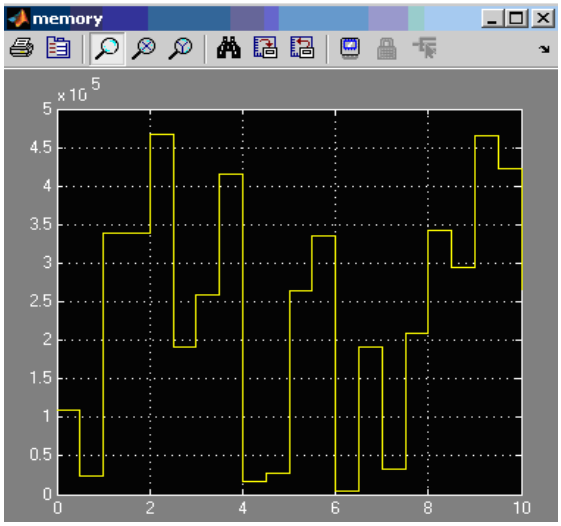


Рисунок 3.15 - Фрагмент схеми розробленого нечіткого контролера

Вхідні змінні задаються випадковим чином з рівномірним розподілом, що зображено на рисунку 3.16.



а) б)



в)

Рисунок 3.16 - Рівномірно розподілене задання випадкових значень вхідних змінних: а) стійкості; б) продуктивності; в) затрат пам’яті

Схема обчислення функцій належності вхідних та вихідної змінних, побудована системою Simulink, подано на рисунку 3.17.

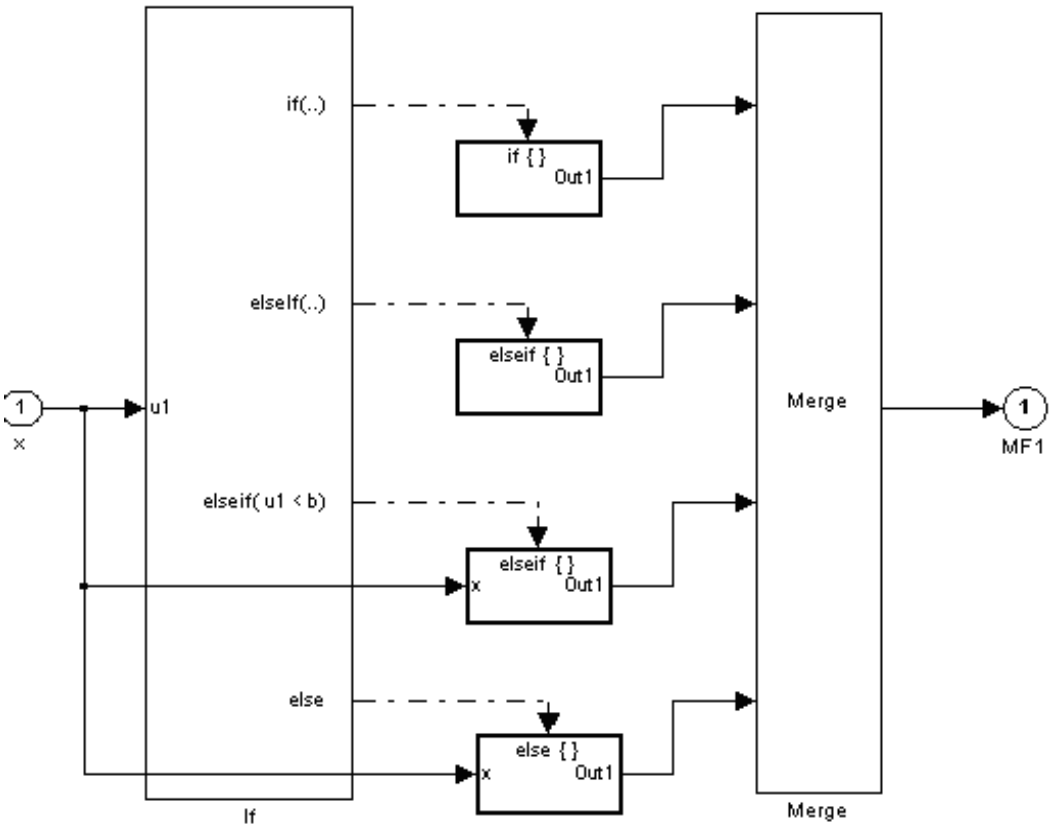


Рисунок 3.17 - Схема визначення функцій належності вхідних і вихідної змінних нечіткого контролера

Опрацювання нечітких змінних та побудова кінцевої фігури для знаходження центру ваги, що є нечітким висновком за механізмом Мамдані, здійснюється за схемою, поданою на рисунку 3.8. Simulink опрацьовує правила з бази знань, враховуючи рейтинг, що відображається константою Weight на рисунку 3.18. Входами правила є значення вхідних змінних стійкості, продуктивності та затрат пам’яті (вхід 1) та відповідне їм значення методу модулярного експоненціювання (вхід 2). Опрацювання цих даних відбувається за мінімальним законом (блок min). Виходами даної схеми є значення функції належності виходу *method* (вихід 1) та послідовність, що відображає інтервал задання цього виходу (вихід 2).

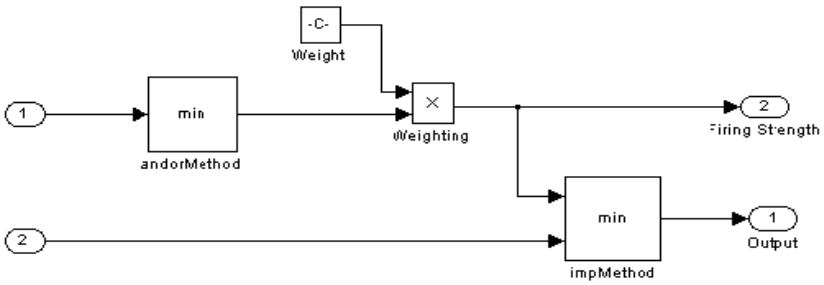


Рисунок 3.18 - Схема опрацювання вхідних нечітких значень за правилом типу «якщо - то»

Для здійснення висновку за механізмом Мамдані нечіткий контролер здійснює дефазифікацію, тобто знаходження центру ваги кінцевої фігури, що утворюється в результаті сумування виходів 63 правил. Схема дефазифікації, подана на рисунку 3.19, реалізує формулу [131]:

$$r_{öâ} = \frac{\sum_{j=1}^{m} r_j \mu(r_j)}{\sum_{j=1}^{m} \mu(r_j)}, \qquad (3.4)$$

де m - кількість прямокутників, на які поділено кінцеву фігуру,

r_j - значення абсциси,

$\mu(r_j)$ - значення ординати j-ї фігури.

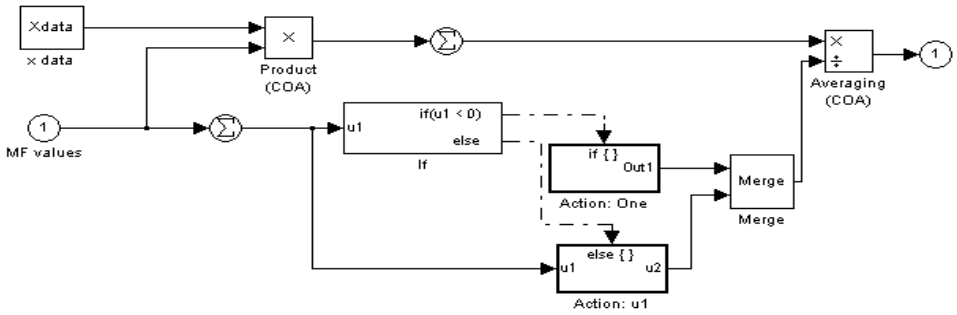


Рисунок 3.19 - Схема дефазифікації нечіткого висновку

Результат роботи моделі при заданні вхідних значень стійкості до часової атаки, продуктивності та допустимих затрат пам’яті системи з

одинаковим розподілом (див. рисунку 3.16), тобто значення центра ваги, зображено на рисунку 3.20.

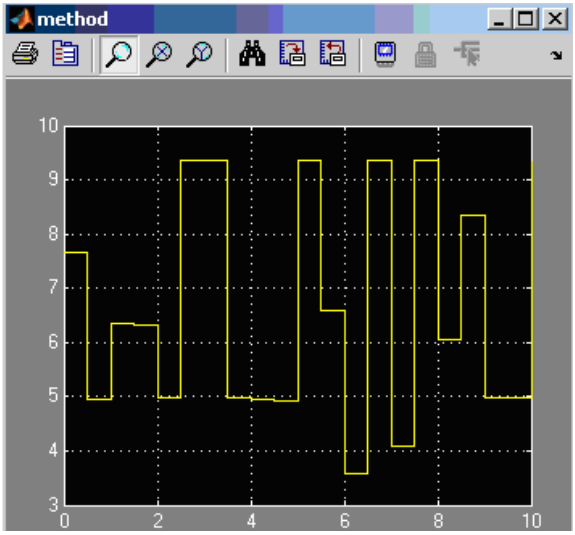


Рисунок 3.20 - Результати роботи розробленої нечіткої моделі

У таблиці 3.3 подано тестові значення вхідних та вихідних значень нечіткої системи вибору оптимального методу модулярного експоненціювання за механізмом Мамдані.

Таблиця 3.3 - Тестові значення змінних нечіткої системи вибору методу модулярного експоненціювання, побудованої за механізмом Мамдані

№п\п	Resistance	Performance	Memory	Method
1	0.0452	1.68e+004	6.65e+003	3.59
2	0.0771	4.55e+004	9.31e+003	5.26
3	0.0239	6.2e+004	1.5e+005	4.79
4	0.104	3.64e+004	3.26e+005	7.27
5	0.157	7.85e+004	1.2e+004	3.88
6	0.604	6.3e+004	2.22e+005	6.27
7	0.96	9.49e+004	1.93e+005	2.43
8	0.0133	7.15e+004	3.99e+003	1.66
9	0.168	3.11e+004	3.5e+005	8.36
10	0.0452	2.95e+004	3.32e+004	2.6

Перевірка роботи побудованого засобу розподілу доступу за класичним механізмом нечіткого висновку Мамдані здійснено за допомогою стандартних тестів середовища Simulink (додаток Д).

Для побудови схеми нечіткого контролера, що реалізує нечіткий висновок за розробленим методом, варто використати схему задання функцій належності, подану на рисунку 3.17, та визначення центра ваги згідно формули (3.4). Схема розробленого нечіткого контролера, що реалізує пропонований метод оброблення нечіткої інформації, подана на рисунку 3.21.

Для задання областей функцій належності виходу, поданих на рисунку 3.13, використано додавання відповідних кожному з методів модулярного експоненціювання інтервалів, що інтерпретуються змінними $x1 \ldots x5$ ($x1 = [0,2]$ 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»).

Згідно схеми рисунку 3.21 спочатку здійснюється обчислення функцій належності вхідних змінних за допомогою блоків «if» та «function» середовища Simulink. Для кожної області з рисунку 3.13 знаходяться мінімальні серед відповідних значень вхідних змінних, що реалізовано в схемі рисунку 3.21. Кінцева фігура описується абсцисами, що задаються з об’єднання виходів відповідних блоків «From Workspace», та ординатами, що відповідають виходам опрацювання функцій належності входів. Центр ваги отриманої фігури обчислюється аналогічно до схеми рисунку 3.19.

Лістинг роботи побудованого засобу оброблення нечітких даних за запропонованим методом, розроблений засобами MATLAB, поданий в додатку Е.

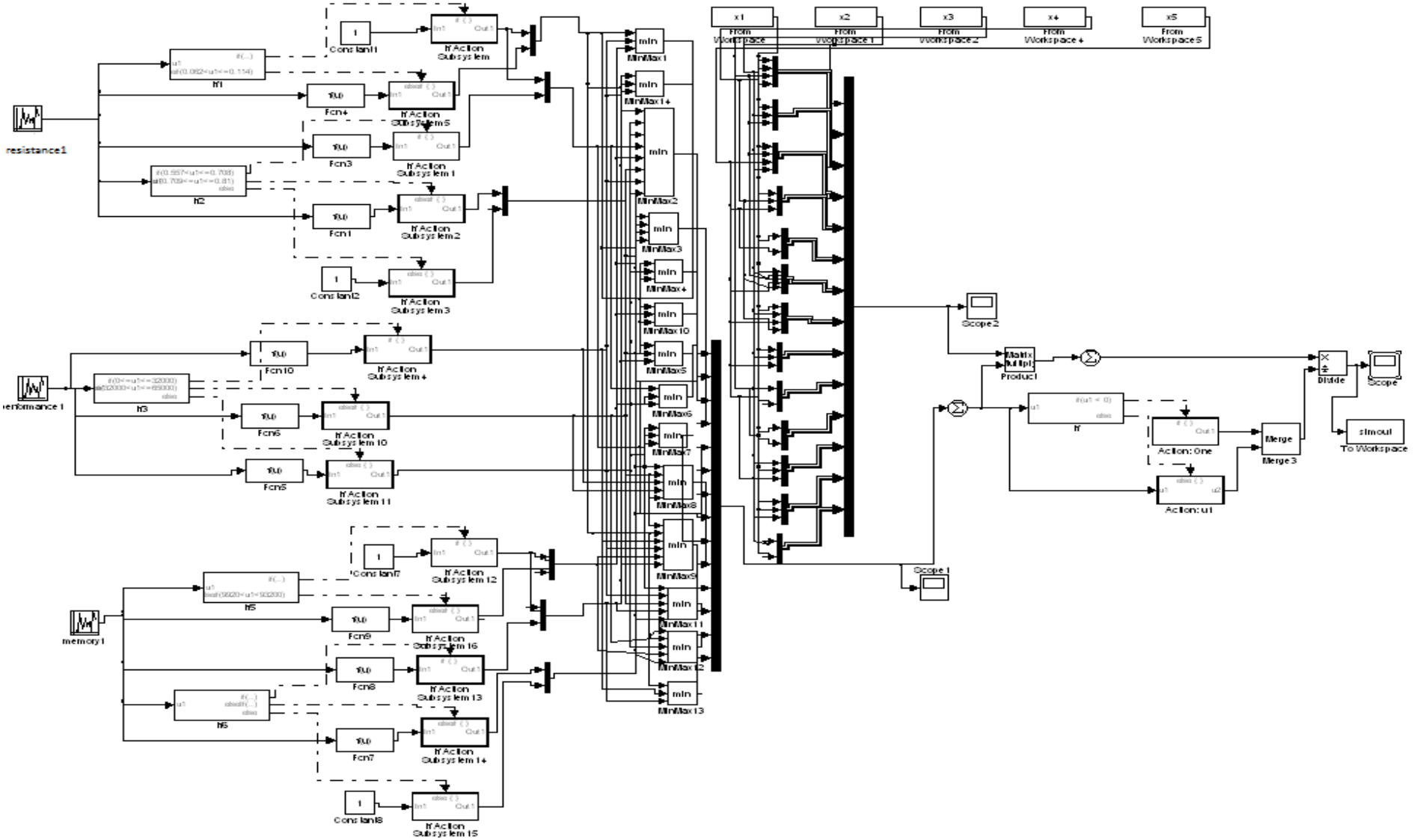


Рисунок 3.21 - Схема розробленого нечіткого контролера

Тестові значення перевірки роботи схеми рисунку 3.21 подано в таблиці 3.4.

Таблиця 3.4 - Тестові значення змінних розробленої нечіткої системи вибору методу модулярного експоненціювання.

№п\п	Resistance	Performance	Memory	Method
1	0.0452	1.68e+004	6.65e+003	3.64
2	0.0771	4.55e+004	9.31e+003	5.2
3	0.0239	6.2e+004	1.5e+005	4.81
4	0.104	3.64e+004	3.26e+005	7.25
5	0.157	7.85e+004	1.2e+004	3.91
6	0.604	6.3e+004	2.22e+005	6.4
7	0.96	9.49e+004	1.93e+005	1.93
8	0.0133	7.15e+004	3.99e+003	1.69
9	0.168	3.11e+004	3.5e+005	8.31
10	0.0452	2.95e+004	3.32e+004	2.65

Таким чином, аналіз таблиць 3.3 та 3.4 показує, що середнє відхилення результату роботи схеми рисунку 3.21 від значення виходу нечіткого контролера за механізмом Мамдані становить мінімально 0,02 та 0,13 максимально, тобто в середньому 0,055, що підтверджує працездатність системи і правильність результатів.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Для оптимальної роботи та швидкої реконфігурації сервера, відповідно до поточних вимог комп'ютерної системи щодо стійкості до часового аналізу, продуктивності та затрат пам'яті, застосовано механізм нечіткої логіки Мамдані, що працює за min-max законом.

2. Розроблено метод оптимального вибору алгоритму модулярного експоненціювання, що базується на класичному механізмі нечіткого висновку Мамдані та методі визначення нормованої стійкості алгоритму до часового аналізу. База правил нечіткого контролера, що працює за методом оптимального вибору алгоритму модулярного експоненціювання, складається з 63 правил.

3. Запропоновано метод оброблення нечітких даних для налаштування сервера, який базується на поділі процесу оброблення нечіткої інформації на етапи навчання та експлуатації, що дало змогу зменшити кількість вихідних областей до 14 і, відповідно, кількість операцій у 4,5 рази, що зменшує час реагування системи захисту інформації в 4 рази.

4. Моделювання та дослідження засобу оброблення нечітких даних, проведені в середовищі Simulink, показали, що відхилення результатів його роботи від роботи нечіткого контролера, базованого на класичному механізмі Мамдані, становить 0,055, що підтверджує правильність його роботи та можливість застосовування для налаштування сервера комп'ютерної системи з метою розподілу доступу до інформації.

РОЗДІЛ 4

ЗАСІБ РОЗПОДІЛУ ДОСТУПУ В КОМП'ЮТЕРНИХ СИСТЕМАХ

4.1 Структурна схема засобу вибору методу модулярного експоненціювання

Як зазначалося вище, на сучасному етапі для захисту інформації використовуються, як правило, асиметричні криптоалгоритми, основною операцією в яких є модулярне експоненціювання. Вибір методу модулярного експоненціювання залежно від значень продуктивності, стійкості до часового аналізу та допустимих затрат пам’яті в описаних умовах невизначеності доцільно реалізувати з допомогою запропонованого в третьому розділі методу обробки нечіткої інформації. Однак, хоча програмна реалізація запропонованого методу, наприклад, на мові С, має відносно невелику обчислювальну та часову складність, все - таки виконання її сервером мережі знижує його продуктивність. Крім того, при програмній реалізації існує ймовірність блокування підсистеми вибору методу модулярного експоненціювання при цілеспрямованій дії комп’ютерного вірусу. При цьому можливе як повне блокування цієї підсистеми (що веде до непрацездатності сервера, а тому відносно легко виявляється), так і цілеспрямований вибір такого методу модулярного експоненціювання, що, для підвищення ефективності атаки, забезпечує мінімальний і незмінний захист (що не веде до непрацездатності сервера, а тому таку дію важко виявити). Тому доцільна апаратна реалізація запропонованого методу.

Засіб вибору методу модулярного експоненціювання на основі нечіткої логіки повинен виконувати наступні функції:

1. Приймати від сервера попередньо оброблені згідно методу обробки нечітких даних, запропонованого в третьому розділі, відповідні функції належності виходу для кожного з правил нечіткого висновку.

2. Приймати від сервера задані поточні значення продуктивності, стійкості до атак та допустимих затрат пам’яті відповідно до оціненої імовірності атаки по поточному каналу.

3. Обчислювати відповідний центр ваги остаточної фігури функцій належності виходу.

4. Приймати від сервера сигнал запуску обчислення центра ваги та подавати на сервер сигнал кінця обчислення.

Обчислення центру ваги можна реалізувати, припустивши, що функції належності представляють собою плоску фігуру однакової товщини. Тоді центр ваги визначається всього двома координатами, а радіус-вектор центра ваги під час обробки нечіткої інформації можна обчислити за формулою [119]

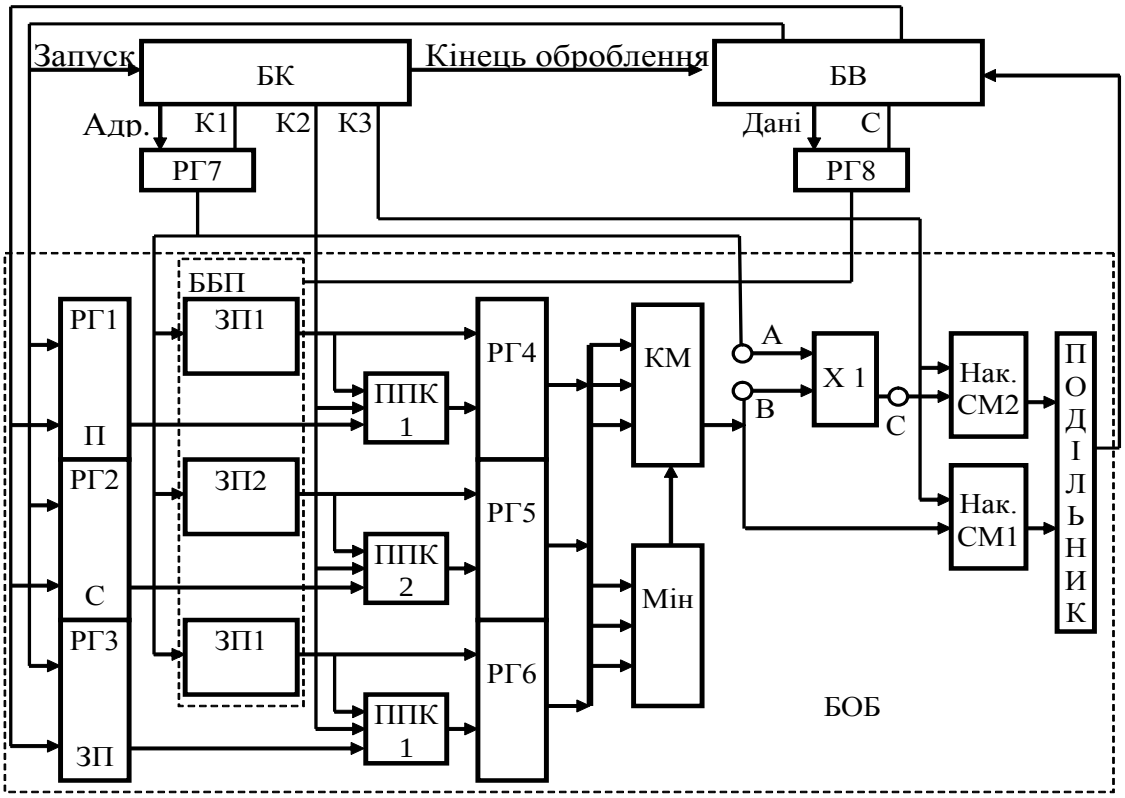
$$r_{цв} = \frac{\sum r_i m_i}{\sum m_i} \quad , \tag{4.1}$$

де $r_{цв}$ – координата центра ваги;

r_i – координата центра ваги i-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти;

m_i – маса i-того прямокутника, з яких складається фігура, центр ваги якої необхідно знайти.

Відповідно до сформованих вимог синтезовано структурну схему пропонованого засобу (рисунок 4.1), що визначає центр ваги фігури, побудованої за правилами Мамдані на основі функцій належності входу. Цей центр ваги, в свою чергу, визначає метод модулярного експоненціювання,



який має використовувати обчислювальна система (сервер) для обміну інформацією по даному каналу передачі даних. Ця обчислювальна система, яка реалізує захист інформації з допомогою деякого методу модулярного експоненціювання, позначена як блок використання результатів обробки нечітких даних БВ. Перед роботою БВ записує у багатоканальний блок пам'яті ББП значення попередньо оброблених (відповідно до методу обробки нечітких даних, розробленого в третьому розділі) функцій належності входу. Для цього блок керування БК формує відповідні адреси, а самі значення функцій належності входу поступають на регістр пам'яті РГ8.

Рисунок 4.1 - Структурна схема засобу вибору методу модулярного експоненціювання на основі методу обробки нечітких даних

При цьому набір значень функцій належності входу, що відповідають продуктивності, записується у запам’ятовуючий пристрій ЗП1, набір значень функцій належності входу, що відповідають стійкості до атак, записується у запам’ятовуючий пристрій ЗП2, а набір значень функцій належності входу, що відповідають допустимому об’єму пам’яті, записується у запам’ятовуючий пристрій ЗП3. Як ЗП1…ЗП3 можна використати оперативний запам’ятовуючий пристрій. Його недоліком є можливість збоїв під час експлуатації за рахунок дії впливаючих факторів, наприклад, перепадів напруги живлення (природних або штучно створених). Тому доцільно в якості ЗП1…ЗП3 використати Flash–пам’ять, стійку до збоїв по напрузі живлення.

При виникненні потреби визначення методу модулярного експоненціювання, що повинен використовуватися при взаємодії з визначеним клієнтом, БВ задає його параметри (визначені згідно методу визначення нормованої стійкості та методу оптимального вибору алгоритму модулярного експоненціювання, розроблених в другому та третьому розділах) – значення необхідної продуктивності, стійкості до атак та допустимого об’єму пам’яті, який може використати даний канал. Ці параметри поступають на регістри пам’яті РГ1…РГ3 і записуються в них сигналом “запуск”, який теж формується БВ. Сигнал “запуск” також запускає блок керування БК, який формує алгоритм роботи засобу вибору методу модулярного експоненціювання.

Згідно цього алгоритму БК спочатку записує сигналом К1 в регістр пам’яті РГ7 початкову адресу набору значень функцій належності входу. Відповідно до цієї адреси на пристрої порівняння кодів ППК1…ППК3 поступають коди поточного значення функцій належності виходу (поступають із ЗП1…ЗП3) та їх допустимі значення (поступають із РГ1…РГ3). За сигналом К2 спрацьовують пристрої порівняння кодів ППК1…ППК3. Якщо деякі із значень, що поступають з РГ1 … РГ3, більші за відповідні значення, що поступають із ЗП1 … ЗП3, то останні записуються у

регістри РГ4 … РГ6. Якщо якісь із значень, що поступають з РГ1 … РГ3, менші за відповідні значення, що поступають із ЗП1 … ЗП3, то запис у регістри РГ4 … РГ6 не проводиться, в них залишаються значення, які були не більші за значення, що поступають з РГ1 … РГ3. Далі, згідно механізму нечіткого висновку Мамдані, вузол вибору мінімального значення Мін вибирає мінімальне значення функції належності входу із значень, записаних в РГ1 … РГ3, і, адресуючи відповідним чином комутатор КМ, подає це значення на входи перемножувача Х1 та накопичуючого суматора Нак. СМ1. Мінімальне значення функції належності входу із значень, записаних в РГ1…РГ3, відповідає масі поточного прямокутника m_i у формулі (4.1). А добуток адреси на мінімальне значення з регістрів РГ1…РГ3, отриманий на виході перемножувача Х1, відповідає добутку $r_i m_i$ у чисельнику цієї формули. Сумування згідно чисельника та знаменника формули (4.1) відбувається в накопичуючих суматорах Нак. СМ2 і Нак. СМ1 відповідно. Значення координати центра ваги, отриманої в результаті виконання механізму нечіткого висновку Мамдані, згідно (4.1) отримуємо шляхом ділення блоком ПОДІЛЬНИК. Це значення поступає на блок використання БВ, де порівнюється із значеннями функцій належності виходу, які характеризують доступні в даній комп'ютерній системі методи модулярного експоненціювання. Так визначається метод модулярного експоненціювання, що відповідає даному клієнту комп'ютерної системи.

Слід відзначити, що в представленій на рисунку 4.1 структурній схемі обчислення довжини векторів r_i реалізовано за спрощеним методом – до уваги береться лише абсциса поточної точки, а ордината ігнорується. Геометрична інтерпретація методу обчислення довжини векторів r_i структурною схемою рисунку 4.1 представлено на рисунку 4.2. Таке спрощення суттєво зменшує час визначення координати центра ваги. Методичною похибкою визначення координати центра ваги, що виникає при цьому, в більшості випадків можна нехтувати через те, що функції виходу визначено теж як нечіткі дані. Крім того, зазвичай, кількість доступних в

даній комп'ютерній системі методів захисту інформації, зокрема, методів модулярного експоненціювання, є невеликою – 5…7 методів. Тому значенням методичної похибки 2…3% можна нехтувати. Більша методична похибка виникає, коли значення функцій належності входу мають значні перепади – тоді ігнорування ординати довжини векторів r_i може привести до збільшення методичної похибки в декілька разів.

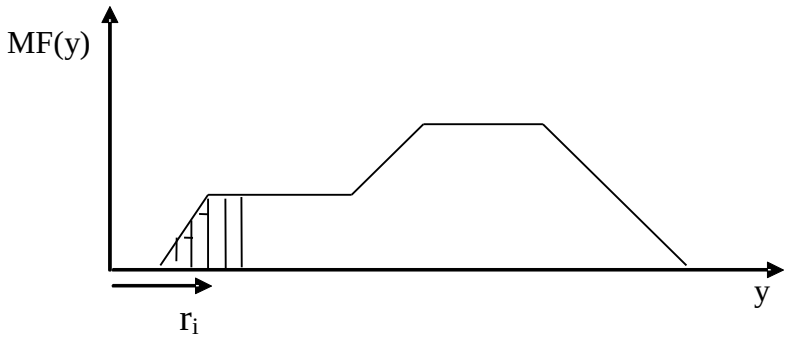


Рисунок 4.2 - Пошук центра ваги фігури без врахування ординати векторів r_i

Для усунення методичної похибки при обчисленні довжини векторів r_i запропоновано в структурну схему рисунку 4.1, замість перемножувача X1, ввести вузол, структурна схема якого представлена на рисунку 4.3. Він складається з подільника на 2, перемножувачів X1 та X2, суматора СМ3 та блоку добування квадратного кореня БДКК. Вузол підключають в схему рисунку 4.1 шинами A, B, C відповідно позначень на рисунках 4.1, 4.3. Цей вузол визначає довжину векторів r_i за теоремою Піфагора, згідно рисунку 4.4.

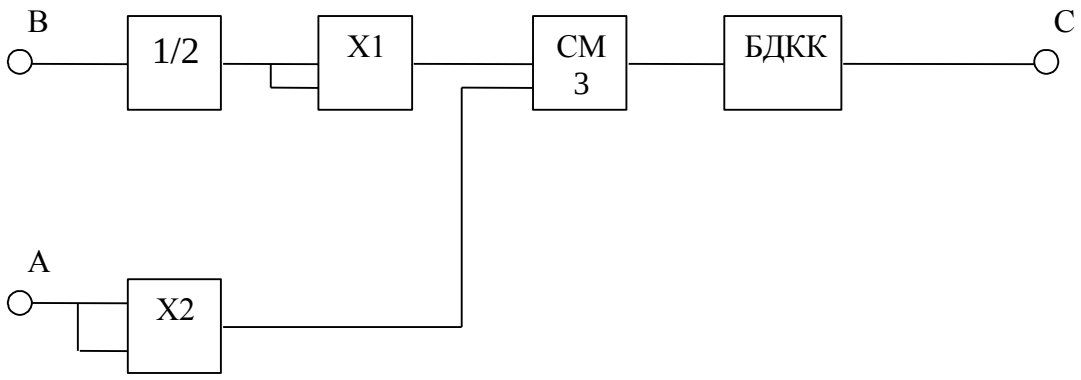


Рисунок 4.3 - Вузол підвищення точності знаходження центру ваги при обробці нечіткої інформації

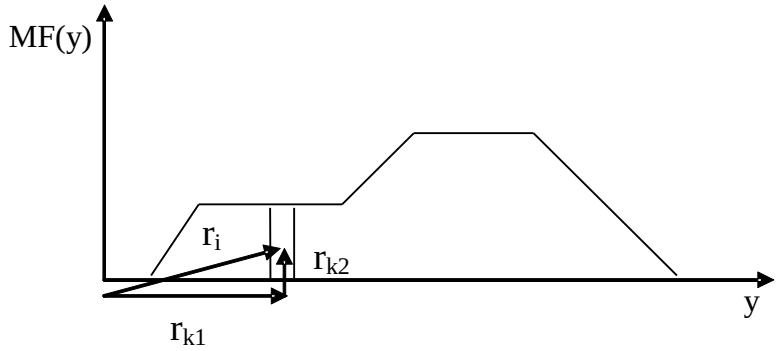


Рисунок 4.4 - Пошук центра ваги фігури з врахуванням його ординати

Синхронізує роботу засобу вибору методу модулярного експоненціювання блок керування БК, який може бути виконаний за різними схемами. Найбільшу регулярність структури (що важливо при виконанні БК на базі програмованих логічних інтегральних схем) та функціональну гнучкість має БК на базі лічильника імпульсів [152]. Його структурну схему представлено на рисунку 4.5.

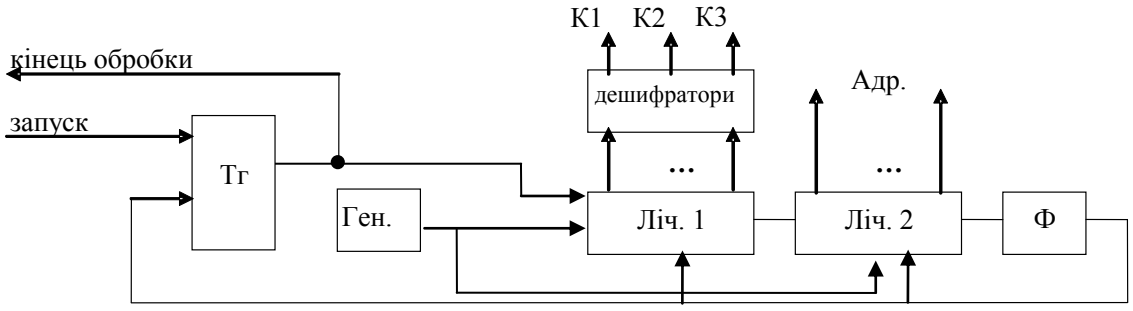


Рисунок 4.5 - Структурна схема блоку керування

Він включає тригер запуску Тг, генератор тактової частоти Ген., послідовно ввімкнені лічильники Ліч.1 і Ліч.2, а також формувач імпульсів Ф. БК починає роботу при поступленні на вхід Тг імпульсу запуску від блоку використання результатів обробки нечітких даних БВ (див. рисунок 4.1). Тригер Тг (див. рисунок 4.5) перемикається і дозволяє роботу лічильника Ліч.1. Дешифратори, підключені до Ліч.1, формують сигнали керування К1…К3 таким чином, щоб відповідні вузли блоку обробки нечітких даних БОБ встигали виконувати свої функції. Сигнал керування К1 не повинен мати затримку відносно сигналу запуску, він може бути сформований одразу при поступленні на Ліч.1 першого імпульсу генератора Ген. Необхідна тривалість К1 визначається мінімальним часом запису коду адреси з лічильника Ліч.2 в регістр РГ7 (див. рисунок 4.1). Передній фронт сигналу керування К2 повинен мати затримку відносно закінчення дії сигналу К1 на час вибірки значень із ЗП1…ЗП3, що досягається відповідним підключенням входів його дешифратора (див. рисунок 4.5). Тривалість К2 повинна бути достатньою для спрацювання пристроїв порівняння кодів ППК1…ППК3 (див. рисунок 4.1) та запису даних в регістри РГ4…РГ6. Передній фронт сигналу керування К3 повинен мати затримку відносно закінчення дії сигналу К2 на час пошуку мінімального значення блоком Мін., передачі цих значень комутатором КМ та перемноження їх на адресу перемножувачем Х1, тобто затримка К3 відносно К2 визначається не тільки використаною елементною базою, а й структурами перелічених вузлів, причому набагато перевищує затримку К2 відносно К1. Власне ця обставина була визначальною при виборі структури блоку керування, згідно [153] блоки керування на лічильниках імпульсів легко забезпечують формування імпульсів різної тривалості та нерівномірно розташованих в часі. Тривалість К3 повинна бути достатньою для спрацювання накопичуючих суматорів Нак.СМ1 та Нак.СМ2.

Перехід імпульсу на лічильник Ліч.2 (див. рисунок 4.5) змінює код адреси і описаний процес оброблення нечітких даних повторюється. При цьому час від закінчення імпульсу К3 до зміни коду повинен забезпечити спрацювання накопичуючих суматорів Нак.СМ1 та Нак.СМ2, а також подільника (див. рисунок 4.1).

Після перебору всіх адрес з виходу лічильника Ліч.2 (див. рисунок 4.5) на формувач Ф поступає фронт імпульсу, який викликає його спрацювання. Тоді Ф формує короткий імпульс перекидання тригера Тг – в результаті з виходу Тг на блок використання результатів обробки нечітких даних БВ (див. рисунок 4.1) поступає сигнал кінець обробки, який повідомляє БВ про наявність на виході ПОДІЛЬНИКА координати центра ваги, згідно якого слід вибирати метод модулярного експоненціювання. Крім того, вихідний імпульс формувача Ф поступає на входи скидання лічильників Ліч.1 та Ліч.2, готуючи їх до наступного циклу обробки нечітких даних.

Таким чином, в даному підрозділі розроблено структурну схему засобу вибору методу модулярного експоненціювання на основі розробленого в третьому розділі методу обробки нечітких даних, який забезпечує знаходження центру ваги для функції належності виходу. Також розроблено структурну схему модифікації цього засобу, яка забезпечує вищу точність знаходження центру ваги та структурну схему блока керування розробленим засобом.

4.2 Дослідження швидкодії засобу вибору методу модулярного експоненціювання

Для дослідження параметрів засобу вибору методу модулярного експоненціювання необхідно розробити принципові схеми нестандартних вузлів, що входять в його структурну схему. Через те, що час реакції сервера

обмежується часом оброблення нечітких даних засобом вибору методу модулярного експоненціювання, цей час є найважливішим параметром засобу, саме він визначає можливість роботи системи захисту (див. рисунок 3.3) в реальному часі, без затримок. Тому вибираємо схемотехнічні рішення, які забезпечують максимальну швидкодію вузлів засобу вибору методу модулярного експоненціювання.

Першими з таких вузлів є пристрої порівняння кодів ППК1…ППК3. Принципова схема вузла ППК представлена на рисунку 4.6. Вона базується на схемах XOR та NO-AND і видає лог. нуль, коли вихідний код ЗП1…ЗП3 більший або рівний вихідному коду РГ1…РГ3. Якщо вихідний код ЗП1…ЗП3 менший від вихідного коду РГ1…РГ3, то на вихід поступає лог. одиниця. Ця схема має затримку τ_{PPK}, яка відповідає трьом спрацюванням логічних елементів τ_{LE}, тобто $\tau_{PPK} = 3\tau_{LE}$. Перевірка роботи схеми на симуляторі Electronics Workbench показала співпадання обчисленого часу з очікуваними результатами.

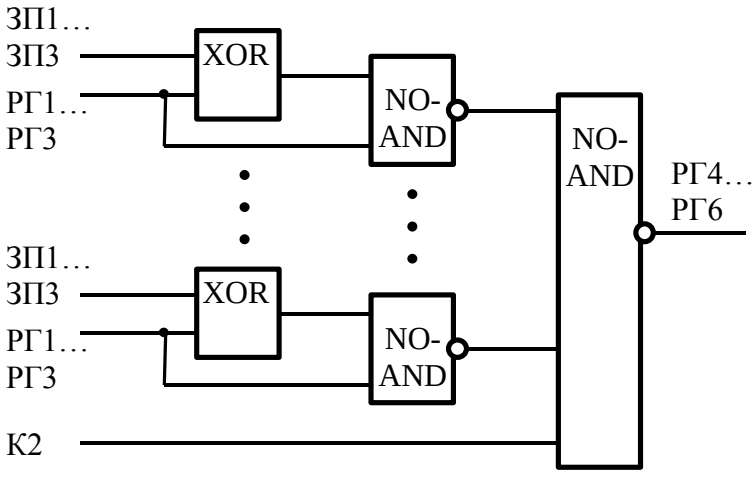


Рисунок 4.6 - Принципова схема вузла порівняння кодів ППК1…ППК3

Ще одним нестандартним вузлом є вузол вибору мінімального значення Мін, представлений на рисунку 4.7. Він базується на попередній схемі вузла порівняння кодів, дешифраторі DC і логічних елементах OR. Вузол вибору мінімального значення Мін порівнює між собою коди в

регістрах РГ4…РГ6 і видає для комутатора КМ порядковий код номера того регістра, в якому знаходиться мінімальне значення коду. Ця схема має затримку τ_{Min}, яка відповідає чотирьом спрацюванням логічних елементів τ_{LE} та часу спрацювання дешифратора τ_{DC}, який відповідає часу спрацювання трьох логічних елементів τ_{LE}, тобто сумарний час спрацювання буде $\tau_{Min} = 7\tau_{LE}$. Перевірка роботи схеми на симуляторі Electronic Workbench показала співпадання обчисленого часу з очікуваними результатами.

Перемножувач X1 та ПОДІЛЬНИК, для підвищення швидкодії розробленого засобу вибору методу модулярного експоненціювання, доцільно виконати на постійних запам'ятовуючих пристроях ПЗП, працюючих постійно в режимі читання. На входи адреси ПЗП поступають співмножники (для ПОДІЛЬНИКА – ділене і дільник відповідно), а в комірках записано значення відповідних добутків (для ПОДІЛЬНИКА – часток). В такому випадку час отримання добутку є найменшим, він визначається лише часом читання ПЗП.

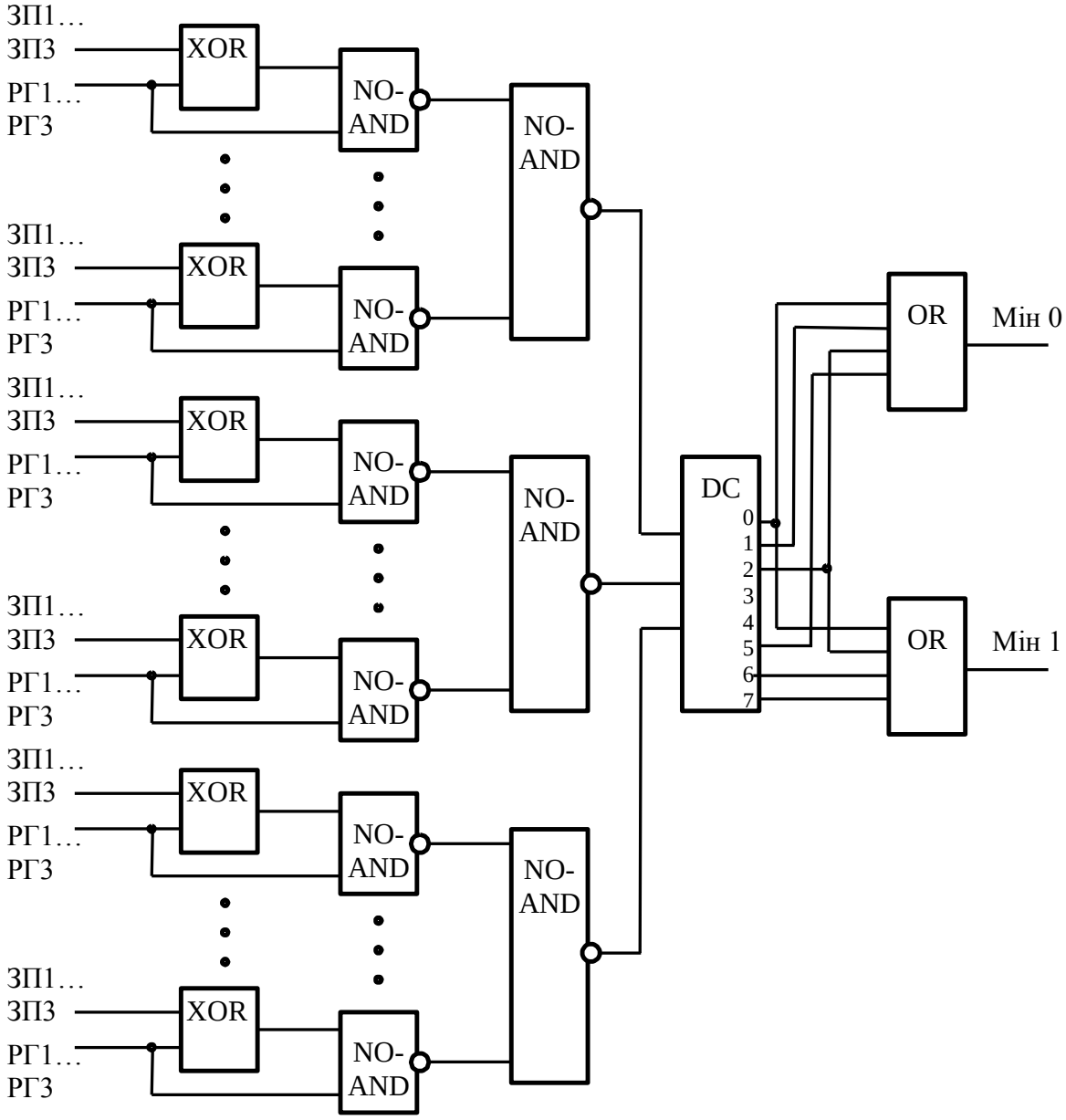


Рисунок 4.7 - Принципова схема вузла вибору мінімального значення Мін

Наступними нестандартними вузлами є вузли накопичуючих суматорів Нак.СМ1 і Нак.СМ2. Час їх спрацювання теоретично не впливає на час знаходження центру ваги досліджуваним засобом через те, що наступний доданок приходить після закінчення всіх процедур вибору наступного мінімального значення коду функції належності входу із значень, записаних в ЗП1…ЗП3 та регістрах РГ1…РГ3. Однак спрацьовують накопичуючі суматори Нак.СМ1 і Нак.СМ2 протягом дії імпульсу керування К3,

тривалість якого впливає на час знаходження центру ваги. Тому, практично, час спрацювання накопичуючих суматорів Нак.СМ1 і Нак.СМ2 теж повинен бути мінімальним. Тому вибираємо схему паралельного накопичуючого суматора, яка має високу швидкодію за рахунок більшої апаратної складності. Така схема представлена на рисунку 4.8. Вона складається з 16-ти розрядних суматора СМ та регістра РГ. На молодші розряди першого входу суматора СМ поступає 8-ми розрядний код з комутатора КМ, на старші входи подано логічні нулі. Вихідний код суматора СМ поступає на 16-ти розрядний регістр РГ, де запам'ятовується по фронту сигналу керування К3. Вихідний код регістра РГ поступає на другі входи суматора СМ. Час сумування суматором СМ не впливає на час оброблення нечітких даних за рахунок того, що він входить в час оброблення даних іншими вузлами. Тому час спрацювання таких накопичуючих суматорів не перевищує часу запам'ятовування отриманої суми в регістрі РГ. Зазвичай цей час не перевищує $\tau_{RG} = 3\tau_{LE}$.

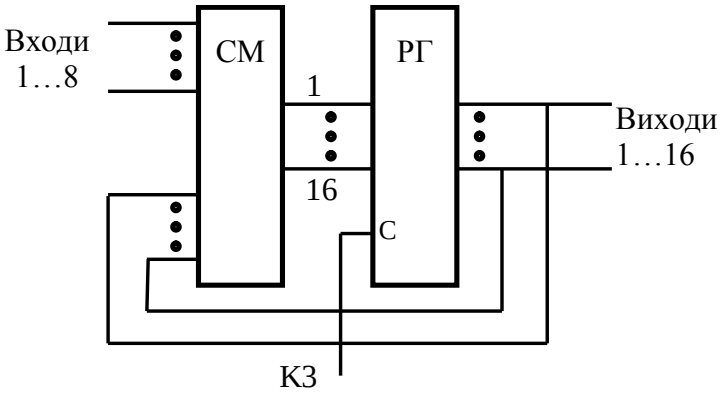


Рисунок 4.8 - Принципова схема вузлів накопичуючих суматорів Нак.СМ1 і Нак.СМ2

Розроблені схеми нестандартних вузлів дозволяють обчислити мінімальний час оброблення нечітких даних розробленим засобом, а також розробити вузол лічильника Ліч.1 блоку керування (див. рисунок 4.5) та підключеного до нього дешифратора.

Мінімальний час оброблення нечітких даних τ_{OND}, згідно найдовшого шляху по схемі рисунку 4.1 і рисунку 4.5, можна оцінити за формулою

$$\tau_{OND} = \tau_{TG} + \tau_{KL} + \tau_{LCH1} + (\tau_{DC} + \tau_{RG7} + \tau_{ZP} + \tau_{PPK} + \\ + \tau_{RG4} + \tau_{Min} + \tau_{KM} + \tau_{X1} + \tau_{NakSM1}) \cdot N + \tau_{POD}, \quad (4.2)$$

де τ_{TG} – час спрацювання тригера (див. рисунок 4.5), $\tau_{TG} = 3\tau_{LE}$;

τ_{KL} – час спрацювання ключа (див. рисунок 4.5) $\tau_{KL} = \tau_{LE}$;

τ_{LCH1} – час спрацювання лічильника Ліч.1 (див. рисунок 4.5) $\tau_{LCH1} = 3\tau_{LE}$;

τ_{DC} – час спрацювання дешифратора (див. рисунок 4.5) $\tau_{DC} = 3\tau_{LE}$;

τ_{RG7} – час спрацювання регістра РГ7 (див. рисунок 4.1) $\tau_{RG} = 3\tau_{LE}$;

τ_{ZP} – час спрацювання запам'ятовуючих пристроїв ЗП1…ЗП3 (див. рисунок 4.1) $\tau_{ZP} = 9\tau_{LE}$;

τ_{PPK} – час спрацювання пристрою порівняння кодів ППК1…ППК3 (див. рисунок 4.1) $\tau_{PPK} = 3\tau_{LE}$;

τ_{RG} – час спрацювання регістрів РГ4…РГ6 (див. рисунок 4.1) $\tau_{RG} = 3\tau_{LE}$;

τ_{Min} – час спрацювання вузла знаходження мінімального значення коду Мін (див. рисунок 4.1) $\tau_{Min} = 7\tau_{LE}$;

τ_{KM} – час спрацювання комутатора КМ (див. рисунок 4.1) $\tau_{KM} = 3\tau_{LE}$;

τ_{X1} – час спрацювання перемножувача Х1 (див. рисунок 4.1) $\tau_{X1} = 9\tau_{LE}$;

τ_{NakSM1} – час спрацювання накопичуючого суматора Нак.СМ2 (див. рисунок 4.1) $\tau_{NakSM} = 3\tau_{LE}$;

τ_{POD} – час спрацювання ПОДІЛЬНИКА (див. рисунок 4.1) $\tau_{POD} = 9\tau_{LE}$;

N – кількість комірок, які займає опис функцій належності входів, тобто роздільна здатність цих описів (згідно даних, приведених в третьому розділі, $N = 32...128$).

Згідно даних, отриманих шляхом аналізу довідкових даних та приведених у поясненнях змінних (4.2), мінімальний час обробки нечітких даних буде складати $\tau_{OND} = 59\tau_{LE}$. При реалізації засобу вибору методу модулярного експоненціювання на основі різної елементної бази отримаємо мінімальний час оброблення нечітких даних, вказаний у таблиці 4.1.

Таблиця 4.1 - Час оброблення нечітких даних залежно від елементної бази та значення $N = 32...128$

Елементна база	Час оброблення		Елементна база	Час оброблення
Стандартна ТТЛ	30,7…95 мкс		Вдосконалена ТТЛШ	11,2…34,5 мкс
ТТЛШ	16,7…51,8 мкс		Програмована логічна матриця	2,9…11,5 мкс

Як видно з таблиці 4.1, у найгіршому випадку мінімальний час оброблення нечітких даних не перевищує 100 мкс, що веде до імовірного очікування сервера, а тому неприйнятне. Однак мінімальний час оброблення нечітких даних при використанні елементів вдосконаленої ТТЛШ (Advanced Shotky TTL) [154], а тим більше програмованих логічних матриць [155], цілком прийнятний.

Таким чином, в даному підрозділі розроблено принципові схеми нестандартних вузлів засобу вибору методу модулярного експоненціювання на основі розробленого в третьому розділі методу обробки нечітких даних. Це дало змогу оцінити час оброблення нечітких даних залежно від використаної для його побудови елементної бази та кількості комірок запам’ятовуючого пристрою, які займають описи функцій належності входів. Оцінка часу оброблення нечітких даних пропонованим засобом показала

його придатність для використання в складі системи захисту сервера при реалізації на сучасних швидкодіючих мікросхемах або програмованих логічних матрицях.

4.3 Дослідження реалізації засобу розподілу доступу на базі ПЛМ

Дослідження ефективності роботи пропонованого засобу розподілу доступу здійснено за допомогою “Spartan-3 Starter Kit”, що містить ПЛМ Spartan-3 обсягом 200 тисяч логічних елементів [155]. Реалізацію здійснено на мові VHDL засобами середовища ISO 10.3 проектування фірми Xilinx. З цією метою проект засобу розподілу доступу на основі нечіткої логіки розділено на 3 основні модулі – модуль реалізації блоку керування (Control Unit), блоку обробки нечіткої інформації (Processing Unit) та блоку знаходження центра ваги, тобто здійснення нечіткого висновку (ROM). Структурна схема спроектованого засобу подана на рисунку 4.9.

На рисунку 4.9 входи data_in_0, data_in_1 та data_in_2 відповідають вхідним значенням продуктивності (П), стійкості до часового аналізу (С) та допустимих затрат пам’яті (ЗП), що записуються в РГ1, РГ2 та РГ3 схеми на рисунку 4.1, відповідно. Ці значення поступають безпосередньо з сервера, де вони попередньо обробляються. Вхід start_processing та вихід end_processing здійснюють дозвіл на обробку нечітких даних та завершення роботи засобу, відповідно. Виходи блоку Control Unit address_mem, K2 і K3 позначають адресу та керуючі сигнали, що є виходами блоку керування, зображеного схемою рисунку 4.5. Сигнал wr_en здійснює дозвіл на запис значень у регістри РГ1…РГ3.

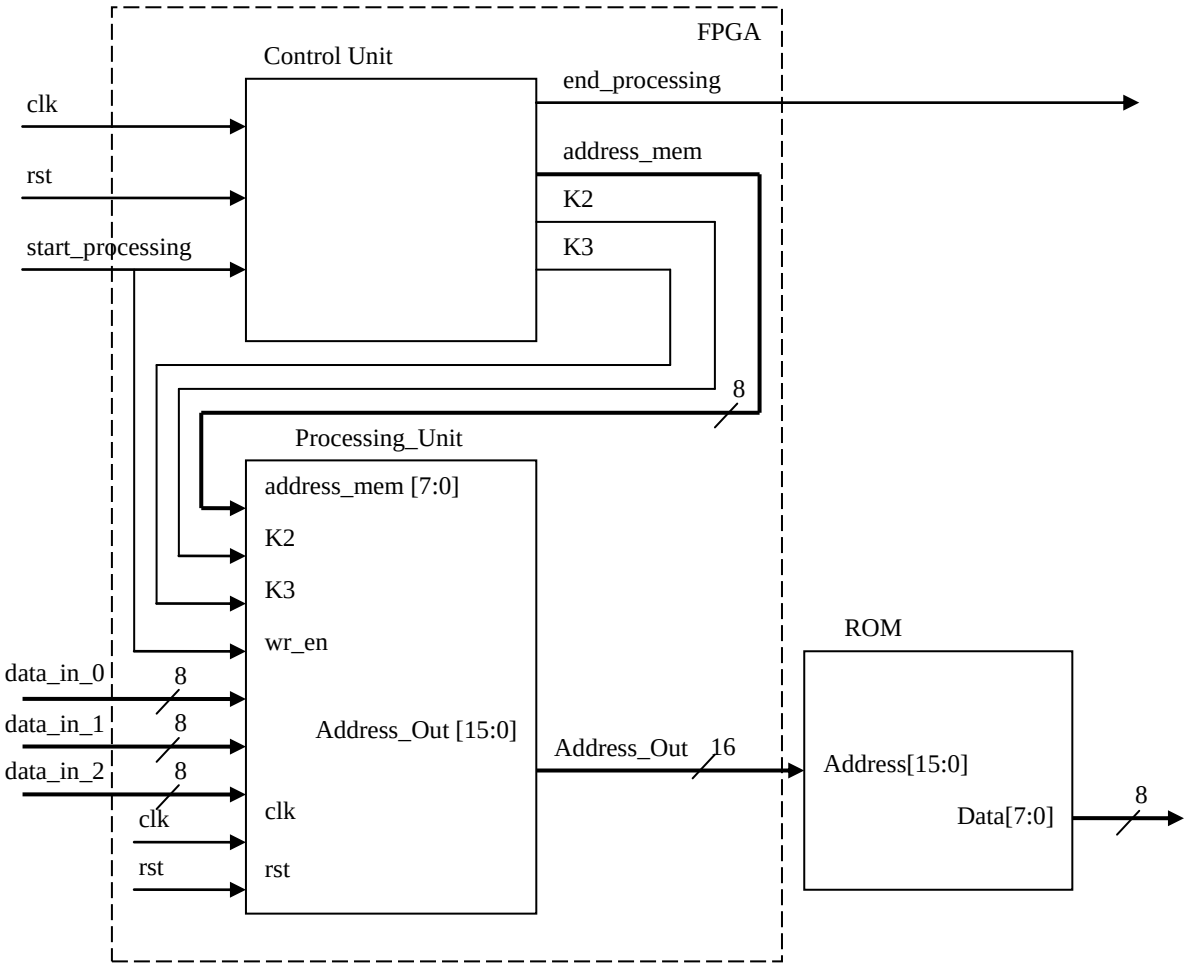


Рисунок 4.9 – Схема структурна засобу розподілу доступу на основі нечіткої логіки

Структурна схема блоку керування Control Unit подана на рисунку 4.10. У цій схемі RS_FF відповідає тригеру Тг на рисунку 4.5, Counter_1 та Counter_2 – лічильникам Ліч.1 та Ліч.2, відповідно. Logical circuits виконує роль дешифратора, виходами якого є керуючі сигнали К1, К2 та К3. Виходом блоку Parraller_Reg є код адреси набору значень функцій належності входу.

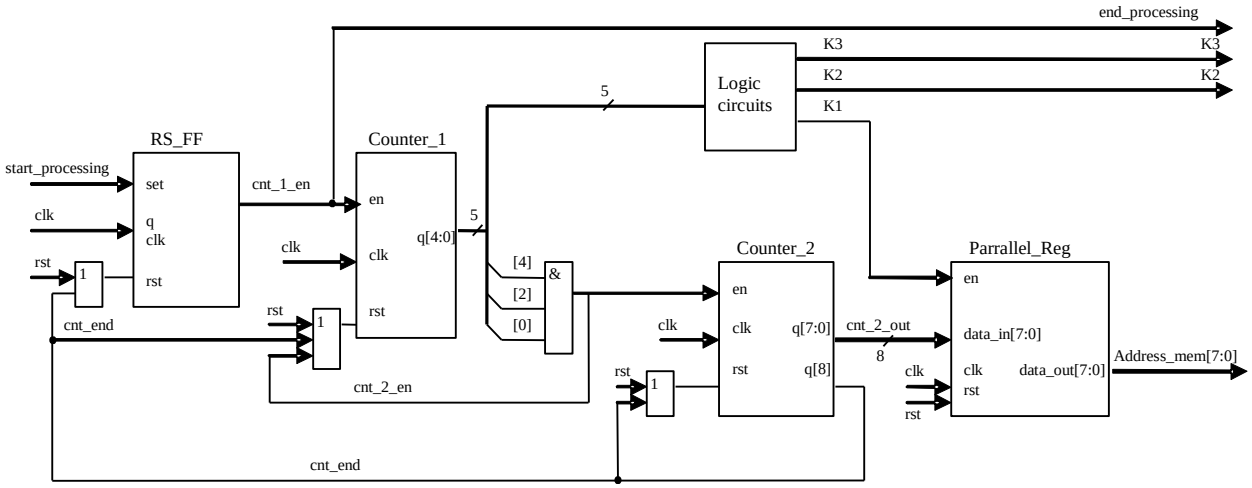


Рисунок 4.10 – Схема структурна блоку керування

В загальному HDL-проект засобу розподілу доступу шляхом вибору методу модулярного експоненціювання складається з наступних модулів:

– control unit – блок керування (див. рисунок 4.9);

– memory unit – модуль виводу коду адреси запису даних у ПЗП (див. рисунок 4.1);

– compare cor – модуль порівняння вхідних даних із даними, що зберігаються в ПЗП;

– adder – модуль роботи суматора;

– min–operand – знаходження мінімального значення;

– multiplier – модуль виконання множення X1 (див. рисунок 4.1);

– parallel_reg – модуль виводу коду адреси набору значень функцій належності входу (див. рисунок 4.10);

– modular_exponentiation – модуль знаходження методу модулярного експоненціювання, відображений на рисунку 4.1;

– processing unit – блок опрацювання даних.

HDL-коди опису модулів проекту подані в додатку Ж.

Схема структурна блоку опрацювання даних засобу вибору методу модулярного експоненціювання згенерована засобами Active-HDL зображена на рисунку 4.11.

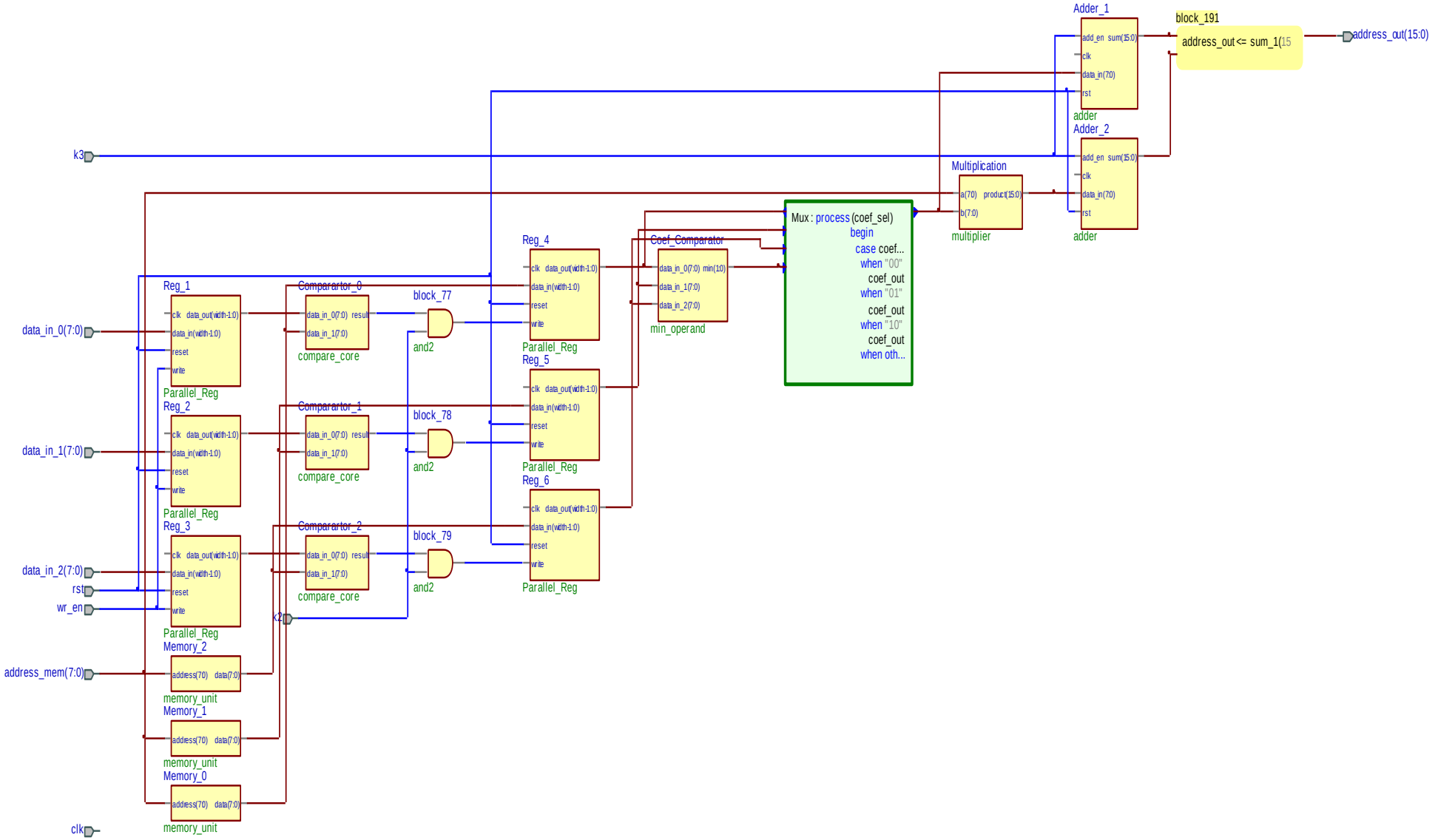


Рисунок 4.11 – Схема структурна блоку обробки даних

Результати симуляції роботи засобу розподілу доступу в комп'ютерних системах на основі нечіткої логіки на базі відлагоджувальної плати Spartan-3 Starter Kit (xc3s200-4-ft256) подані в таблиці 4.2.

Таблиця 4.2 – Витрати на реалізацію засобу

Параметр	Значення
Апаратні затрати	
Кількість слайсів	121 з 1920 (6%)
Кількість тригерів	103 з 3840 (2%)
Кількість 4-входових LUT, з них в якості ПЗП	549 з 3840 (14%), 384
Кількість ліній вводу-виводу	44
Часовий аналіз	
Мінімальний період виконання	32.053ns
Максимальна частота	31.198MHz
Час затримки у логічних схемах засобу	20.023ns (62,5 %)
Час проходження (затримки) у лініях зв'язку та вхідних і вихідних шинних формувачах	12.030ns (37,5 %)

Загальний звіт про симуляцію роботи засобу розподілу доступу на базі ПЛМ подано в додатку И.

Аналіз таблиці 4.2 показує, що в загальному апаратні затрати прийнятні для застосування пропонованого засобу в комп'ютерних системах. При цьому доцільно апаратно реалізувати в цій же ПЛМ інші вузли, що відносяться до системи захисту.

Дослідження часової ефективності роботи засобу розподілу доступу в комп'ютерних системах, здійснені за допомогою "Spartan-3 Starter Kit", що містить ПЛМ Spartan-3 обсягом 200 тисяч логічних елементів, показали, що

загальний час одного циклу роботи засобу розподілу доступу становить $\tau 1 \approx 32\,\text{ns}$, а максимальна частота - $f \approx 31{,}2$ MHz. Отриманий час не враховує кількості циклів роботи $N = 32...128$. Якщо знехтувати часом спрацювання блоків, що, згідно рисунка 4.1 та (4.2), не працюють циклічно, то час роботи засобу розподілу доступу можна приблизно оцінити як $\tau_{\Sigma} \approx \tau 1 \cdot N \approx 1...4{,}2\,\text{мкс}$. Отримане значення значно менше, за вказане в таблиці 4.1. Це можна пояснити, по-перше, значною залежністю вказуваного в технічній документації часу затримки елементів ПЛМ від методу нормування, і, по-друге, різницею у використовуваних у структурі засобу розподілу доступу технічних рішень при його виконанні на дискретних логічних елементах та засобами ПЛМ.

Таким чином, в даному підрозділі синтезовано структурну схему засобу визначення методу модулярного експоненціювання та проведено дослідження його роботи, що підтвердили працездатність та можливість застосування у комп'ютерних системах даного засобу з метою розподілу доступу до інформаційних ресурсів.

ВИСНОВКИ ДО РОЗДІЛУ 4

1. Сформовано вимоги та, відповідно до них, синтезовано структурну схему засобу вибору методу модулярного експоненціювання, який має використовувати комп’ютерна система (сервер) для обміну інформацією за заданим каналом.

2. Проведено дослідження роботи пропонованого засобу у симуляторі Electronics Workbench та середовищі ISO 10.3 проектування фірми Xilinx, які показали прийнятність обчисленого часу визначення методу модулярного експоненціювання для комп’ютерних систем, що підтверджує працездатність засобу розподілу доступу в таких системах.

3. Дослідження ефективності роботи засобу розподілу доступу до інформаційних ресурсів комп’ютерної системи, здійснені за допомогою “Spartan-3 Starter Kit”, показали, що залежно від кількості комірок (32 - 128), які описують функції належності входів, час оброблення нечітких даних становить 1 – 4,2 мкс, що підтверджує його працездатність і можливість застосування в сучасних комп’ютерних системах.

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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про кіберзлочинність [Електронний ресурс] - Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.
2. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем / Я.М.Николайчук, Н.Я.Возна, І.Р.Пітух – Тернопіль: ТзОВ «Терно-граф», 2010. – 392 с.
3. Архітектура клієнт-сервер [Електронний ресурс] - Режим доступу: http://www.intelsd.com/?tc=175&sc=197&lvl=2.
4. Васильцов І.В.Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В.Васильцов / За ред. В.П.Широчина – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.
5. Кулаков Ю.О. Комп'ютерні мережі: Підручник. / Ю.О.Кулаков, Г.М.Луцький / За ред. Ю.С.Ковтанюка – К.: Видавництво «Юніор», 2005. – 400 с.
6. Романец Ю.В. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, / Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. - М.: Радио и связь, 1999. -328 с.
7. Широчин В.П. Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях / В.П.Широчин, В.Е.Мухин, А.В.Кулик. - К.: "ВЕК+", 2000. – 112 с.
8. Дудикевич В.Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв'язку / В.Б.Дудикевич, Ю.Л.Пархуць // Інформаційна безпека. – 2011. - №1(5). – С.83-87.
9. Василенко В. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ / В.Василенко, М.Будько. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – Випуск 9. – С.110-120.

10. Тичковський Р.О. Математичне та програмне забезпечення оптимального розподілу ресурсів серед вузлів комп'ютерних мереж: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 01.05.03 «Математичне та програмне забезпечення обчислювальних машин і систем» / Р.О.Тичковський. – Львів, 2010. – 20 с.
11. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. / В.Столлингс. – М.: Изд. Дом «Вильямс», 2001. – 672 с.
12. Безмалый Н.В. Как ломаются пароли / Н.В.Безмалый // Журнал информационных технологий СНІР. – 2008. - №7. – С.124-126.
13. Україна значно піднялася в рейтингу країн з найбільшою кількістю кібер-загроз [Електронний ресурс] - Режим доступу: http://www.rbc.ua/ukr/top/show/
14. Зайчук А.В. Основные пути утечки информации и несанкионированного доступа в корпоративных сетях / А.В.Зайчук // Захист інформації. – 2003. – № 4. – С. 19-24.
15. Чеховский С.А. Побочные излучения и защита информации в локальных сетях. / С.А.Чеховский, Ю.М.Рудаков // Захист інформації. – 2003. – № 4. – С. 30-38.
16. Koeune F. A Tutorial on Physical Security and Side-Channel Attacks/ F.Koeune, F.-X. Standaert : Foundations of Security Analysis and Design III (FOSAD 2004/2005), November 2006. – 2006. - LNCS 3655. – P. 78-108.
17. Заболотний В.І. Класифікація технічних каналів витоку інформації / В.І.Заболотний // Радіотехніка. Тематичний випуск "Інформаційна безпека". - 2003. - № 134. - С.210-218.
18. Журавель Т.Н. Некоторые особенности защиты информации с ограниченным доступом от утечки по виброакустическому каналу / Т.Н.Журавель // Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003. - С.91-95.
19. Васильченко И.И. Магнитоэлектрические виброизлучатели с пониженным уровнем акустического шума для систем технической защиты информации /

И.И.Васильченко, И.А.Кравченко / Защита информации: Сборник научных трудов. Выпуск 10. – Киев: НАУ, 2003. - С.96-105.

20. Безруков К. Н. Классификация компьютерных вирусов MS DOS и методы защиты от них / К.Н.Безруков.— М.; СПб "ICE", 1990. – 48 с.
21. Brier E. Chemical Combinatorial Attacks on Keyboards / E.Brier, D.Naccache, P.Paillier [Електронний ресурс] - Режим доступу: http://eprint.iacr.org/2003/217.pdf
22. Skorobogatov S. Optical Fault Induction Attacks / S.Skorobogatov, R.Anderson // Cryptographic Hardware and Embedded Systems – CHES 2002): 4th International Workshop, August 13-15, 2002: Proceedings. − San Francisco (USA), 2002.− P.2-12.
23. Горбачёв В. Модель угроз, реализуемых аппаратными ресурсами компьютерных систем / В.Горбачёв, В.Степаненко, Т.Гриценко. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – Випуск 9. – С.75-78.
24. Agrawal D. The EM Side-Channel(s) / D.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi // Cryptographic Hardware and Embedded Systems – CHES 2002): 4th International Workshop, August 13-15, 2002: Proceedings. - San Francisco 2002. - LNCS 2523. - P. 29 - 45.
25. Kocher P. Differential Power Analysis / P.Kocher, J.Jaffe, B.Jun // in Advances in Cryptology (CRYPTO'99): 19th Annual International Cryptology Conf., August 1999: Proceedings. - Santa Barbara, California, USA, 1999. - LNCS 1666. - P.388-397.
26. Гопиенко А.В. Формирование потайных каналов передачи информации в компьютеризированных измерительных системах / А.В.Гопиенко, Ю.В.Куц, Е.В.Монченко // Системи обробки інформації. – 2012. – Вип. 3(101). – Т.1. – С.123-126.
27. 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.

28. Васильцов І.В. Класифікація сучасних атак спеціального виду на реалізацію / І.В.Васильцов, Л.О.Дубчак // Захист інформації. – 2007. - №4. – С.10-21.
29. Floyd J.J. 6.587 Computer & Network Security / J.J.Floyd, K.E.Fu, P.Sun // Differential Fault Analysis: Final Project. December 19, 1996. – 24 p. [Електронний ресурс] - Режим доступу: http://people.cs.umass.edu/~kevinfu/papers/rc5-dfa-paper.pdf
30. Biham E. Differential Fault Analysis of Secret Key Cryptosystems / E.Biham, A.Shamir // Advances in Cryptology (CRYPTO '97): 17th Annual International Cryptology Conf., 1997: Proceedings. -Santa Barbara (USA). - LNCS 1294 . Springer-Verlag, 1997.− P.513-525.
31. Borst J. Block Ciphers: Design, Analysis and Side-Channel Analysis: Doctoral dissertation / J.Borst. − K.U.Leuven, 2001.−152p.
32. Biham E. Diferential fault analysis of secret key cryptosystems / E.Biham, A.Shamir // Advances in Cryptology {Crypto '97): LNCS, Vol.1294. - Berlin, Springer-Verlag, 1997. - P. 513-525.
33. Muir J.A. Techniques of Side Channel Cryptanalysis: thesis requirement for the degree of Master of Mathematics in Combinatorics and Optimization. / J.A.Muir – Waterloo, Ontario, Canada, 2001. – 92 p.
34. Muir J. Techniques of side channel cryptanalysis: Technical report / University of Waterloo. Dept. of Combinatorics and Optimization.− Waterloo (CA), 2001. – 153 p.
35. Kelsey J. Side Channel Cryptanalysis of Product Ciphers / J.Kelsey, B.Schneier, D.Wagner, C.Hall // Journal of Computer Security. – 2000. - v.8, №2-3. - P. 141-158.
36. Tiri K. Side-Channel Attack Pitfalls / K.Tiri // Design Automation Conference (DAC 2007), June 4-8, 2007: Proceedings. - San Diego, California, USA, 2007. - P.15-20.
37. Коркішко Л. Статистична модель суматора за модулем 2N для проведення інженерно-криптографічних атак за побічними каналами витоку інформації / Л.Коркішко, І.Васильцов. // Правове, нормативне та метрологічне

забезпечення системи захисту інформації в Україні. – 2004. – Випуск 8. – С.115-121.

38. Карпінський Б.З. Пристрої потокового шифрування підвищеної стійкості до спеціальних впливів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.05 «Елементи та пристрої обчислювальної техніки та систем керування» / Б.З.Карпінський. - Тернопіль, 2007. – 21 с.

39. Чмора А.Л. Современная прикладная криптография.−2-е изд./ А.Л.Чмора. − М.: Гелиос АРВ, 2002. – 256 с.

40. Якименко І.З. Методи та алгоритми опрацювання інформаційних потоків в комп'ютерних мережах за умови застосування еліптичних кривих: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.05 «Комп'ютерні системи та компоненти» / І.З.Якименко. – Тернопіль, 2012. – 20 с.

41. Wollinger T. How Secure Are FPGAs in Cryptographic Applications? / T.Wollinger, C. Paar // Field Programmable Logic and Applications (FPL 2003): 13th International Conf., September 1-3, 2003: Proceedings. - Lisbon, Portugal, 2003. – P.91-100.

42. Messerges T.S. Power Analysis Attacks of Modular Exponentiation in Smartcards / T.S.Messerges, E.A.Dabbish, R.H.Sloan // Cryptographic Hardware and Embedded Systems (CHES'99): First International Workshop, August 1999. - Worcester, MA, USA. - LNCS 1717. – Springer-Verlag Berlin Heidelberg 1999. – P.144-157.

43. Vasyltsov I. Power and Fault Analysis in ECC. Problems and Solutions / I.Vasyltsov, H.-K.Son, E.Baek // e-Smart 2005 Conference, September, 2005. - Sophia-Anthipolis, France, 2005.

44. Ding C. The Differential Cryptanalysis and Design of Natural Stream Ciphers / C.Ding //In Fast Software Encryption: Cambridge Security Workshop, December 1993. - Springer-Verlag, Berlin, 1994. - P. 101-115.

45. Hanley N. Correlation Power Analysis of Large Word Sizes / N.Hanley, R.McEvoy, M.Tunstall, C.Whelan, C.Murphy, W.P.Marnane // Irish Signals and

Systems Conference (ISSC 2007), September 13-14, 2007: Proceeding. - Derry, 2007 – 6 p.

46. Groza B. Cryptanalysis of an Autentication Protocol / B.Groza, D.Petrica // Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'05): 7-th Symposium, 2006: Proceedings. – 2005. – P.147-157.
47. Xiao L. An Improved Power Analysis Attack Against Camellia's Key Schedule / L.Xiao, H.M.Heys // September 22, 2005. – 16 p. [Електронний ресурс] - Режим доступу: http://eprint.iacr.org/2005/338.pdf
48. Fouque P. Power Attack on Small RSA Public Exponent / P.Fouque, S.Kunz-Jacques, G.Martinet, F.Muller, F.Valette / 15 p. [Електронний ресурс] - Режим доступу: http://www.iacr.org/archive/ches2006/27/27.pdf
49. Капустян М.В. Оценка эффективности функционирования сложных систем / М.В.Капустян, В.А.Хорошко // Інформаційна безпека. – 2011. - №1(5). – С.5-8.
50. Brumley D. Remote Timing Attacks are Practical / D.Brumley, D. Boneh [Електронний ресурс] - Режим доступу: http://crypto.stanford.edu/~dabo/pubs/papers/ssl-timing.pdf
51. Quisquater J.-J. Side Channel Attacks / J.-J.Quisquater, F.Koeune.// State-of-the-art regarding side channel attacks: report, October, 2010. – 2010. – 47 p. [Електронний ресурс] - Режим доступу: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf
52. Вельшенбах М. Криптография на Си и С++ в действии: Учебное пособие. / М.Вельшенбах. – М.: Издательство Триумф, 2004. – 464 с.
53. Молдовян А.А. Криптография. / А.А.Молдовян, В.А.Молдовян, Б.Я.Советов –СПб.: Издательство "Лань", 2000. – 224 с.
54. Задірака В.К. Методи захисту фінансової інформації: Навч. посібник / В.К.Задірака, О.С.Олексюк. – К.: Вища школа, 2000. – 460 с.
55. Ємець В. Сучасна криптографія. Основні поняття / В.Ємець, А.Мельник, Р.Попович. - Львів: БаК, 2003. – 144 с.

56. Фергюсон Н. Практическая криптография : Пер. с англ. / Н.Фергюсон, Б.Шнайер. – М.: Издательский дом «Вильямс», 2005. – 424 с.
57. Ховард М. Защищенный код: Пер. с англ. / М.Ховард, Д.Лебланк. – М.: Издательско-торговый дом «Русская Редакция», 2004. – 704 с.
58. Biehl I. Differential Fault Attacks on Elliptic Curve Cryptosystems / I.Biehl, B.Meyer, V.Muller.// Advances in Cryptology (CRYPTO 2000): 20th Annual International Cryptology Conference, August 2000: Proceedings. - Santa Barbara, California, USA, 2000. - P.131 –146.
59. Chevallier-Mames B. Low-Cost Solutions for Preventing Simple Side-Channel Analysis: / B.Chevallier-Mames, M.Ciet, M.Joye / Side-Channel Atomicity. Cryptology ePrint Archive, Report 2003/237. [Електронний ресурс] - Режим доступу: http://citeseer.ist.psu.edu/bellezza01countermeasures.html.
60. Николайчук Я.М. Теорія джерел інформації / Я.М.Николайчук – Тернопіль: ТзОВ «Терно-граф», 2010. – 536 с.
61. Oswald E. Randomized addition-subtraction chains as a countermeasure against power attacks / E.Oswald, M.Aigner // Cryptographic Hardware and Embedded Systems (CHES 2001): Third International Workshop, May 14-16, 2001: Proceedings. - Paris, France, 2001. - P.39-50.
62. Karri R. Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers / R.Karri, K.Wu, P.Mishra, Y.Kim // Design Automation Conference: International Conf., 2001: Proc.− New York (USA), 2001.− P.579-585.
63. Васильцов І.В. Методи структурної надлишковості як протидія атакам апаратних помилок / І.В.Васильцов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2004. - Вип. 8.- С.108-115.
64. Васильцов І.В. Топологічний підхід до побудови криптопристроїв, стійких до атаки апаратних помилок / І.В.Васильцов // Захист інформації – 2004. - №3. - С.5-13.

65. Mamiya H. Efficient countermeasure against RPA, DPA, and SPA / H.Mamiya, A.Miyaji, H.Morimoto // Cryptographic Hardware and Embedded Systems (CHES'04), LNCS 3156 - Springer-Verlag, 2004. - P.343-356.
66. Горпенюк А.Я. Підвищення швидкодії при обчисленні важкооборотних функцій в асиметричних алгоритмах шифрування. / А.Я.Горпенюк, В.Б.Дудикевич, І.Б.Ломницький // Захист інформації. – 2003 – №1(18) – С.36-43.
67. Stoll M. On the Reduction Theory of Binary Forms / M.Stoll, J.E.Cremona / P.1-18. [Електронний ресурс] - Режим доступу: http://www.mathe2.uni-bayreuth.de/stoll/papers/reduction-part-1.pdf
68. Kholosha A. Clock-Controlled Shift Registers for Key-Stream Generation / A.Kholosha // Cryptology in India: Progress in Cryptology (INDOCRYPT '01): Second International Conference, 2001: Proceedings. - Springer-Verlag, London, UK – P. 287-296.
69. Messerges T.S. Power Analysis Attack Countermeasures and Their Weaknesses / T.S. Messerges // Communications, Electromagnetics, Propagation and Signal (CEPS): Workshop, 2000.: Processing. – University of Illinois at Urbana-Champaign, 2000. – P.1-28.
70. Iftene S. General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting / S.Iftene // ICS 2006 . – P.45-60. / Electronic Notes in Theoretical Computer Sciense URL : [Електронний ресурс] - Режим доступу: www.elsevier.nl/locate/entcs
71. Kim C.K. An Improved and Efficient Countermeasure against Power Analysis Attacks / C.K.Kim, J.C.Ha, S.J.Moon, S.M.Yen, W.C.Lien, S.H.Kim / 14 p. [Електронний ресурс] - Режим доступу: http://eprint.iacr.org/2005/022.pdf
72. Galibus T. Mignotte's sequences over polynomial rings / T.Galibus, G.Matveev // ICS 2006 . – P.39-44. / Electronic Notes in Theoretical Computer Sciense URL : [Електронний ресурс] - Режим доступу: www.elsevier.nl/locate/entcs
73. 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.

74. Шевчук Р.П. Багатоканальні комп'ютерні засоби перетворення та криптографічного захисту форматів стиснених мовних сигналів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.05 «Комп'ютерні системи та компоненти» / Р.П.Шевчук. – Тернопіль, 2008. – 20 с.

75. Зибін С.В.Захист інформації від несанкціонованого доступу в системах обробки інформації / С.В.Зибін // Інформаційна безпека. – 2011. - №1(5). – С.137-142.

76. Сорокопуд С.А. Обеспечение информационной безопасности корпоративной сети предприятия / С.А.Сорокопуд, Л.В.Мудрова, С.В.Ширяев // Захист інформації. – 2005. - № 1. - С.21-30.

77. Шорошев В. Системы обнаружения атак для защиты Интранет / В.Шорошев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – Випуск 9. – С.78-94.

78. Вербіцький О.В. Вступ до криптографії./ О.В. Вербіцький – Львів: Видавництво науково-технічної літератури, 1998. – 247 с.

79. 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.

80. 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.

81. Рудницький В.М. Систематизація повної множини логічних функцій для криптографічного перетворення інформації / В.М.Рудницький, І.В.Миронець, В.Г.Бабенко // Системи обробки інформації. – 2011. – Вип. 8(98). – С. 184-188.

82. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. - [Чинний від 1997-01-01.] – К.: Держстандарт України, 1996. – 5 с. – (Національний стандарт України).
83. Кінах Я.І. Методи паралельних обчислень та обґрунтування рівня криптографічного захисту інформації в комп'ютерних мережах: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.13 «Обчислювальні машини, системи та мережі» / Я.І.Кінах. – Тернопіль, 2007. – 20 с.
84. Hong S.-M. New Modular Multiplication Algorithms for Fast Modular Exponentiation / S.-M.Hong, S.-Y.Oh, H.Yoon // Theory and Application of Cryptographic Techniques (EUROCRYPT'96): 15th annual international conference, 1996: Proceedings. – Springer-Verlag, Germany, 1996. – P.166-177.
85. Лахно В.А. Експериментальні дослідження зміни продуктивності корпоративних інформаційних систем підприємств в умовах реалізації комп'ютерних атак / В.А.Лахно, О.С.Петров // Інформаційна безпека. – 2011. - №1(5). – С.181-189.
86. Кондратенко Ю. П., Сидоренко С. А. Програмно-алгоритмічне забезпечення комп'ютеризованих систем технічної діагностики і прогнозування поведінки складних технічних об'єктів / Ю.П.Кондратенко, С.А.Сидоренко // Оброблення сигналів і зображень та розпізнавання образів: Четверта всеукр. міжн. конф., 1 9—23 жовтня, 1998 р.— К., 1998.— С. 125—126.
87. Ross T.J. Fuzzy Logic with Engineering Applications / T.J.Ross. – McGraw-Hill Inc.(USA), 1995. – 600 p.
88. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику / С.Д.Штовба [Електронний ресурс] - Режим доступу: http://matlab.exponenta.ru/fuzzylogic/book1/
89. Бережная М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах. / М.А. Бережная // Технология приборостроения. – 2009. – №2. – С. 16–23.

90. Михайленко В.С. Использование нечеткой адаптивной системы управления для компьютерного мониторинга сетью котельных установок / В.С.Михайленко, В.В.Никольский [Електронний ресурс] - Режим доступу: http://aaecs.org/mihailenko-vs-nikolskii-vv-ispolzovanie-nechetkoi-adaptivnoi-sistemi-upravleniya-dlya-kompyuternogo-monitoringa-setyu-kotelnih-ustanovok.html
91. Ozyer T. Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening / T.Ozyer, R.Alhajj, K.Barker // Journal of Network and Computer Applications. – 2007. – №30. – P.99-113.
92. Корченко А.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения / А.Г.Корченко. – К. : МК-Пресс, 2006. – 320 с.
93. Гнатчук Є.Г. Інформаційна технологія подання та опрацювання знань на основі нечіткої логіки в експертних системах діагностування комп'ютерних засобів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 «Інформаційні технології» / Є.Г.Гнатчук. – Львів, 2008. – 20 с.
94. Ротштейн О.П. Soft Computing в біотехнології: багатофакторний аналіз і діагностика / О.П.Ротштейн, Є.П.Ларюшкін, Ю.І.Мітюшкін – Вінниця: УНІВЕРСУМ-Вінниця, 2008. – 144 с.
95. Мороз О.В. Економічна ідентифікація параметрів стійкості та ризикованості функціонування господарських систем / О.В.Мороз, А.О.Свентух – Вінниця: УНІВЕРСУМ-Вінниця, 2008. – 168 с.
96. Панкевич О.Д. Діагностування тріщин будівельних конструкцій за допомогою нечітких баз знань / О. Д. Панкевич, С. Д. Штовба – Вінниця: УНІВЕРСУМ-Вінниця, 2005. – 108с.
97. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы./ Д.Рутковская, М.Пилиньский, Л.Рутковский. - М.: Телеком, 2006. – 382 с.

98. Abadeh M.S. Intrusion Detection Using a Fuzzy Genetics-Based Learning Algorithm / M.S.Abadeh, J.Habibi, C.Lucas // Journal of Network and Computer Applications. – 2007. – №30. – P.414-428.
99. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д.Штовба // Проблемы управления и информатики. – 2007. – №4. – С. 102–114.
100. Zimmermann R. Computer Arithmetic: Principles, Architectures and VLSI Design / R.Zimmermann / Lecture notes Swiss Federal Institute of Technology, June 25, 1998. – Zurich, 1998. - 98p. [Електронний ресурс] - Режим доступу: http: //www.iis.ee.ethz.ch/ zimmi/publications/ comp.arith.notes.ps.gz
101. Ахо А.В. Структуры данных и алгоритмы: Пер. с англ. / А.В.Ахо, Д.Э.Хопкрофт, Д.Д.Ульман. – М.: Издательский дом «Вильямс», 2001. – 384с.
102. 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.
103. Васильцов І.В. Стійкість сучасних алгоритмів модулярного експоненціювання до часового аналізу / І.В.Васильцов, Л.О.Васильків // Захист інформації. – 2005. - №1. - С. 54-69.
104. Семейство микроконтроллеров MSP430x1xx. Руководство пользователя: Пер. С англ. – М.: Серия «Библиотека Компэла». ЗАО «Компэл», 2004. – 368 с.
105. MSP430 Family Assembly Language Tools User's Guide. Texas Instruments Incorporated. 2008 [Електронний ресурс] - Режим доступу: http://www.ti.com/lit/ug/slau131c/slau131c.pdf
106. MSP430 Family Software User's Guide. Texas Instruments Incorporated. Printed in Germany by Sellier Druck, Freising, 1994
107. MSP430 Family Architecture Guide and Module Library TII. - Printed by Staples Printer, ME2 4LT, England, 1996.

108. Intel Corporation. MCS 51 Microcontroller Family User's Manual. Order No: 272383-002. February 1994. Printed in UK by O& i LTd Embedded Microcontrollers

109. 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.

110. 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.

111. 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.

112. 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.

113. 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.

114. Бронштейн И.Н. Справочник по математике / И.Н.Бронштейн, К.А.Семендяев. – М.: Наука. Главная редакция физико-математической литературы, 1967. – 608 с.

115. 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.

116. 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, Україна, 2009. - С.110-111.

117. 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.

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

119. Карасев А.И. Теория вероятностей и математическая статистика / А.И.Карасев. – м.: Статистика, 1979. – 279 с.

120. Гмурман В.Е. Руководство к решению задач по теории вероятностей и математической статистике / В.Е.Гмурман. – М.: Высшая школа, 1975. – 333с.

121. Крайников А.В. Вероятностные методы в вычислительной технике: Учебное пособе для вузов/ А.В.Крайников, Б.А.Курдиков, А.Н.Лебедев и др.; Под ред. А.Н.Лебедева и Е.А.Чернявского. – М.: Высшая школа, 1986. – 312 с.

122. Королюк В.С. Справочник по теории вероятностей и математической статистике / В.С.Королюк, Н.И.Портенко, А.В.Скороход, А.Ф.Турбин. – М.: Наука. Главная редакция физико-математической литературы, 1985. – 640 с.

123. Петров А.О. Принципи проектування та оцінки систем захисту інформації в мережах загального користування / А.О.Петров // Інформаційна безпека. – 2011. - №1(5). – С.49-56.

124. Patent US 2010/0177887A1, Int.Cl. H04L9/28. Montgomery-based modular exponentiation secured against hidden channel attacks / M.Ciet, B.Feix; Gemalto SA (FR). – Appl. No. 12/666,892; May 2, 2008; Jul.15,2010.

125. Patent US 7,020,281B2, Int.Cl. H04L9/00. Timing attack resistant cryptographic system / A.Vadekar, R.J.Lambert; Certicom Corp. (CA). – Appl. No.09/761,700; Oct.25, 2001; Mar.28,2006

126. Patent US 2011/0131424A1, Int.Cl. G06F21/00. Zero divisors protecting exponentiation / D.Vigilant; Gemalto (FR). – Appl. No. 13/057,703; Jul.30, 2009; Jun.2, 2011.

127. Patent US 7,664,810B2, Int.Cl. G06F7/38, H04L9/00. Microprocessor apparatus and method for modular exponentiation / T.A.Crispin, G.G.Henry, T.Parks; Via Technologies, Inc. (TW). – Appl. No.11/130,472; Nov.17, 2005; Feb.16,2010.

128. Patent US 2003/0065696A1, Int.Cl. G06F7/38. Method and apparatus for performing modular exponentiation / M.D.Ruehle, J.A.Morelli. – Appl. No.09/966,224; Sep.28, 2001; Apr.3,2003.

129. Patent US 2003/0133567A1, Int.Cl. H04L9/00. Encryption operating apparatus and method having side-channel attack resistance / J.Yajima, K.Itoh, M.Takenaka, N.Torii; Fujitsu Limited (JP). – Appl. No.10/278,838; Oct.24, 2002; Jul.17,2003.

130. Patent US 6,282,290B1, Int.Cl. H04K9/28. High speed modular exponentiator / G.A.Powell, M.W.Wilson, K.Q.Truong, C.P.Curren; Mykotronx, Inc. (US). – Appl. No.08/828,368; Mar.28, 1997; Aug.28,2001.

131. Лазарєв Ю.Ф. Моделювання динамічних систем у Matlab. Електронний навчальний посібник / Ю.Ф.Лазарєв – К.: НТУУ «КПІ», 2011. – 421 с. : [Електронний ресурс] - Режим доступу: http://kafpson.kpi.ua/Arhiv/Lazarev/mds_matlab.pdf

132. 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. - Т.1, №3 . – С.236-242.

133. Гостев В.И. Определение управляющих воздействий на выходе нечеткого регулятора при идентичных треугольных функциях принадлежности с увеличенным наклоном / В.И.Гостев, С.Н.Скуртов, И.В.Панченко // Вісник Хмельницького національного університету. Технічні науки. – 2007. - № 5. – С.253-256.

134. 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.

135. 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.

136. Пат. 22731 Україна, МПК G 06F 15/00, G06F 7/06 (2006.01). Пристрій для обробки нечіткої інформації / А.А.Рідкокаша, К.К.Голдер, М.М.Рахман. – №97031243; заявл. 19.03.1997; опубл. 07.04.1998, Бюл. № 3.

137. Пат. 44595 Україна, МПК G06F 17/00. Пристрій для обробки нечіткої інформації / В.Ю.Кондратенко, Ю.П.Кондратенко. – №u200903880; заявл. 21.04.2009; опубл. 12.10.2009, Бюл. № 19.

138. Пат. 71851 Україна, МПК G06Q 99/00, G06N 7/00. Спосіб одержання якісних експертних оцінок при моделюванні економічних, соціальних, біологічних систем / Л.О.Коршевнюк, Д.О.Коршевнюк, М.Ю.Мінін. – №20031213217; заявл. 31.12.2003; опубл. 15.12.2004, Бюл. № 12.

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

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

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

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

143. Белов М.П. Основы алгоритмизации в информационных системах: Учеб. пособие / М.П.Белов. – СПб.: СЗТУ, 2003 – 85 с.

144. Черкаський М.В. Аналіз складності пристроїв множення / М.В.Черкаський, Мурад Хусейн Халіл // Комп'ютерні системи проектування. Теорія і практика: Вісник Національного університету "Львівська політехніка" – 2005. – № 548. – С.15-21.

145. Hawarah L. The Complexity of a Probabilistic Approarch to Deal with Missing Values in a Decision Tree / L.Hawarah, A.Simonet, M.Simonet // Symbolic and Numeric Algorithms for Scientific Computing (SYNASC'06): 8-th Symposium, 2006: Proceedings. –2006. - P. 69-72.

146. Constantinescu N. Linear Complexity Computations of Cryptographic Systems / N.Constantinescu, E.Simion // Telecommunications: International Conference, 4 - 7 June, 2001: IEEE, Bucharest, 2001. - Vol.1. – P. 85 - 89.

147. 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.

148. Баранов С.И. Синтез микропрограммных автоматов / Баранов С.И. – Л.: Энергия, 1979. – 232 с.

149. Мельник А.О. Архітектура комп'ютера / А.О. Мельник – Луцьк: Волинська обласна друкарня, 2008. – 470 с.

150. Шило В.Л. Популярные цифровые микросхемы: Справочник. – М.: Радио и связь, 1987. – 352 с.

151. Spartan-3 Generation FPGA User Guide. Extended Spartan-3A, Spartan-3E, and Spartan-3 FPGA Families. UG331 [Електронний ресурс] // Xilinx Inc. - 2011. – Rev.1.8. - Режим доступу - http://www.xilinx.com/support/documentation/user_guides/ug331.pdf.