НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

До захисту допущено:

Завідувач кафедри

_____ Олександр РОЛІК

«___»_____2025 р.

Дипломний проєкт

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційні управляючі системи та технології»
спеціальності 126 «Інформаційні системи та технології»
на тему: «Інформаційна система ідентифікації віддалених користувачів»

Виконала:
студентка IV курсу, групи ІС-12
Бойко Катерина Сергіївна _____

Керівник:
доцент кафедри ІСТ ФІОТ, к.т.н., доцент
Жураковська Оксана Сергіївна _____

Рецензент:
Доцент кафедри ОТ ФІОТ, к.т.н., доцент
Марковський Олександр Петрович _____

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра інформаційних систем та технологій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 126 «Інформаційні системи та технології»

Освітньо-професійна програма «Інформаційні управляючі системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Олександр РОЛІК
«___»_____2025 р.

ЗАВДАННЯ
на дипломний проєкт студентці
Бойко Катерині Сергіївні

1. Тема проєкту «Інформаційна система ідентифікації віддалених користувачів», керівник проєкту Жураковська Оксана Сергіївна, к. т. н., доцент, затверджені наказом по університету від «23» травня 2025 р. № 1705-с

2. Термін подання студентом проєкту: «9» червня 2025 р

3. Вихідні дані до проєкту: мова програмування C++ та її бібліотеки, середовище розробки Visual Studio Code

4.1. Опис предметної області: аналіз проблем криптографічно строгої ідентифікації абонентів інформаційної системи, постановка задачі розробки механізмів криптографічно строгої ідентифікації з блокуванням повторного використання перехоплених паролів, призначення системи, цілі і задачі розробки;

4.2. Аналіз існуючих методів ідентифікації: класифікація існуючих методів, огляд методів криптографічно строгої ідентифікації;

4.3. Формування вимог до системи: вимоги до системи в цілому, вимоги до функціональних характеристик, вимоги до видів забезпечення;

4.4. Вибір технологій розробки;

4.5. Розробка інформаційної системи: структура системи, функціональна модель системи, структура масивів інформації, передавання та обробка даних, архітектура програмного забезпечення, аналіз результатів моделювання;

4.6. Математичне забезпечення: безпекова модель інформаційної системи, вибір та опис прототипу, розробка методу крипт графічно строгої ідентифікації на основі незворотніх перетворень теорії чисел, оцінка ефективності;

4.7. Тестування системи;

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо):

5.1. Діаграма варіантів використання;

5.2. Структура масивів інформації;

5.3. Діаграма послідовності;

6. Дата видачі завдання: «20» лютого 2025 року

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1	Вивчення запропонованої літератури	25 лютого 2025	
2	Аналіз предметної області	10 березня 2025	
3	Огляд існуючих рішень	12 березня 2025	
4	Формування вимог до розробленої системи	18 березня 2025	
5	Розробка функціональної моделі системи	19 березня 2025	
6	Вибір технології розробки	24 березня 2025	
7	Математична постановка задачі	7 квітня 2025	
8	Програмна реалізація розробленої системи	10 квітня 2025	
9	Опис технічного рішення	13 травня 2025	
10	Тестування системи	19 травня 2025	
11	Опис результатів тестування	23 травня 2025	
12	Побудова креслеників	24 травня 2025	
13	Оформлення пояснювальної записки	7 червня 2025	

Студентка Катерина БОЙКО

Керівник Оксана ЖУРАКОВСЬКА

АНОТАЦІЯ

Бойко К. С. Інформаційна система ідентифікації віддалених користувачів. КПІ ім. Ігоря Сікорського, Київ, 2025.

Проєкт містить 73 с. тексту, 6 рисунків, 4 таблиці, посилання на 23 літературні джерела та додатки.

Ключові слова: ідентифікація, користувачі, інформаційна система, незворотні перетворення теорії чисел.

Мета дослідження – покращення методу строгої ідентифікації користувачів в віддалених інформаційних системах, шляхом прискорення і підвищення рівня захищеності процедури ідентифікації.

Об’єкт дослідження – інформаційні системи ідентифікації віддалених користувачів.

У дипломному проєкті розроблено інформаційну систему ідентифікації віддалених користувачів. Розроблено метод, що дозволяє значно пришвидшити строгу ідентифікацію на основі незворотних перетворень теорії чисел шляхом використання таблиць передобчислень. Також, розроблено посилення захищеності процедури ідентифікації абонентів взаємодії шляхом використання геш перетворень над конкатенацією номеру сеансу і випадкового числа згенерованого системою.

Отримані результати можуть бути корисними при розробці систем що потребують максимального рівня захищеності процедури ідентифікації, зокрема в військовій, медичній і банківській сферах.

SUMMARY

Boiko, K. S. Information System for Remote User Identification. Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, 2025.

The project comprises 73 pages of text, 6 figures, 4 tables, references to 23 bibliographic sources, appendices, and design documents.

Keywords: identification, users, information system, irreversible transformations of number theory.

The purpose of the study is to improve the method of strict user identification in remote information systems by accelerating and enhancing the security of the identification procedure.

The object of research is information systems for remote user identification.

In this diploma project, an information system for remote user identification has been developed. A method has been devised that significantly speeds up strict identification based on irreversible transformations from number theory by using precomputed tables. In addition, the security of the subscriber interaction identification procedure has been strengthened through the use of hash transformations on the concatenation of the session number and a random number generated by the system.

The results obtained may be useful in developing systems that require the highest level of security for the identification procedure, particularly in military, medical, and banking spheres.

№ рядка	Формат	Позначення	Найменування	Кіл. аркушів	№ екз.	Примітка
1			Документація загальна			
2						
3			Знову розроблена			
4						
5	А4	ІС12.020БАК.005 ПЗ	Інформаційна система	73		
6			ідентифікації віддалених користувачів			
7			Пояснювальна записка			
8						
9	А3	ІС12.020БАК.005 Д1	Інформаційна система	1		
10			ідентифікації віддалених користувачів			
11			Структурна схема			
12			експонеціювання			
13						
14	А3	ІС12.020БАК.005 Д2	Інформаційна система	1		
15			ідентифікації віддалених користувачів			
16			Діаграма варіантів використання			
17						
18	А3	ІС12.020БАК.005 Д3	Інформаційна система	1		
19			ідентифікації віддалених користувачів			
20			Структура масивів інформації			
21						
22	А3	ІС12.020БАК.005 Д4	Інформаційна система	1		
23			ідентифікації віддалених користувачів			
24			Схема передавання та обробки даних			
25						
26						
27						
28						

Зм.	Лист	№ докум.	Підпис		ІС12.020БАК.005 ТП		
Розробив		Бойко К.С.			Інформаційна система ідентифікації віддалених користувачів Відомість дипломного проєкту	Літ.	Арк. 1 / Аркушів 1
Перевірила		Жураковська О. С				Т	
Затв.					КПІ ім. Ігоря Сікорського Група ІС-12		

Пояснювальна записка
до дипломного проєкту
на тему: «Інформаційна система ідентифікації віддалених користувачів»

Київ – 2025 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС — інформаційна система

CPU — Central Processing Unit

KPI — Kyiv Polytechnic Institute

ZKI — Zero-knowledge identification

ВСТУП

Основною характеристикою сучасного етапу розвитку інформаційних систем стало стрімке розширення використання технологій віддаленої інформаційної взаємодії в усіх сферах життя людини. Значним поштовхом такого розширення стала пандемія вірусу COVID-19. Також, невід'ємною частиною популяризації використання цих технологій на території України стала війна. З метою захисту людей, все більше компаній, закладів освіти, тощо, обрали для себе дистанційну форму взаємодії в якості основної, на час воєнних дій.

Проте віддалена інформаційна взаємодія отримала поширення і на більш чутливі сфери життя людини, такі як, медична, банківська, адміністративна сфери, сфера надання ресурсів на комерційній основі і, звісно ж, військова сфера. Відповідно, цінність інформації що передається шляхом віддаленої взаємодії зросла, разом з цим підвищилась і кількість атак на такі системи з метою отримання певної матеріальної вигоди. Проведений аналіз показав, що більшість таких атак націлені на незаконний доступ до ресурсів системи шляхом підміни легального користувача. Такі підміни основним чином відбуваються двома способами: перехопленням правильного користувацького паролю, або витіснення легального користувача з взаємодії. Особливим видом атак, вважається підміна самої системи взаємодії легального користувача з нею.

Відповідно, всі вище описані атаки направлені на процедуру ідентифікації користувача в системі.

Тобто, основною задачею сучасного етапу розвитку віддаленої інформаційної взаємодії є підвищення рівня захищеності процедури ідентифікації користувачів. Разом з тим, в зв'язку з стрімким збільшенням кількості абонентів, що взаємодіють з системою в режимі реального часу і новим вимогам до швидкості відповіді системи, метод ідентифікації має бути достатньо ефективним.

В результаті проведених досліджень визначенно, що з метою забезпечення, високого рівня захисту користувацької інформації найкращим рішенням буде ви-

користовувати методи строгої ідентифікації. Проте, основним недоліком такого виду ідентифікації є її повільність.

Натомість, слабка ідентифікація надає користувачеві бажану швидкість відповіді, але майже не захищає його від атак.

Аналіз сучасного стану систем ідентифікації [1] віддалених користувачів показав, що існуючі методи не в повній мірі задовольняють вимогам сьогодення, тому існує об’єктивна необхідність в розробці методу, що поєднує в собі одразу дві характеристики: висока захищеність і швидкодія.

Розроблений метод передбачає модифікацію відомої схеми Шнорра, що являє собою метод строгої ідентифікації на основі незворотних перетворень теорії чисел, шляхом прискорення за рахунок передобчислень і підвищення рівня її захищеності. Тобто, розроблений метод в повній мірі задовольняє вимогам до сучасних систем ідентифікації віддалених користувачів.

Дипломний проєкт присвячено розробці інформаційній системі віддаленої ідентифікації користувачів. Результати дипломного проєкту опубліковані Proceeding of 14-th IEEE International Conference on Dependable system, Service and Technologies DESSERT-2024, 11-13 October, Greece, Athens. -2024.- P.674-677. DOI :10.1109/ DESSERT61349.2024.10416477.

Результати дипл. проєкту пройшли апробацію на конференції. Proceeding of 14-th IEEE International Conference on Dependable system, Service and Technologies DESSERT-2024, 11-13 October, Greece, Athens. -2024

1 ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ

Яскравою ознакою сучасного етапу розвитку інформаційних технологій стало розширене використання систем віддаленої інформаційної взаємодії. Що, в свою чергу, призвело до стрімкого зростання кіберзлочинів, спрямованих на незаконне отримання й використання конфіденційної інформації з метою отримання фінансової вигоди. Це зумовлює об'єктивну необхідність створення ефективних засобів ідентифікації користувачів, які б відповідали актуальним вимогам. Відповідно, розробка системи ідентифікації віддалених користувачів повинна враховувати специфіку віддаленої інформаційної взаємодії сьогодення, розгляд та аналіз існуючих рішень з огляду на цю специфіку та пошук можливостей їх вдосконалення.

1.1 Аналіз вимог до ідентифікації віддалених користувачів у сучасних системах

В загальному розумінні процедура ідентифікації являє собою процес визначення особи або об'єкта за допомогою унікальних ознак що вирізняють одного від інших. В запропонованій роботі розглядається один з найбільш важливих на практиці типів взаємодії, а саме взаємодія великої кількості користувачів з системою. Типовим прикладом такої взаємодії являються інтегровані системи віддаленого надання інформаційних та інших ресурсів великій кількості користувачів [2]. Структура системи досліджуваної в представленій роботі показана на рисунку 1.1

Характерними ознаками запропонованої структури є такі особливості здійснення ідентифікації як:

— основною задачею таких систем є ідентифікація користувача, який отримує певні інформаційні послуги або доступ до ресурсів на комерційній основі. При цьому ідентифікація самої системи для користувача не є необхідною;

— критично важливим аспектом таких систем є швидкодія самої процедури ідентифікації. Фактично, ця система направлена на масове обслуговування корис-

тувачів в режимі реального часу. Тобто виникає потреба одномоментного надання ресурсів великій кількості користувачів.

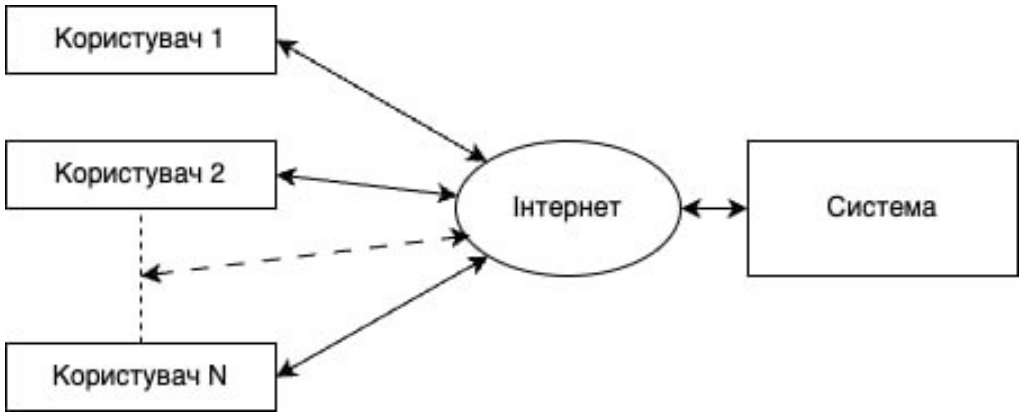

Рисунок 1.1 – Структура моделі дистанційної взаємодії інтегрованої інформаційної системи з віддаленими абонентами

Аналіз показав, що основним чином вищеописані системи торкаються сфер що потребують найвищого рівня захисту інформації, тому крім вимоги до швидкодії треба знайти компроміс в наданні ресурсів для забезпечення належного рівня захисту.

Більшість існуючих методів ідентифікації передбачають наявність двох основних процедур, а саме авторизацію віддаленого користувача в системі, що відбувається лише один раз на старті його роботи з нею і, безпосередньо, ідентифікацію, що повторюється кожного сеансу взаємодії.

Під час першого підключення здійснюється процедура авторизації, в межах якої користувач надає системі певний перелік інформації в зашифрованому вигляді на основі якої вона зможе ідентифікувати його під час подальших взаємодій.

В ході процедури ідентифікації, система запрошує у користувача певну ідентифікуючу інформацію, обумовлену в ході процедури авторизації, що дозволяє з високою стелінню ймовірності підтвердити особу користувача для подальшої взаємодії.

Критерієм ефективності розробленої системи ідентифікації віддаленого користувача являється рівень захищеності системи від спроб несанкціонованого доступу до її ресурсів з боку зловмисника. Тобто, під час розробки ефективних методів ідентифікації [3], детального аналізу також вимагають сучасні методи атак на процедуру ідентифікації.

У сучасних розподілених мережах обмін інформацією вимагає врахування можливих загроз як із локального, так і з мережевого середовища. Основна мета атак на такі системи полягає у отриманні несанкціонованого доступу до ресурсів системи шляхом перехоплення та використання пароля легітимного користувацького паролю. При цьому об’єктами атак можуть бути як середовище передачі даних, тобто інтернет, так і пам'ять системи, де зберігаються паролі користувачів. Схематично види і об’єкти атак зображені на рисунку 1.2.

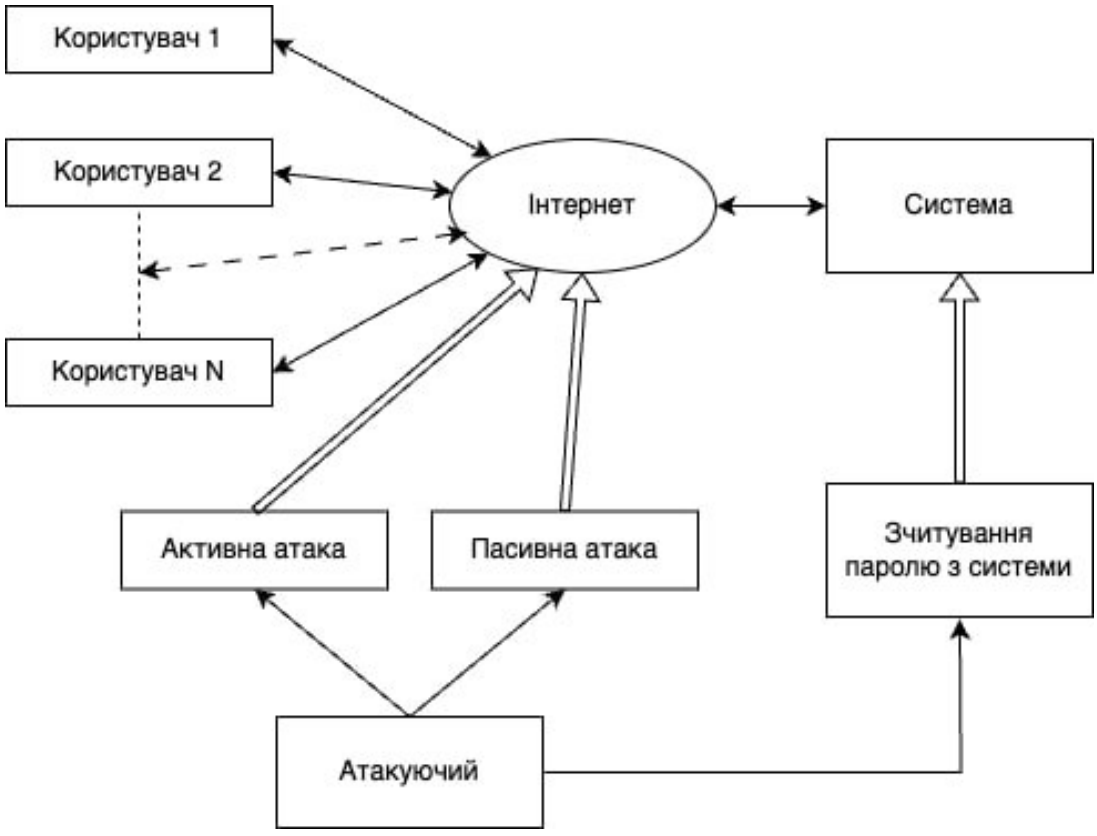

Рисунок 1.2 – Схема атак під час ідентифікації користувачів у розподілених мережах

Розрізняють два основних види атак на середовище передачі даних: пасивні і активні. Пасивні атаки заключаються в прослуховуванні правильного користувацького паролю під час його передачі, тоді як активні, або як їх ще називають middle attacks – направлені на витіснення легітимного користувача з взаємодії безпосередньо після його ідентифікації в системі [4]. Фактично що пасивні, що активні атаки здійснюються на сервери центрів комутації глобальної мережі.

Атаки на систему полягають в спробах отримати незаконний доступ до пам'яті де зберігається інформація що забезпечує проходження процесу ідентифікації легальним користувачем. Ці атаки здійснюються за допомогою зараження системи вірусними програмними забезпеченнями або з використанням людей що безпосередньо мають доступ до системи.

Особливим видом атак є імітація самою системою звернення до самої себе [5]. Такий вид атак найчастіше застосовується у багатокористувацьких системах де імітується звернення великої кількості користувачів на відносно маленьку суму, що в результаті дозволяє отримати велику фінансову вигоду.

Виходячи з описаного вище аналізу система ідентифікації віддалених користувачів має відповідати наступним вимогам безпеки [6]:

— для забезпечення захисту від пасивних атак процедура ідентифікації має запобігати повторного використання правильного паролю. Тобто паролі мають бути сеансовими, відповідно перехопивши пароль зловмисник не зможе його використати адже він не матиме сенсу при наступних процедурах ідентифікації;

— процедура ідентифікації на пряму не може запобігти пасивних атак, адже вони відбуваються вже після того як користувач ідентифікувався в системі. Одним з методів їх запобігання є повторна ідентифікація через певний проміжок часу. Тобто для ефективного запобігання такої атаки процедура ідентифікації має виконуватись достатньо швидко;

— для запобігання атаки на пам'ять системи, потрібно забезпечити відсутність необхідності зберігання інформації для отримання правильних паролей безпосередньо в системі;

— забезпечити неможливість системи самостійно генерувати правильні користувацькі паролі.

Таким чином, у сучасних умовах зростання кількості видів атак, існує потреба використання більш потужних криптографічних механізмів ідентифікації. Проте, разом з розширенням сфер використання, стрімким збільшенням кількості користувачів що перебувають в системі в режимі реального часу і вимогами до обробки даних під час безпосередньо етапу ідентифікації їх у системі, проблема забезпечення високої швидкодії дистанційної інформаційної взаємодії стала критично важливою, вимагаючи впровадження інноваційних рішень для оптимізації обчислювальних процесів. Виходячи з наведеного, у сучасних умовах забезпечення надійної та ефективної віддаленої інформаційної взаємодії вимагає розробки нових протоколів ідентифікації користувачів, які забезпечать одночасно посилений криптографічний захист та підвищену швидкодію [7]. У цьому контексті є нагальна потреба у знаходженні компромісного рішення для протиріччя між забезпеченням відповідності сучасним вимогам криптографічного захисту та підвищенням швидкодії при розробці нових методів ідентифікації. Такі методи повинні ефективно інтегруватися в існуючі системи, гарантувати їхню надійність і ефективність у процесі віддаленої інформаційної взаємодії.

1.2 Постановка задачі розробки механізмів криптографічно строгої ідентифікації з блокуванням повторного використання перехоплених паролів

1.2.1 Призначення системи

Область застосування розробки – системи віддаленого надання на комерційній основі інформаційних, програмних та обчислювальних ресурсів віддаленим користувачам інтегрованою інформаційною системою з розмежуванням та контролем прав доступу.

Призначення розробки – покращення безпекових і часових характеристик процесу ідентифікації віддалених користувачів інформаційних систем за рахунок

використання передобчислень і прив’язки складової відкритого ключа системи до номеру сеансу взаємодії.

1.2.2 Цілі і задачі розробки

Мета проекту полягає в підвищенні ефективності ідентифікації віддалених користувачів інформаційних систем за рахунок прискорення його обчислювальної реалізації шляхом використання передобчислень та забезпечення підвищеного рівня захисту прав доступу до ресурсів інформаційної системи шляхом застосування криптографічно строгої технології, основаної на концепції нульових знань з блокуванням повторного використання перехоплених третьою стороною сеансових паролів.

Розробка призначена для прискорення ідентифікації віддалених користувачів інформаційних систем, які надають на комерційній основі визначені інформаційні ресурси. Прискорення процесу ідентифікації досягається за рахунок використання передобчислень, які залежать тільки від відкритого ключа криптографічного механізму ідентифікації.

Для досягнення поставленої мети необхідно вирішити такі завдання: аналіз існуючих рішень, розробка алгоритму строгої ідентифікації користувачів віддалених інформаційних систем, що задовольняє усім вимогам сучасного етапу розвитку інформаційних систем, розроблення інформаційної системи ідентифікації віддалених користувачів, розробка класів даних і тестування самого алгоритму.

Висновок до розділу 1

В результаті виконання досліджень сучасного стану ідентифікації учасників віддаленої інформаційної взаємодії та аналітичного огляду існуючих схем ідентифікації, які складають перший розділ бакалаврського проєкта можуть бути сформульовані наступні висновки:

Аналіз показав , що у сучасних умовах зростання кількості видів атак, існує потреба використання більш потужних криптографічних механізмів ідентифікації. Проте, разом з розширенням сфер використання, стрімким збільшенням кількості користувачів що перебувають в системі в режимі реального часу і вимогами до обробки даних під час безпосередньо етапу ідентифікації їх у системі, проблема забезпечення високої швидкодії дистанційної інформаційної взаємодії стала критично важливою, вимагаючи впровадження інноваційних рішень для оптимізації обчислювальних процесів. Виходячи з наведеного, у сучасних умовах забезпечення надійної та ефективної віддаленої інформаційної взаємодії вимагає розробки нових протоколів ідентифікації користувачів, які забезпечать одночасно посилений криптографічний захист та підвищену швидкодію. У цьому контексті є нагальна потреба у знаходженні компромісного рішення для протиріччя між забезпеченням відповідності сучасним вимогам криптографічного захисту та підвищенням швидкодії при розробці нових методів ідентифікації. Такі методи повинні ефективно інтегруватися в існуючі системи, гарантувати їхню надійність і ефективність у процесі віддаленої інформаційної взаємодії.

2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

2.1Класифікація існуючих методів ідентифікації

Існують два основні класи методів ідентифікації [8]:

— криптографічно слабка ідентифікація – забезпечує дуже високу швидкодію і малі вимоги до пам’яті, проте втрачає у рівні захищеності;

— криптографічно строга – ідентифікація що може забезпечити найбільш повний захист від усіх видів атак.

Виходячи з вимог сформульованих раніше для поставленої задачі найбільш підходящим буде використовувати строгу ідентифікацію, яка відома як Zero Knowledge Identification [9]. Цей метод базується на трьох основних парадигмах. Згідно першої, користувач має криптографічні механізми для генерації правильних паролів. В рамках другої парадигми, система має криптографічні механізми для перевірки правильності паролів і немає можливості генерувати їх самостійно. Відповідно до третьої парадигми паролі мають змінюватись кожен сеанс взаємодії.

Деякі джерела виділяють також клас напівстрогої ідентифікації типу UNIX [10]. Проте при детальному розгляді таких ідентифікацій можна помітити що вони не надають повного захисту від атак і скоріше наділені якостями криптографічно слабких ідентифікацій. Такі методи можуть забезпечити захист лише від деяких видів атак на систему, оскільки в пам’яті системи паролі зберігаються не в явному вигляді, а в хешованому, табто сам пароль відновити неможливо. Проте, головним недоліком методів по типу UNIX являється використаня постійного паролю, що дозволяє зловмиснику використовувати пасивні атаки для його отримання.

Більшість наявних систем віддаленої ідентифікації користувачів що відповідають вимогам до рівня захищеності сучасності є концепція що базується на підтвердженні користувачем знання певної інформації. Наприклад, при застосуванні ідентифікації, що відповідає принципам теоретичної концепції “нульового розголошення”, інформація знання якої має підтвердити користувач представлена

секретним ключем, який використовується для створення правильних паролів абонента.

До критеріїв ефективності процедур віддаленої ідентифікації користувачів відносять стійкість системи до спроб несанкціонованого доступу до неї з боку незаконних користувачів [11], які можуть нелегально отримувати послуги і ресурси системи.

Одним з найскладніших для оцінки ефективності критерієм є рівень захищеності що надає процедура ідентифікації. Криптографічно нестрога і строга ідентифікації мають різні схеми підходу до оцінки ефективності за цим критерієм. Для систем що не задовольняють принципам криптографічно строгої ідентифікації для оцінки рівня захищеності перевіряється складність перехоплення незмінного пароля абонента. Тоді як для строгої ідентифікації, що відповідає принципам Zero Knowledge рівень захищеності визначається як об'єм затрачених ресурсів для незворотного перетворення що використовується для генерації коректних паролей. Математичною основою можуть стати як незворотні перетворення теорії чисел, так і незворотні перетворення мулевої алгебри.

Більшвсть схем ідентифікації складаються з двох принципових етапів:

— ініціалізація – користувач генерує певну секретну інформацію що буде використовуватись для генерації правильних паролей. Після цього користувач передає системі певну секретну інформацію з використанням відкритого ключа системи. Для криптографічно слабкої ідентифікації користувач надає системі правильний пароль або на пряму, або в зашифрованому виді. Для строгої ж ідентифікації в якості цієї інформації виступає публічний ключ для перевірки системою коректності згенерованих користувачем сеансових паролей;

— перевірка абонента на права доступу – етап коли система має пересвідчитись чи користувач дійсно володіє знанням секретної інформації.

2.2 Огляд методів криптографічно строгої ідентифікації

На сьогодні запропоновано досить багато методів криптографічно строгої ідентифікації. Способи реалізації zero-knowledge ідентифікації, залежно від математичної бази, покладеної в їхню основу, як зазначалось раніше, можна розділити на дві основні групи: на основі необоротних перетворень булевої алгебри та на основі необоротних перетворень теорії чисел [12].

Більш швидким способом виконання стргої ідентифікації є методи, засновані на необоротних перетвореннях булевої алгебри, які, своєю чергою, можуть бути реалізовані на основі ланцюжка паролів або на основі хеш-перетворень з програмованими колізіями.

Фактично, якщо при застосуванні незалежних сеансових паролів користувач доводить, що він той самий, який здійснював авторизацію в системі на стадії ініціалізації, то при застосуванні ланцюжків коректних паролів абонент доводить те, що він той самий, який взаємодіяв з віддаленою системою в попередньому сеансі дистанційної взаємодії.

Перша схема ідентифікації на основі незворотних булевих перетворень, що задовольняє вимоги Zero Knowledge, описана в роботі [13]. Цей метод використовує стандартизоване хеш-перетворення, наприклад SHA-256 або RIPEMD-160, як незворотне булеве перетворення. Перед початком авторизації абонент випадковим чином вибирає початковий сеансовий пароль P_i. Потім послідовно генерується серія з i сеансових паролів P_{i-1} , P_{i-2} , …, P_1, P_0, де кожен попередній пароль P_j отримується шляхом застосування хеш-перетворення до наступного пароля P_{j+1}: $P_j = H(P_{j+1})$ для $j \in \{0,1,...,i-1\}$j. Таким чином, користувач має i сеансових паролів, згенерованих у зворотному порядку, де кожен з них є результатом хешування попереднього.

Цей метод забезпечує високий рівень надійності завдяки перевіреній незворотності хеш-перетворень, таких як SHA-256 або RIPEMD-160, яка підтверджена багаторічною практикою. Додатковою перевагою є висока швидкість обчислення

і можливість апаратної реалізації на сучасних криптопроцесорах, що дозволяє забезпечити швидку ідентифікацію.

У роботі [14] запропоновано та теоретично обґрунтовано схему ідентифікації, що базується на незворотних булевих перетвореннях і відповідає парадигмам “Zero-Knowledge”. Схема використовує ланцюжок взаємопов’язаних коректних сеансових паролів та стандартизовані шифроблоки типу DES або AES. Ключовими перевагами цього методу є забезпечення високої швидкості ідентифікації користувача в системі, з одночасним підвищенням рівня захищеності, що забезпечується за допомогою додаткового контролю номера сеансу і додаткової функції ідентифікації.

Тобто, в обох вищеописаних схемах строгої ідентифікації, поточний сеансів пароль застосовується в якості перевірки автентичності користувача для наступного сеансу ідентифікації. Фактично користувач має довести системі, на основі зв’язків між паролями, що саме він виконував минулий вхід до системи. За забезпечення певного рівня захисту від атак у цих схемах, а саме незворотність цього перетворення, відповідає шифроблок, розроблений з використанням нелінійних булевих функцій. Значна перевага цих схем полягає в тому, що шифроблоки є стандартизованими і добре досліджені. Відповідно ці шифроблоки є добре захищеними і передбачають можливість їх апаратної реалізації.

Ще один метод ідентифікації на основі незворотних булевих перетвореннях, що відповідає відповідає парадигмам “Zero-Knowledge”, запропоновано в роботі [14]. В якості незворотного перетворення на булевих нелінійних функціях тут застосовано стандартизовані генератори псевдовипадкових двійкових послідовностей. Цей метод дозволяє в 3-4 рази пришвидшити обчислення в порівнянні із запропонованими раніше методами криптографічно строгої ідентифікації. Важливою перевагою цього методу є його можливість ефективного застосування для вторинної ідентифікації або потокового шифрування даних, що передаються між віддаленим користувачем і системою. Це забезпечує надійний захист від серединних атак шляхом запобігання витісненню легітимного користувача із сеансу віддаленої взаємодії.

Недоліками запропонованих методів строгої ідентифікації є те, що кількість сеансових паролей є обмежена і має бути згенерована заздалегідь. Також проблемою є й те, що весь ланцюжок має зберігатися в пам'яті, що робить ці схеми більш чутливими до атак. Відповідно ці методи є достатньо чутливими до синхронізації, що також може бути використано з метою отримання незаконного доступу до системи.

Цих недоліків позбавлені методи строгої ідентифікації що базуються на основі незворотніх перетворень теорії чисел. Найвідомішими з яких є всім відомі FESIS, Guillou-Quisquater і Schnorr. Основною операцією в усіх згаданих методах є піднесення числа *A*, розрядністю 4096 і більше, в ступінь *E* по модулю *M*. Відмінність між цими методами полягає в тому, що FESIS передбачає виконання модулярного експоненціювання розподіленого в часі між пересилками обміну даними між користувачем та системою, тоді як два інші виконують цю операцію в явному вигляді.

Ключовим методом що береться за основу в запропонованій роботі являється схема Шнорра. Умовно, ідентифікацію за допомогою цієї схеми можна поділити на два етапи: реєстрацію, на якій відбувається генерація усіх необхідних значень, і, безпосередньо, ідентифікацію.

Процедура авторизації в схемі Шнорра [15] виконується лише раз і передбачає виконання наступної послідовності кроків:

1) користувач обирає велике просте n-розрядне число p.Користувач обирає просте число q, таке що, $p - 1$ націло ділиться на q;

2) користувач обирає не рівне одиниці значення числа a, що задовольняє наступну рівність: $a^q mod p = 1$;

3) користувач обирає довільне число s, що є меншим від q : $s < q$, в якості секретного ключа;

4) користувач обраховує значення закритого ключа v як мультиплікативну інверсію до a^s, використовуючи формулу: $v = a^{p-1-s} = a^{-s} mod p$;

5) користувач шифрує відкритим ключем системи значення p, v і a, і надсилає їй їх;

6) система розшифровує своїм секретним ключем надіслані користувачем значення p, v і a і зберігає отриману інформацію у пам'яті.

В ході виконання процедури реєстрації в пам'яті користувача зберігатимуться значення p, q, a, s, а в системи значення p, v і a.

Відповідно до п.1 і п.2 описаної процедури реєстрації p обирається рівним 83: $p = 83$, а q рівне 41: $q = 41$. В рамках п.3, користувач обирає значення a = 11, оскільки воно задовольняє умову $11^{41} mod 83 = 1$. В межах п.4, користувач обирає $s = 21$, в якості приватного ключа. Відповідно до п.5, користувач обраховує значення приватного ключа $v = 11^{-21} mod 83 = 63$. В межах п.6 користувач шифрує відкритим ключем системи значення $p = 83$, $v = 63$ і $a = 11$ і надсилає їй їх. В рамках п.7 система розшифровує і зберігає надіслані користувачем дані. В ході виконання процедури реєстрації в пам'яті користувача зберігатимуться значення p = 83, q = 41,a = 11, s = 21, а в системи значення p = 83, v = 63, a = 11.

Використовуючи дані отримані в рамках процедури реєстрації, процедура ідентифікації користувача в системі передбачатиме наступну послідовність дій:

1) користувач обирає випадкове значення r, що є меншим від q;

2) користувач, обраховує значення x по формулі $x = a^r mod p$ і надсилає його системі;

3) система обирає з діапазону від 0 до 2^{t-1} значення e і надсилає його користувачеві;

4) користувач обраховує значення y за формулою $y = (r + s \cdot e) mod q$ і надсилає його системі;

5) система, обраховує значення x' по формулі $x' = a^y \cdot v^e mod p$;

6) система порівнює значення x та x'. Якщо x рівне x', система надає дозвіл на подальшу взаємодію.

В методі Шнорра процедура ідентифікації ілюструється наступним прикладом.

В межах п.1, в якості r обрано число 6: $r = 6$. Згідно з п.2, користувач обраховує значення x і надсилає його системі: $x = 11^6 mod 83 = 9$. В рамках п.3, запропонованої процедури ідентифікації, система обирає e рівне 4: $e = 4$. Згідно з п.4, користувач обчислює значення y по формулі: $y = (6 + 21 \cdot 4) mod 41 = 8$ і надсилає його системі. В межах п.5 система, обраховує значення $x' = 11^8 \cdot 63^4 mod 83 = 9$. Відповідно до п.6 система порівнявши значення $x = x' = 9$, система дає дозвіл на подальшу взаємодію.

Популярність отримали і модифікації схеми Шнорра, зокрема, схема Шнорра є широко розповсюджена для отримання електронно цифрового підпису. Єдина відмінність цих двох типів використань полягає в тому, що користувач робить хеш перетворення над конкатенацією свого повідомлення L і обрахованого значення x.

Перевагою цього методу криптографічно строгої ідентифікації стала його ефективність, оскільки при достатньо високій обчислювальній швидкості він показує хороший рівень криптостійкості, проте, цей метод, також має ряд недоліків, які може усунути його модифікація.

Захищеність цієї схеми базується на складності обрахунку дискретних логарифмів, що в свою чергу робить її стійкою до більшості видів кібер атак, включаючи атаки на основі квантових обчислень. Крім того, ця схема має важливу перевагу над іншими криптографічними алгоритмами: вона дозволяє генерувати короткі підписи, що сприяє зменшенню обсягу даних що передаються, це особливо важливо в умовах обмежених ресурсів і підвищених вимог до швидкості обробки інформаціїї.

Проте, незважаючи на всі переваги, схема Шнорра має ряд суттєвих недоліків, які обмежують її застосування в умовах сучасних вимог до безпеки ідентифікації користувачів. Одним із головних викликів є її вразливість до атаки повторного відправлення правильного паролю, згенерованого під час попередніх сеансів ідентифікації. Ще однією проблемою, яка може послабити ефективність цієї схеми, є ризик генерації слабких або недостатньо випадкових чисел. Також, схема Шнора не захищає від спроби системи імітувати доступ до неї.

Крім схеми Шнорра широкого розповсюдження отримав і метод FESIS.

Метод FESIS полягає в тому, що на етапі реєстрації користувач обирає два великих простих числа p і q, на основі яких формує значення модуля M, $M = p \cdot q$. Наступним кроком, користувач обирає випадкове число n і обчислює значення відкритого ключа v, як квадрат цього числа по модулю M: $v = n^2 \bmod M$. Тоді, користувач обраховує v^{-1} ,мультиплікативну інверсію числа v, таку, що $v \cdot v^{-1} \bmod M = 1$. Тоді користувач підбирає закритий ключ s, як найменше ціле число, що задовольняє наступне рівняння $v^{-1} = s^2 \bmod M$.

В рамках процедури ідентифікації в запропонованому методі користувач обирає випадкове значення r і обчислює двокомпонентний сеансовий пароль у вигляді модулярного добутку $W_1 = s \cdot r \bmod M$ та модулярного квадрату $W_2 = r^2 \bmod M$. Коди обох компонентів сеансового паролю W_1 та W_2 надсилаються системі, яка обчислює $K = W_1^2 \cdot v \bmod M$ і порівнює обчислене значення з W_2. Якщо $K = W_2$, то ідентифікація вважається успішною.

Недоліком розглянутої схеми криптографічно строгої ідентифікації FFSIS є необхідність виконання 10–12 циклів ідентифікації через мережеві канали Інтернету. Така особливість зумовлює потенційне зниження ефективності процесу ідентифікації, оскільки збільшення кількості циклів може істотно впливати на його швидкість залежно від стану мережевого трафіку. Крім того, вразливістю цієї схеми є можливість атак на рівні каналу передачі даних, що відкриває широкий спектр загроз, які можуть спричинити дискредитацію запропонованого методу.

Таким чином, існуючі методи ідентифікації віддалених абонентів, що відповідають критеріям концепції нульового розголошення не в повній мірі задовольняють вимогам сучасного стану розвитку систем віддаленої інформаційної взаємодії. Відповідно, ці методи, недоцільно використовувати в системах що вимагають найвищого рівня захисту інформації.

З урахуванням вищезазначених аспектів, питання створення ефективного і безпечного методу ідентифікації користувачів у системах залишається надзвичайно актуальним і сьогодні. Вирішення цієї проблеми вимагає розробки нових під-

ходів, які здатні враховувати сучасні загрози і водночас забезпечувати компроміс між безпекою, ефективністю та зручністю використання.

Метою дослідження є удосконалення криптографічно строгої ідентифікації віддалених користувачів шляхом оптимізації обчислювальних процесів та запобігання повторному використанню сеансових паролів, що в свою чергу підвищує її рівень захищеності.

Висновок до розділу 2

В результаті проведених досліджень, які складають другий розділ бакалаврського проєкта і направлені на аналіз сучасного стану ідентифікації віддалених користувачів інформаційних систем з позицій сформульованих вище сучасних вимог, можуть бути зроблені наступні висновки:

В сучасних умовах розширення використання інформаційних систем на сфері застосування,які вимагають підвищеного рівня безпеки, домінуючою вимогою до систем ідентифікації є забезпечення високого рівня захищеності який потенційно може бути досягнений лише в рамках застосування криптографічно строгих методів ідентифікації, що базуються на теоретичній концепції нульових знань.

Способи реалізації ідентифікації за принципом zero-knowledge, залежно від математичної основи, покладеної в їх основу, можуть бути розділені на дві основні групи: на основі необоротних перетворень теорії чисел і на основі необоротних перетворень булевої алгебри. Перевагою першої групи є можливість користувача генерувати необмежену кількість правильних паролів, оскільки кожен новий пароль є незалежним від попереднього. Однак через високу складність обчислень математичних операцій, на яких базується цей метод, спостерігається досить низька швидкодія, яка не задовольняє сучасним вимогам ефективного функціонування інтегрованих інформаційних систем з великою кількістю віддалених користувачів, що функціонують в режимі реального часу.

Більш швидким способом реалізації строгої ідентифікації є методи, засновані на необоротних перетвореннях булевої алгебри, які, своєю чергою, можуть бути реалізовані на основі ланцюжка паролів або хеш-перетворень із програмованими колізіями. Недоліком ланцюжка паролів є заздалегідь визначена максимальна кількість ідентифікацій користувача в системі, тобто обмежена кількість пов'язаних паролів. Цього недоліку позбавлені методи на основі хеш-перетворень, однак сама процедура формування паролів у них є досить складною.

Таким чином, існуючі методи ідентифікації віддалених абонентів, що відповідають критеріям концепції нульового розголошення не в повній мірі задовольняють вимогам сучасного стану розвитку систем віддаленої інформаційної взаємодії. Це робить сучасні системи ідентифікації вразливими майже до всіх видів атак на них.

Виходячи з цього, метою дослідження є удосконалення криптографічно строгої ідентифікації віддалених користувачів шляхом оптимізації обчислювальних процесів та запобігання повторному використанню сеансових паролів, що в свою чергу підвищує її рівень захищеності.

3 ФОРМУВАННЯ ВИМОГ ДО СИСТЕМИ

3.1 Вимоги до системи в цілому

Для забезпечення коректної роботи розробленої інформаційної системи ідентифікації віддалених користувачів, і проведення якісних тестів направлених на вирішення проблеми пришвидшення роботи процедури ідентифікації необхідно розробити консольний додаток на мові програмування C++. Ця мова забезпечує високий рівень контролю над ресурсами при цьому дозволяючи написати швидкий машинний код без додаткових заповільнень спричинених використанням тяжких бібліотек.

3.2 Вимоги до функціональних характеристик

Для забезпечення якісної роботи системи ідентифікації віддалених користувачів необхідно гарантувати виконання певного переліку функціональних вимог. Результати наведені у таблиці 3.1

Таблиця 3.1 – Перелік функціональних вимог та їх пріоритети

Функціональна вимога	Пріоритет
Система надає інформаційні ресурси віддаленим користувачам на комерційній основі	Середній
Доступ до ресурсів системи здійснюється за допомогою генерації та надсилання віддаленими користувачами сеансових паролів	Високий
Сеансові паролі мають змінюватись при кожному зверненні до системи	Середній

Продовження таблиці 3.1

Система має криптографічний механізм для перевірки правильності користувацького паролю	Високий
Система нездатна генерувати правильний користувацький пароль	Середній
Користувач має криптографічний механізм генерації правильних паролів	Всокий
Користувацький пароль не може бути використаний повторно	Середній
Робота механізму ідентифікації користувачів віддаленої інформаційної системи має мати високою швидкодію для забезпечення можливості одночасного обслуговування системою великої кількості віддалених користувачів, створення можливостей для високого рівня оперативності інтерактивної взаємодії віддаленого користувача системи	Високий
Надійний захист від атак спрямованих на перехоплення користувацького паролю і його повторного використвння	Всокий
Забезпечення можливості реалізації захисту від middle attack	Середній

3.3. Вимоги до видів забезпечення

3.3.1 Вимоги до видів забезпечення

Передбачена реалізація підсистеми ідентифікації віддалених користувачів інтегрованої інформаційної системи, яка надає визначені інформаційні ресурси на комерційній основі в режимі колективного доступу має вигляд консольного додатку, компоненти якого працюють як на стороні користувача, так і на стороні системи.

Інформаційна система надає на комерційній основі інформаційні ресурси незалежним віддаленим користувачам в режимі реального часу з використанням глобальної мережі Інтернет. Розрахункова кількість віддалених користувачів не перевищує 5000. За статистичними дослідженнями математична модель потоку заявок на обслуговування віддалених користувачів інформаційною системою являє собою локально стаціонарний потік Пуассона з інтенсивністю 400 запитів на обслуговування на хвилину. Для забезпечення ефективного інтерфейсу інформаційної системи з віддаленими користувачами в режимі реального часу, час ідентифікації має не перевищувати 0.1 секунди.

Оскільки надання інформаційних ресурсів системою надається на комерційній основі, існує мотивація для спроб незаконного доступу до ресурсів інформаційної системи. Для протидії спробам підбору сеансових паролів, розрядність сеансових паролів, які мають змінюватися в кожному циклі ідентифікації віддаленого користувача має бути 512 біт. Для ефективної протидії спробам отримання несанкційного доступу до ресурсів інформаційної системи або розширення прав доступу легальниит користувачами, а також з метою протидії потенційно можливим спробам системи імітувати звернення користувача та отримання ним інформаційних ресурсів з метою отримання незаконної комерційної вигоди, ідентифікація віддалених користувачів має бути криптографічно строгою, тобто відповідати теоретичній концепції “нульових знань”.

Для ефективної протидії спробам перехоплення сеансових паролів легальних користувачів з метою їх повторного використання для отримання незаконного

доступу до ресурсів інформаційної системи підсистема криптографічно строгої ідентифікації має реалізувати блокування повторного застосування тих сеансових паролів, які були раніше використані легальними користувачами. Крім того, задля протидії middle-атакам, які полягають в витісненні легального користувача з сеансу дистанційної взаємодії після його ідентифікацією системою, в проектованій підсистеми криптографічно строгої ідентифікації мають бути передбачені механізми повторної ідентифікації, що проводяться безпосередньо під час сеансу віддаленої взаємодії користувача та інформаційної системи.

3.3.2 Технічні вимоги

Інформаційна система має бути реалізована у вигляді Desktop додатку, що здатний працювати на будь-якій операційній системі, браузері та програмному забезпеченні. Для забезпечення ефективного функціонування розробки на стороні системи, остання має реалізовуватися на сучасному потужному сервері. Процесор сервера 2 x Intel XEON 6 Core E5-2630 V3 (2.4 GHz-3.20GHz) DDR4-1866, криптопроцесор T7456, оперативна пам'ять 8GB DDR4 ECC 2133 Mhz. Обєм флеш-пам’яті для зберігання таблиць передобчислень – не менша 8 Тбайт. Програмні вимоги: – операційна система ОС Windows 10.

На стороні користувача обчислювальна платформа – ноутбук з операційною системою ОС Windows 10, з процесором Intel Core i3 або AMD з частотою не нижче 2,5 ГГц. Це дозволить системі швидко обробляти дані і виконувати задачі; – оперативна пам'ять: мінімум 8 ГБ оперативної пам'яті рекомендується для ефективної роботи системи та оброблення великого обсягу даних; – місце на жорсткому диску: мінімум 1 ГБ вільного місця для стабільної роботи та збереження даних.

Висновок до розділу 3

В результаті напрацювань, які складають третій розділ бакалаврського проєкту, можуть бути зроблені наступні висновки:

Інформаційна система надає на комерційній основі інформаційні ресурси незалежним віддаленим користувачам в режимі реального часу з використанням глобальної мережі Інтернет. Розрахункова кількість віддалених користувачів не перевищує 50 тисяч. Потік заявок на обслуговування підпорядковано потоку Пуассона з інтенсивністю 400 запитів на обслуговування на хвилину. Відповідно, для забезпечення ефективної дистанційної взаємодії користувачів з системою в режимі реального часу час ідентифікації має не перевищувати 0.1 секунди.

Оскільки надання інформаційних ресурсів системою надається на комерційній основі, існує мотивація для спроб незаконного доступу до ресурсів інформаційної системи. Для протидії спробам незаконного отримання доступу до ресурсів системи сторонніми особами, чи розширення прав доступу за межі зумовлених прав з боку легальних користувачів, а також з метою протидії потенційно можливим спробам системи імітувати звернення користувача та отримання ним інформаційних ресурсів з метою отримання незаконної комерційної вигоди, ідентифікація віддалених користувачів має бути криптографічно строгою, тобто відповідати теоретичній концепції “нульових знань”.

Для протидії спробам перехоплення сеансових паролів легальних користувачів з метою їх повторного використання для отримання незаконного доступу до ресурсів інформаційної системи підсистема криптографічно строгої ідентифікації має реалізувати блокування повторного застосування тих сеансових паролів, які були раніше використані легальними користувачами.

Для ефективної протидії middle-атакам, які полягають в витісненні легального користувача з сеансу дистанційної взаємодії після його ідентифікацією системою, в проектованій підсистеми криптографічно строгої ідентифікації мають бути передбачені механізми повторної ідентифікації, що проводяться безпосередньо під час сеансу віддаленої взаємодії користувача та інформаційної системи.

4 ВИБІР ТЕХНОЛОГІЇ РОЗРОБКИ

Важливим чинником ефективності програмного продукту що розроблюється є організація даних. В структурному плані існує декілька варіантів організації даних які відрізняються в таких показниках як: простота реалізації функцій та методів, об’єм задіяної пам’яті та часовими характеристиками. Важливим аспектом вибору організації даних є за діяння в найбільшій мірі всіх можливостей мови програмування С++. В свою чергу, вибір мови програмування, С++, як інструменту створення програмного продукту зумовлений тим, що в рамках цієї мови можна найбільш ефективно використовувати можливості апаратних засобів комп’ютерної системи. В силу того, що базовим показником ефективності розробленої системи є швидкодія, важливим є за діяння всіх можливостей апаратних засобів. Для цього потрібно забезпечити високу якість об’єктного коду програми в ракурсі як її об’єму, так і часових характеристик реалізації. З огляду на це, найбільш ефективним інструментом створення програмного продукту є мова програмування С++, яка відрізняється від інших саме високими якісними характеристиками об’єктного кода програми.

В якості середовища розробки програмного забезпечення на мові С++ використано Visual Studio Code. Програмний інтерфейс середовища розробки Visual Studio Code зображено на рисунку 4.1. Це середовище розробки має багато переваг, серед яких вирізняються легкий, але потужний редактор коду, інтерактивність взаємодії з користувачем та підтримка великої кількості мов програмування з можливістю підключення різноманітної кількості бібліотек. Невід’ємною перевагою Visual Studio Code є те що цей продукт являється безкоштовним та розроблений компанією Microsoft, що в свою чергу дозволяє ефективно застосовувати їхні навчальні посібники по мові С++ та середовищу розробки Visual Studio Code.

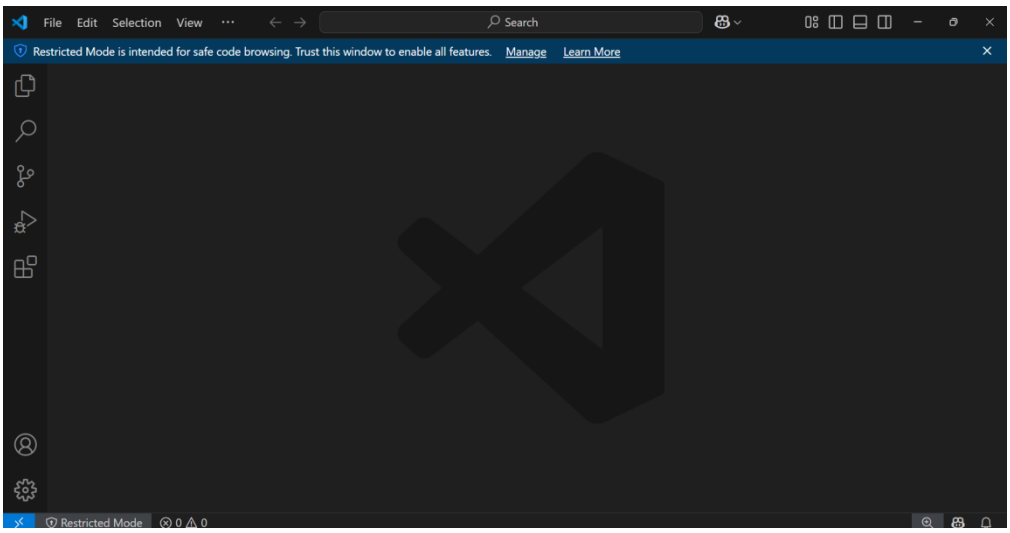

Рисунок 4.1 – Інтерфейс Visual Studio Code

Для розробленого програмного продукту на мові програмування C++, було задіяно наступні бібліотеки:

— iostream: базова бібліотека C++, розроблена спеціально для ефективного зчитування та запису інформації на зовнішній носій зберігання даних. Ця бібліотека надає можливості вводу та виводу різних типів даних за допомогою стандартного простору імені std;

— cmath: незамінна для більшості математичних обрахунків бібліотека. Вона надає можливості обчислення всіх видів тригонометричних функцій, експоненціювання та логарифмічних функцій. З повноспектровим використанням функціоналу бібліотеки cmath досягається створення значно спрощеного для сприйняття людині програмного коду.

Для досягнення поставленої мети - розробка системи яка дозволяє виконувати модулярне експоненціювання над числами розрядності, які значно перевищують розрядність процесора, проаналізовано значну кількість можливих підходів до реалізації системного рішення. Головним критерієм до вибраного підходу була ефективність роботи готового системного продукту, що суттєво вплинуло на прийняття рішень.

Висновок до розділу 4

В результаті виконання дослідження можливих варіантів вибору технологій розробки інформаційної системи з криптографічно строгою ідентифікацією великої кількості віддалених користувачів, які складають зміст четвертого розділу бакалаврського проєкту можна зробити наступний висновок:

В силу того, що запропонований метод криптографічно строгої ідентифікації віддалених користувачів інформаційної системи потребує складних обчислень, що виконуються над числами великої розрядності, що на порядок перевищує розрядність процесору, мова програмування має надавати змогу використовувати всі можливості процесорної платформи. Відповідно, мова програмування має надає можливість працювати з асемблерними вставками, які дозволяють ефективно реалізувати роботу з багатосекційними числами.

Виходячи з того, що на боці інформаційної системи потрібно забезпечити найбільшу швидкість реалізації криптографічно строгої ідентифікації задля можливості обробки запитів великої кількості дистанційно-віддалених користувачів в режимі реального часу, а також задля запобігання ефективним middle-атакам, потрібно забезпечити максимальне використання можливостей процесору серверну. Для цього, потрібно обрати такі технології програмування, які надають змогу ефективно організувати паралельну роботу на сучасних багатоядерних процесорах.

Оскільки передбачені запропонованим методом обчислення передбачають часте звернення до таблиць, технології розробки програмного продукту мають забезпечувати високу ефективність роботи з пам’яттю і дозволяти напряму керувати розміщенням даних таблиць по рівням комп’ютерної пам'яті, включаючи швидкодіючу кеш-пам'ять.

5 РОЗРОБЛЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

5.1 Структура системи

Клас long_numbers

Відповідає за зберігання й базові операції над “довгими” числами розрядністю до 2048 біт. Всередині він тримає три поля: ціле n, яке визначає фактичну розрядність, масив MOD з 32 цілих по 32 біт — незмінний модуль, і масив number того ж розміру — власне значення числа. Обидва масиви розглядаються як підрядкові слова великого числа, але дійсний діапазон бітів обмежується значенням n. Приватно клас реалізує два допоміжні методи: ADDMOD, який додає до number значення MOD з урахуванням переносів, і SubMOD, який віднімає MOD, також із врахуванням переносів і боргу. Ці методи не приймають параметрів і не повертають значень, бо змінюють стан об’єкта безпосередньо.

Публічний інтерфейс включає:

— конструктор із параметром розрядності, який встановлює n та обнуляє обидва масиви;

— метод check_Number, що повертає true, якщо число менше модуля, і false в протилежному разі;

— методи input_long_number і input_long_number_manually для заповнення масиву number з готового масиву або з термінала (в hex-коді з перетворенням у двійковий вигляд);

— метод output_long_number, що виводить число в шістнадцятковому форматі від старших розрядів до молодших;

— copy_Array для копіювання вмісту одного масиву в інший; copy_module_to_number, який переносить MOD у number;

— оператори зсувів (>>= та <<=) для двійкових зсувів масиву number вправо та вліво на задану кількість біт;

— оператори арифметики (+=, -=, *=) для додавання, віднімання й множення Монтґомері над двома об’єктами long_numbers. Реалізація множення включає цикл по бітах множника, додавання з урахуванням MOD та кінцеву редукцію;

— додаткові допоміжні методи last_bit_number і last_bit_module для пошуку найвищого встановленого біта, а також nbm як внутрішній інструмент при порівняннях.

Клас exponentiation

Призначений для модульного експоненціювання великих чисел за алгоритмом Монтґомері. Має одне поле n — розрядність чисел, яка потрібна для побудови початкових Montgomery-параметрів.

Відкриті методи:

— конструктор, який просто зберігає значення n;

— reduction, що приймає об’єкт long_numbers і виконує звичайну редукцію поки число вищезначне за модуль, зсуває копію модуля на різницю в бітах і віднімає його;

— exponentiation, який бере два об’єкти long_numbers: базове число A і степінь E. Спочатку обчислює допоміжні значення $P = 2^n \bmod M$ та $C = P^2 \bmod M$, потім організовує цикл від старшого біта E до молодшого, на кожній ітерації робить квадрат результату та, якщо поточний біт E = 1, множить на C. Після завершення застосовує звичайну редукцію й повертає остаточний результат.

Клас table_exp

Розширює можливості exponentiation за рахунок кешування попередніх степенів для пришвидшення повторних піднесень до ступеня. Містить три поля: n — розрядність, A — базове число як long_numbers і динамічний масив table довжини n, де table[i] зберігає $A^{(2\wedge i)} \bmod M$.

Відкриті методи:

— конструктор, який ініціалізує table: на першому кроці table[0] = A, далі для кожного i від 1 до n−1 будує table[i] як результат квадрату table[i−1] методом MONT(table[i−1], table[i−1]);

— out_put_Table, який виводить усі значення кешу в шістнадцятковому форматі для перевірки;

— exponentiation, що приймає степінь E, ініціалізує result як “1” (копіює модуль у number), пробігає всі біти E і, якщо біт і рівний 1, виконує result = MUL(result, table[i]).

Таким чином, замість повного алгоритму Montgomery кожного разу використовує вже обчислені частини. Структурна схему експоненціювання представлена на кресленику ІС12.020БАК.005 Д1.

5.2 Функціональна модель системи

Дійовою особою в запропонованій інформаційній системі являється віддалений користувач. Тоді як головна ціль самої системи полягає в його ідентифікації. Діаграма варіантів використання представлена на кресленику ІС12.020БАК.005 Д2.

Запропонований кресленик ілюструє

a) при першому зверненні до системи користувач ініціалізує процедуру реєстрації;

b) користувач реєструє у системі свій публічний ключ, що є парою до його приватного ключа і зберігає його на боці системи;

c) користувач через клієнтський додаток ініціює ідентифікацію;

1) користувач відправляє системі запит на видачу одноразового випадкового числа — r;

2) система генерує challenge e, ґрунтуючись на отриманому r, і повертає його клієнту;

3) користувач обирає випадкове значення k, обчислює проміжну величину t = g^k і передає її системі;

4) за отриманим значенням e Користувач обчислює відповідь s = k + e·x, де x — його приватний ключ, і надсилає s системі;

d) система перевіряє автентичність користувача, оцінюючи, чи виконується перевірочна рівність протоколу модифікованого метода Шнорра.

Якщо це співвідношення коректне, Система вважає, що запит дісно надійшов від власника приватного ключа, і запускає процедуру “Issue Token” — видає користувачу одноразовий токен доступу до захищеного ресурсу.

Завдяки одноразовим значенням r і e (nonce та challenge), ця модифікація протоколу Шнора запобігає атакам відтворення і гарантує, що жодна третя сторона не зможе зімітувати відповідь s без знання секретного ключа x. Така схема ідеально інтегрується в системи, які видають токени віддаленим користувачам після успішної криптографічної перевірки.

5.3 Структура масивів інформації

Була розроблена структура масивів інформації, яка зберігає інформацію про передобчислення. Структура масивів інформації представлена на кресленику ІС12.020БАК.005 Д3.

Схема ілюструє трирівневу побудову рушія, який забезпечує усі необхідні операції для криптографії з великими цілими числами до 2048:

— long_numbers формує базовий рівень: зберігає саме число та модуль у вигляді масивів 32-бітових слів і реалізує елементарні дії – додавання, віднімання, логічні зсуви та швидке Montgomery-множення, що дозволяє виконувати добуток за модулем без апаратного ділення;

— exponentiation спирається на ці примітиви і реалізує експонентування за модулем методом «квадрат-та-множ» у просторі Montgomery, тобто забезпечує операцію A^E mod M з асимптотичною складністю $O(n^2)$ у словах замість традиційної $O(n^3)$;

— table_exp призначений для сценаріїв із фіксованою основою та змінними експонентами; він попередньо обчислює таблицю ступенів основи й, використовуючи віконну методику, дає додаткове 2–3-кратне прискорення повторних обчислень.

Стрілки «Використовує» відображають ієрархічну залежність: table_exp звертається до exponentiation, а той – до низькорівневих методів long_numbers

Така шарувата архітектура спрощує тестування, масштабування до більшої розрядності та адаптацію під SIMD/GPU, що робить модуль придатним для практичної реалізації алгоритмів RSA, Diffie-Hellman та цифрових підписів.

5.4 Передавання та обробка даних

В ході виконання бакалаврської роботи розроблена схема передавання та обробки даних. Схема передавання та обробки даних на рисунку представлена на кресленику ІС12.020БАК.005 Д4.

Інформаційна система з колективним доступом великої кількості віддалених користувачів, яка надає їм певні інформаційні ресурси на комерційній основі має забезпечити їх обслуговування в режимі реального часу. При цьому має забезпечуватися високий рівень захищеності від спроб незаконнного отрмання доступу до інформаційних ресурсів шляхом перехоплення паролю на серверах Інтернету. В самій системі не має зберігатися ніякої інформації, яка б давала змогу системі або особам, що мають доступ до її памяті самостійно генерувати коректні паролі легальних користувачів.

Відповідно, в структурному плані система має спецальну пам'ять даних користувачів, в якій в відкритому вигляді зберігається настпна інформація:

— ідентифікатор віддаленого користувача;

— відкритий пароль користувача;

— поточний хеш для блокування повторного використання паролів;

— таблиця передобчислень для відкритого ключа, яка дозволяє швидко обчислювати код доступу з використаннм незворотних перетворень теорії чисел;

— коди доступу до ресурсів системи.

Користувачі підлючаються до інформаційної системи через глобальну мережу Інтернет.

При зверненні віддаленого користувача до інформаційної системи, він за описаною процедурою генерує код сеансового паролю, який, разом з кодом ідентифікації пересилається інформаційній системі.

Система, по отриманню сеансового паролю, запускає криптографічний механізм його перевірки. Для цього обчислюється модулярна експонента постійного числа – відкритого ключа користувача, що зберігається в памяті системи. Після обчислення коду доступу, з використанням стандартизованого алгоритму SHA-256 по коду доступу і поточному хешу обчислюється нове значення коду хешу, яке порівнюється з надісланим користувачем. Права доступу до ресурсів надаються лише в разі співпадіння вказаних кодів.

5.5 Архітектура програмного забезпечення

Специфіка криптографії з відкритим ключем базовою операцією якої є медулярне експоненціювання над числами стандартною мінімальною розрядністю 4096 біт, створює значний виклик для розробника програмного забезпечення. Так, в представленому дипломному проекті цю задачу було вирішено за рахунок створення спеціального класу для роботи з довгими числами.

Клас long_numbers грає фундаментальну роль в розробленій системі. Він дозволяє зберігати числа розрядністю до 2048 біт, та виконувати над ними операції додавання, віднімання, множення та логічного зсуву праворуч, враховуючи специфіку роботи з такими числами. Додатковими можливостями класу long_numbers являється ефективний ввід та вивід довгих чисел розрядністю 2048 біт.

Організація даних в класі long_numbers продемонстрована на рисунку 5.1.

Масив даних MOD, типу unsigned int та розмірністю 32, виконує функцію зберігання модуля максимальною розрядністю 2048. Цей масив виступає приватним типом даних, оскільки не передбачає його зімну користувачем системного продукту. Це зумовлено особливістю модулярного експоненціювання, а саме незмінністю модуля при практичному використанні криптографії з відкритим ключем.

Масив даних number, типу unsigned int та розмірністю 32, виконує функцію зберігання числа максимальною розрядністю 2048. Цей масив виступає приват-

ним типом даних, оскільки його зміна реалізована за допомогою додаткових функцій вводу та виводу довгих чисел. Як і в попередньому масиві використано тип даних unsigned int, що зумовлено специфікою роботи з довгими числами, адже в C++ не існує типів даних розрядністю більше чотирьох біт. Такий недолік диктує необхідність сприймання масиву як одного числа, відповідно не передбачає від'ємних чисел в середині цього масиву.

Змінна n типу int передбачає зберігання розрядності числа в діапазоні від 1 до 2048. Ця змінна відіграє важливу роль в ефективності роботи системного продукту, оскілки дозволяє оброблювати не всю можливу розрядність, а ту, яка практично використовується.

Опис функцій і процедур класу long_numbers продемонстрована нижче

До приватних методів цього класу відносяться:

— void ADDMOD();

— void SubMOD().

Перший метод ADDMOD не повертає на вихід значень оскільки напряму працює з об'єктами класу long_numbers. З цієї ж причини метод не передбачає задавання параметрів. Всередині нього реалізовано бінарне додавання до числа значення модуля враховуючи переноси.

Другий метод SubMOD не повертає на вихід значень оскільки, як і попередник напряму працює з об'єктами класу long_numbers. З цієї ж причини метод не передбачає задавання параметрів. Всередині нього реалізовано бінарне віднімання від числа значення модуля враховуючи переноси.

Публічні методи цього класу представлені на рисунку 5.1:

```
long_numbers(int = 5);
  bool check_Number();
void input_long_number(unsigned int *);
void input_long_number_manually();
void output_long_number();
void copy_Array(unsigned int*,unsigned int*);
void copy_modele_to_number();
long_numbers operator>>=(int);
long_numbers operator<<=(int);
long_numbers operator+=(long_numbers);
long_numbers operator*=(long_numbers);
long_numbers operator-=(long_numbers);
long_numbers MUL(long_numbers,long_numbers);
int last_bit_number();
int last_bit_module();
int nbm(long_numbers,long_numbers, int,int);
```

Рисунок 5.1 – Публічні методи класу long_numbers

Перший метод – конструктор класу long_numbers з ідентичною назвою приймає на вхід параметр типу int, який відповідає за розрядність довгих чисел. Всередині цього методу значення розрядності чисел n – типу даних класу long_numbers присвоюється значення отриманого параметру. Для зручності всі елементи масивів long_number: number, MOD встановлюються в 0. Після чого, масиву MOD присвоюється його значення.

Другий метод - check_Number повертає false в випадку, якщо значення модуля більше за значення числа, в протилежному випадку, тобто числа менше модуля, метод повертає значення true.

Третій метод - inpute_long_number в якості параметру запрошує вказівник на початок масиву де зберігається число заданої в конструктор розрядності, після чого проводить запис наданого числа в змінну number.

Четвертий метод - inpute_long_number_manually дозволяє ввести довге число через термінал, безпосередньо самим користувачем. В методі реалізовано перетворення символів ASCII як значення шіснадцятеричної системи в двійкову систему, а також реалізований механізм виявлення найбільш можливих при вводі помилок.

П’ятий метод – output_long_number передбачає вивід довгого числа в «зручному» для сприйняття шіснадцятковому форматі. Вивід числа починається з старших розрядів і закінчується молодшими.

Шостий метод – copy_Array в якості вхідних параметрів приймає два вказівники типу unsigned int. Перший вказівник показує на початок масиву з якого відбуватиметься подальше копіювання, а другий – в який масив потрібно скопіювати значення першого. Оскільки метод працює на пряму з пам’яттю і помилки в його роботі не передбачено, тому в якості вихідного значення нічого не повертається.

Сьомий метод – copy_module_to_number в рамках класу копіює значення масиву де зберігається модуль, тобто MOD в масив де зберігається довге число, тобто number.

Восьмий метод – перевизначення оператора «>>=» працює над змінною типу long_numbers, та числом типу int. В якості перевизначеної операції виступає логічний зсув праворуч на k разів масиву number.

Дев’ятий метод – перевизначення операції «<<=» принципом роботи схожий з попереднім, лише зсув відбувається ліворуч.

Десятий метод - перевизначення оператора «+=» працює над двома змінними типу long_numbers. В якості перевизначеної операції виступає бінарне додавання до першого значення другого. Додавання двох довгих чисел організовано з врахуванням переносів, що є критично важливим.

Одинадцятий метод - перевизначення оператора «-=» працює над двома змінними типу long_numbers. В якості перевизначеної операції виступає бінарне віднімання від першого значення другого. Як і в попередньому методі, віднімання двох довгих чисел організовано з врахуванням переносів, що є критично важливим.

Дванадцятий метод - перевизначення оператора «*=» втілює метод множення Монтґомері над довгими числами. В якості перевизначеної операції виступає бінарне множення першого значення на друге. Метод множення Монтгомері передбачає створення змінної результату R класу long_numbers, початкове значення

якої встановлюється в нуль. В циклі організовано аналіз всіх бітах множеного, в тому випадку якщо значення поточного розряду не дорівнює нулю, до результату додається значення числа A, за допомогою вище описаного методу. Значення множеного зсувається на один біт праворуч. Якщо поточний результат непарний, до нього додається модуль, після чого, в будь-якому випадку, результат зсувається праворуч на один біт. Після закінчення циклу, якщо значення поточного результату більше модуля, то проводиться віднімання модулю від результату.

Тринадцятий метод – MUL передбачає отримання двох параметрів типу long_numbers. В результаті роботи метод повертає змінну аналогічного типу. Природа цього методу полягає в виконанні множення з старших розрядів множеного з зсувом результату ліворуч. В методі використовуються описані вище перевизначення операцій, а саме логічний зсув ліворуч та додавання.

Чотирнадцятий метод – last_bit_number відповідає за знаходження останнього біту довгого числа, яке зберігається в масиві number.

П’ятнадцятий метод – last_bit_number, як і попередній, відповідає за знаходження останнього біту, але вже в модуля.

Клас exponentiantion в розробленій системі відіграє роль модулярного експоненціювання над числами великої розрадності. Ключова функція цього класу – за допомогою, вже описаного long_numbers надати можливість користувачу підносити довгі числа в степінь, розрядність якої значно перевищує розрядність процесора. Реалізація такої складної задачі полягає в широкому погляді на проблему сучасного експоненціювання. Так, для обчислення експоненти в 128 біт, реальні часові затрати середньостатистичного комп’ютера спокійно можуть перевищити 1.5 години. Відповідно для оптимізації цього процесу доцільно використовувати нові технологічні підходи для обчислення експоненти. Серед всіх можливих варто виділити ті, які безпосередньо скорочують час виконання найскладніших процедур. В випадку модулярного експоненціювання це – редукція та множення. Виконання редукції на числах великої розрядності – це колосальна по об’єму задач процедура, адже вона дуже чутлива до деталей, з тим і потребує врахування багатьох моментів, як от порівняння певних частин числа, яке в нашому випадку роз-

поділено по масиву, знаходження старшого біту, віднімання і зсуви. Підходів до прискорення обчислення редукції існує багато, але найефективнішим вважають метод Пітера Монтґомері. Його підхід дозволяє замінити операцію модулярної редукції на зсув та додавання, а замість звичного множення використовувати множення Монтґомері, що теж значно прискорює загальний процес обчислення. Власне такий підхід і реалізовано с класі exponentiation.

Клас exponentiation працює з числами типу long_numbers, тому окрім їх розрядності в приватній змінній n типу int нічого не зберігає.

Публічні методи згаданого вище класу зображено на рисунку 5.2:

```
exponentiation(int);
long_numbers reduction(long_numbers);
long_numbers Exponentiation(long_numbers, long_numbers);
```

Рисунок 5.2 – Публічні методи класу exponentiation

Перший метод – конструктор класу, який в якості параметрів потребує змінну типу int значення якої він присвоює внутрішній змінній n.

Другий метод – reduction, потребує в якості параметру змінну number класу long_numbers, яку ж він і повертає після виконання редукції. В тілі методу реалізована звичайна редукція над великими числами. Її ідея полягає в постійному відніманні від числа значення модуля, зсунутого на різницю останніх бітів цих чисел. В випадку, якщо віднімання реалізувати не можна, тобто частина числа менша, за модуль, хоча ціле число все ще більше, модуль необхідно зсунути праворуч до тих пір, поки не стане можливим віднімання.

Третій метод – Exponrntioation в якості вхідних параметрів приймає два довгих числа: A - число яке буде підноситися в ступінь, та E - власне сам ступінь. В середині методу реалізовано експоненціювання Монтґомері. На стадії підготовки перед циклом обчислюються довгі числа P, як 2 в ступені n по модулю M та C, як P в квадраті по модулю M. Варто зазначити, що метод Монтґомері потребує використання звичного й резурсозатратного експоненціювання і редукції на початку.

Останньою дією перед циклом є множення Монтґомері числа C на задану число A. Оскільки система носить більше наукову ніж прикладну цінність, відповідно й числа часто змінюють розрядність, в реальному ж житі їх розмір не змінюється, тому ці обчислення можна порахувати заздалегідь та зберігати в пам'яті для подальших експоненціювань. Власне експоненціювання Монтґомері передбачає цикл з старшого розряду експоненти до нульового. В середині циклу реалізовано піднесення числа P до квадрату та, якщо поточний біт експоненти E не дорівнює нулю множення результату P на значення C. Для знаходження остаточного результату необхідно помножити отримане в змінній P значення на 1. Звісно ж, це множення, як всі множення в циклі здійснюється за методом Монтґомері.

Третій клас розробленого системного продукту з назвою table_exp поєднує в собі модулярне експоненціювання з передобчисленнями. Цей клас реалізує поставлену на початку роботи ціль покращення відомого методу ідентифікації Шнора в вигляді обчислення модулярного експоненціювання з використанням таблички передобчислень.

Організація данних в середині класу передбачає зберігання таблиці передобчислень в обмеженому доступі разом з розрядністю оброблюваних чисел. Важливою складовою цього класу є саме створення цієї таблиці довгих чисел та робота з нею.

До публічних методів цього класу проілюстровані на рисунку 5.3:

```
table_exp(int,long_numbers);
void out_put_Table();
long_numbers Exponentiation(long_numbers);
```

Рисунок 5.2 – Публічні методи класу table_exp

Перший метод – table_exp (конструктор) відповідає за створення таблиці передобчислень, тобто несе в собі головну функцію розробленого класу. На вік конструктор приймає значення int в якому зберігається розрядність оброблюваних чисел та значення числа A, складової модулярного експоненціювання. В тілі ме-

тоду відбувається побудова таблиці передобчислення за описаною в попередніх розділах схемою.

Другий метод – out_put_Table відповідає за вивід значень таблички користувачеві.

Третій метод – Exponentation на вхід приймає значення довгого числа E, а в тілі реалізує модулярне експоненціювання числа A в ступені E по модулю M за описаною в попередніх розділах схемою.

5.6 Аналіз результатів моделювання

В результаті проведених досліджень з використанням розроблених програмних продуктів отримано наступний результат. Доведена на практиці функціональна конструктивність розробленого методу криптографічно строгої ідентифікації віддалених абонентів інформаційних систем колективного доступу, що функціонують в реальному часі.

Практично перевірено коректність теоретично розробленої процедури формування таблиць передобчислень, що дозволяють досягти радикального прискорення процесу криптографічно строгої ідентифікації з використанням незворотних перетворень теорії чисел. Експерементально доведено для чисел розрядністю 4096 що використання запропонованої сисеми застосування таблиць передобчислень дозволяє реально прискорити виконання операцій модулярного експоненціювання, а значить і криптографічно строгу ідентифікацію з використанням модифікованого метода Шнорра на три порядки, що в цілому підтверджує теоретичні розрахунки прискорення процесу ідентифікації.

Експериментальними дослідженнями підтверджена функціональна конструктивність запропонованої схеми блокування повторного використання перехоплених зловмисником сеансових паролей, що використовувались легальними віддаленими користувачам. Проведено моделювання стандартизованої схеми незворотніх хеш перетворень SHA-512. При цьому реалізовано і проаналізовано обидва варіанти реалізації схеми стандартизованого геш перетворення SHA-512:

З використанням криптопроцесора 74688, що має вбудовану функцію геш перетворення та програмними засобами термінальних мікроконтролерів користувачів. Показано що різниця обчислення геш сигнатури становила три порядки.

Висновок до розділу 5

В результаті виконання робіт та досліджень націлених на створення програмних засобів моделювання криптографічно строгої ідентифікації віддалених користувачі інтегрованих інформаційних систем, а також експериментального дослідження запропонованого методу ідентифікації віддалених користувачі інтегрованих інформаційних систем можуть бути зроблені наступні висновки:

Виходячи з особливостей запропонованого методу віддалених користувачі інтегрованих інформаційних систем визначено, що базовою обчислювальною операцією виступає модулярне експоненціювання. Відповідно, базовим об'єктом програми визначено клас довгих чисел розрядністю 4096 над яким виконуються методи модулярного піднесення до квадрату, модулярного множення, а також модулярної редукції Монтгомері – технології, яка дозволяє замінити неефективну в обчислювальній реалізації операцію ділення на додавання та логічні зсуви.

Для створення ефективного програмного продукту визначена організація даних у вигляді байтових масивів з можливістю адресації їх вказівниками різних типів, що дозволяє вирішити компроміс між можливістю обробки окремих бітів, та ефективного використання сучасних багато розрядних процесорів. Створений клас дозволяє реалізувати зовнішній інтерфейс з використанням даних різних типів, що підвищує гнучкість роботи з ними.

Для прискорення роботи розробленого класу при створені його методів широко використовуються перед обчислення які залежать тільки від модуля, який, в свою чергу, є частиною відкритого ключа і, відповідно, змінюється рідко.

З використанням розробленого прогрмного продукту проведені експериментальні дослідження запропонованого методу ідентифікації віддалених абонентів інформаційних систем колективного доступу, що функціонують в реальному часі.

6 МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ

6.1 Безпекова модель інформаційної системи

Основним чином атаки на системи ідентифікації користувачів націлені на отримання незаконного доступу до ресурсів системи шляхом перехоплення коректного користувацького паролю. Об’єктами атак можуть стати як сам інтернет, як місце передачі даних, так і пам’ять системи, тобто місце зберігання коректних паролей чи їх гешів. Ще одним способом атак що спрямовані на отримання коректних ідентифікаційних даних або на пряму доступу до ресурсів системи є інсталювання шкідливого програмного забезпечення на користувацькі пристрої.

З огляду на види атак, їх поділяють на активні і пасивні. Під час пасивної атаки зловмисник намагається отримати пароль шляхом його перехоплення в процесі передачі, тобто він не втручається в сам процес ідентифікації. Відповідно, помітити такі атаки може бути дуже складно. В ході активних атак, або добре відомих як middle attack – зловмисник витісняє користувача з взаємодії після його ідентифікації [16].

Останнім часом широкої популярності набули атаки, під час яких користувача пере спрямовують на сервіси що імітують справжні. Таким чином, користувач умовно добровільно надає зловмисникам свої секретні дані.

Також існує специфічний вид атак, що широко поширився останнім часом – це імітація самою системою звернення до неї. Головною ціллю всіх цих атак є отримання певної комерційної вигоди.

Аналіз сучасних систем ідентифікації показав, що переважна більшість з них використовує так звану криптографічно слабку ідентифікацію. Це зумовлено сучасними вимогами до швидкодії систем. Проте, незважаючи на швидкість процедури ідентифікації, такі системи лишаються надзвичайно вразливими до всіх видів атак. Одною з основних причин цієї вразливості є те, що велика кількість «недобросовісних» сайтів зберігає секретну інформацію у вигляді простих гешів, або навіть, просто у відкритому вигляді. Також, часто користувач використовує один постійний пароль для кожної процедури ідентифікації. Ще одною, великою

проблемою є те, що більшість з цих паролей генеруються не випадковим чином, тобто, існує певна залежність створення пароля від набутого життєвого досвіду, уподобань людини, або просто популярних словникових наборів. Важливим є й те, що користувач може повторно використовувати придуманий ним пароль в декількох системах. З усього вище зазначеного можна зробити висновок, що для отримання незаконного доступу до системи ідентифікації зловмисник не завжди змушений прикладати багато зусиль для отримання правильного користувацького паролю, а отримавши доступ до одного ресурсу, може без проблем відкрити інші, використавши повторно перехоплений пароль.

Крім того, відсутність регулярної зміни секретів дозволяє протягом тривалого часу використовувати вкрадений пароль, а незахищене зберігання чи передача робить систему вразливою до пасивного перехоплення.

Тобто, для підвищення рівня захищеності системи ідентифікації віддалених користувачів, в умовах використання віддаленої взаємодії в усіх сферах життя, варто обрати криптографічно строгу ідентифікацію, яка добре відома як “zero-knowledge identification” [17]. В рамках цієї концепції, при кожній процедурі ідентифікації користувач використовує новий сеансовий пароль. Це дозволяє захиститись від пасивних атак, оскільки перехопивши один сеансовий пароль, зловмисник не матиме доступу до наступної сесії.

Також, ідентифікація нульових знань захищає і від імітації системою доступу до неї від імені користувача, оскільки zki передбачає що у користувача є математичний механізм генерації правильних паролей, а в системи – перевірки їх правильності. Тобто сама система нездатна генерувати коректний пароль. Ну і відповідно, через мережу ніколи не передається справжній секрет. Учасник взаємодії повинен довести, що володіє вихідним знанням, не розкриваючи його, а система може засвідчити коректність цього доведення.

Проте, незважаючи на всі вище описані переваги zero-knowledge identification, лишається загроза middle атак, оскільки вони націлені не на саму процедуру ідентифікації, а на витіснення легального користувача після неї.

Є два основних методи захисту від такого типу атак. Перший – шифрування усієї комунікації, наприклад за допомогою використання VPN. Проте це рішення вимагає значної кількості ресурсів і не може бути ефективним в рамках багатокористувацьких систем, Оскільки може значно уповільнювати взаємодію користувача і системи. Другий – це зробити процедуру ідентифікації достатньо ефективною, тобто швидкою і легкою, щоб повторювати її автоматично через певні регулярні інтервали часу, після ключових подій у сесії. Цей підхід може якісно і умовно просто запобігти довгому зловмисниць кому утриманню сесії.

Тобто, вимогами до розробленої моделі є використання парадигм ідентифікації нульових знань, з метою захисту від більшості атак і пришвидшення процедури ідентифікації для зхисту від middle attack.

6.2 Вибір та опис прототипу

На сьогодні існує велика кількість методів що реалізують концепцію нульових знань [18]. В залежності від математичного базиса покладеного в їх основу. Ці методи поділяються на дві великі групи: на основі незворотніх перетворень булевої алгебри і на основі незворотніх перетворень теорії чисел.

Перші, в свою чергу також поділяються на два види, а саме: методи що базуються на ланцюжку паролей і методи засновані на геш перетвореннях. Всі ці варіанти підходу до реалізації ідентифікації нульових знань на основі незворотніх перетворень булевої алгебри мають перевагу в вигляді високої швидкодії, проте, говорячи про ланцюжок паролей варто зазначити що він обмежений в кількості паролів. Також в цьому методі всі паролі зберігаються в пам’яті, тобто отримавши до неї доступ зловмисник отримає доступ і до наступних сесій. Якщо паролі вже були викрадені, то єдиний метод захисту – повне перестворення усього ланцюжку. Метод заснований на геш перетвореннях позбавлений такого мінусу, але має складну процедуру генерації паролей.

Методи ідентифікації нульових знань на основі незворотніх перетворень теорії чисел мають значну перевагу в тому, що їх паролі є незалежні і необмежені,

проте в умовах підвищення вимог до швидкості систем вони показують незадовільні результати.

Порівняння двох основних підходів до реалізації zero-knowledge identification призвело до вибору методу криптографічно строгої ідентифікації на основі незворотніх перетворень теорії чисел для подальших досліджень.

Найбільш відомі методи що використовують незворотні перетворення теорії чисел для реалізації zki є добре відомі FESIS, Guillou - Quisquater и Schnorr. Метод FESIS [19] побудований багаторазовому використанні модулярних операцій над великим числом *M,* що в свою чергу є добутком великих простих чисел *p* і *q*. Користувач випадково обирає секретне значення *s,* і обчислює його модулярне піднесення до квадрату, значення якого використовуватиметься як відкритий ключ системи *t*. Наступним кроком користувач знаходить мультиплікативну інверсію отриманого числа. Далі підбирається закритий ключ *k* так, щоб його піднесення до квадрату відповідало значенню мультиплікативної інверсії взятої по модулю *M*. Після цього, система отримує відкритий ключ.

При кожному циклі ідентифікації генерується нове випадкове число *a*, з якого формується двокомпонентний сеансовий пароль, після чого система перевіряє його справжність за певною рівністю. Проблематика такої схеми заключається в потребі десятків раундів обміну, що значно уповільнює процес і робить його вразливим до мережевих затримок.

Схема Guillou-Quisquater [20] теж спирається на модуль, але зводить ідентифікацію до одного раунду. Абонент генерує випадкове *A*, обчислює $p_1=A^n \bmod M$ і надсилає це значення системі, яка у відповідь передає випадкове *m*. Тоді користувач формує другу частину паролю $p_2=A\cdot B^m \bmod M$, а система перевіряє відповідність $(p_2^u \cdot K^m) \bmod M = p_1$. Основна складність цієї процедури полягає в тому, що серверу доводиться виконати два повних модульних експоненціювання, що вимагає мільйонних обчислень і створює суттєве навантаження на процесор.

В схемі Шнорра користувач також обирає два великих простих числа *p* и *q*. Наступним кроком обирається довільне число *a* що не дорівнює одиниці і задовольнє наступну умову $a^q \bmod p = 1$. Обирається секретний ключ *s*, такий що $s < q$.

Відкритий ключ обраховується за наступною формулою $v = a^{-s} \bmod p$. Основну операцію ідентифікації користувача в системі можна описати наступним чином $x' = a^{y} \cdot v^{e} \bmod p = a^{(r+s \cdot e)} \cdot a^{-s \cdot e} \bmod p = a^{r} \cdot a^{s \cdot e} \cdot a^{-s \cdot e} \bmod p = a^{r} \bmod p = x$.

Детально проаналізувавши ці методи було помічено, що основною операцією усіх цих методів є приведення в ступінь *E* по модулю *M* числа *A*, що в свою чергу мусить мати розрядність 4096 і більше. Операції модулярного експоненціювання над такими великими числами вимагають значних часових і обчислювальних ресурсів. Відповідно, розроблений метод має напряму вирішувати цю проблему.

В запропонованій вашій увазі дипломній роботі за базовий метод було обрано схему Шнорра.

За рахунок того що в схемі Шнорра всі операції виконуються над постійними числами, для прискорення її роботи, усі підрахунки можна винести на етап передобчислень. Це дозволить отримати значний виграш в часі в порівнянні з усім відомою схемою Шнорра.

Якщо код показника подається у вигляді двійкового рядка, то обчислення експоненти виконують за відомою бінарною формулою. З цього випливає, що модульне піднесення до ступеня *E* можна уявити як добуток степенів числа *A* в ступенях двійки, помножених на відповідні біти двійкового коду експоненти. Далі цей вираз переписують так, щоб множилися лише ті степені A^{2i} для яких у двійковому коді експоненти стоїть одиниця. Оскільки значення $A^{2i} \bmod M$ залежать лише від сталих A та M, їх можна заздалегідь обчислити і занести в таблицю. Тоді власне обчислення $A^{E} \bmod M$ зводиться до послідовних модульних множень тих табличних значень, що відповідають одиничним розрядам двійкового коду експоненти.

Основною перевагою запропонованої модифікації методу Шнорра є радикальне підвищення швидкодії ідентифікації. Як чисельну міру приросту продуктивності використовують коефіцієнт β прискорення, який визначається як відношення часу ідентифікації в відомій схемі до часу ідентифікації в запропонованій.

Ураховуючи, що модульне експоненціювання займає на порядки більше часу, ніж інші операції в процедурі, при оцінці часової ефективності враховують лише операції модульного експоненціювання. У класичному алгоритмі час виконання цієї операції пропорційний числу n циклів, у кожному з яких виконують півтори операції модульного множення. А модульне множення довгих чисел саме по собі потребує для реалізації 2·n операцій додавання. Відтак у відомих методах загальний час експоненціювання пропорційний квадрату довжини чисел, n^2.

У запропонованій модифікації використовуються лише операції додавання. Під час модульного експоненціювання перевіряють розряди двійкового коду показника, і якщо поточний розряд рівний одиниці, до результату додають відповідне табличне значення. Таким чином час обчислення модульної експоненти лінійно залежить від n.

6.3 Розробка методу криптографічно строгої ідентифікації на основі незворотніх перетворень теорії чисел

На сам перед, метою дослідження є удосконалення криптографічно строгої ідентифікації віддалених користувачів шляхом оптимізації обчислювальних процесів та запобігання повторному використанню сеансових паролів. В свою чергу, запропоновані безпекові заходи напряму впливають на підвищення рівня захищеності відповідної процедури в системах ідентифікації.

Відповідно, розроблений метод може якісно захищати систему і користувача від переважної більшості атак на систему ідентифікації.

Досягнення поставленої мети реалізується завдяки розробленому методу ідентифікації віддалених користувачів, який є модифікацією відомої схеми Шнорра в рамках концепції нульових знань.

Запропонований метод включає в себе чотири процедури.

Першою з яких є формування таблиць передобчислень швидкого модулярного експоненціювання постійного числа. Цей етап дозволяє значно прискорити процедуру ідентифікації за рахунок передобчислень. Такі дії можливі, оскільки в

ході досліджень було помічено, що в методі що взято за основу, а саме методі Шнорра [21], математичні перетворення виконуються над постійними числами, що дозволяє винести певні підрахунки за межі самої процедури ідентифікації.

Наступна розроблена процедура, як і вище зазначена, також направлена на підвищення часової ефективності ідентифікації. Сама процедура прискореного обрахунку модулярної експоненти використовується в межах двох інших процедур, таких як реєстрація і ідентифікація користувача в інформаційній системі з використанням раніше створених таблиць передобчислень. За рахунок цього отримується значна економія часу витраченого на ідентифікацію.

Як вже було зазначено, наступна процедура – це процедура реєстрації користувача в системі. Ці дії виконуються одноразово, а саме при першій взаємодії користувача з інформаційною системою ідентифікації. За рахунок того що на цьому етапі відбувається генерація таблиць передобчислень постійного числа в ступінь n – ця процедура займає найбільше часу.

Останньою є, безпосередньо процедура ідентифікації користувача в системі перед початком сеансу взаємодії. Ця процедура виконується при кожному вході користувача в систему гарантуючи захищеність від атак і високу швидкодію.

Запропонована процедура формування таблиць передобчислень для швидкого експоненціювання числа b по модулю p включає в себе формування двох таблиць і передбачає виконання наступної послідовності дій:

1) індекс j встановлюється в одиницю: $j = 1$, а значення першого елементу таблиці передобчислень $T_b[1]$ рівним значенню b : $T_b = b$;

2) значення індексу j збільшується на 1: $j = j + 1$. Якщо нове значення індексу є більше від n, n – кількість розрядів в значенні модуля p: $j > n$,перехід на п.4;

3) значення j елемента таблиці T_b, обчислюється за формулою: $T[j] = T[j-1]^2 mod p$. Перехід на повторне виконання п.2;

4) завершення формування таблиць.

Запропонована процедура формування таблиць передобчислень, демонструється на прикладі формування таблиці T_a для постійного числа b = 11 і модуля p = 1010011_2 = 83.

Відповідно до п.1, індекс j встановлюється в одиницю: $j = 1$, а значення першого елементу таблиці T_a прирівнюється до одинадцяти: $T_a[1] = 11$. В межах другого пункту процедури, Значення індексу інкрементується: $j = 2$ і порівнюється з сімкою, оскільки 2 < 7, перехід на пункт 3. В рамках п.3, обраховується значення відповідного елемента таблиці T_a: $T[2] = T[2-1]^2 mod 83 = 11^2 mod 83 = 38$ і заноситься у таблицю. Подальше заповнення таблиці T_a виконується аналогічно, приклад заповненої таблиці для b = 11 приведений в таблиці 6.1. Таблиця T_v для b = 63 заповнюється аналогічно, приклад заповненої таблиці приведений в таблиці 6.2.

Таблиця 6.1 – Приклад заповненої таблиці T_a для постійного числа b = 11 і модуля p = 1010011_2 = 83

j	**T[j]**
1	11
2	38
3	33
4	10
5	17
6	40
7	23

Таблиця 6.2 – Приклад заповненої таблиці T_v для постійного числа b = 63 і модуля p = 1010011_2 = 83

j	**T[j]**
1	63

Продовження таблиці 6.2

2	68
3	59
4	78
5	25
6	44
7	27

Запропонована процедура швидкого експоненціювання постійного числа в ступінь E по модулю p з використанням таблиць передобчислень передбачає виконання наступної послідовності дій:

1) початкове значення результату R і номера біта експоненти j встановлюються рівними 1: $R = 1, j = 1$;

2) якщо поточне значення e_j біта експоненти рівне одиниці: $e_j = 1$, поточне значення результату множиться на j-ий стовбець таблиці передобчислень: $R = R \cdot T[j] mod p$;

3) інкрементується номер j-ого біта кода експоненти: $j = j + 1$. Якщо j менше або рівне n, де n – кількість розрядів в коді експоненти: $j \leq n$, перехід на п.2;

4) кінець процедури результат R: $R = a^e mod p$.

Запропонована процедура швидкого експоненціювання постійного числа з використанням таблиць передобчислень, демонструється на прикладі піднесення постійного числа $a = 11$ в ступінь $e = 110_2 = 6$ з використанням таблиці T_a, приведеної в таблиці 6.1.

В межах пункту 1, процедури швидкого експоненціювання постійного числа, початкове значення результату R і номера біта експоненти j встановлюються рівними одиниці: $R = 1$, $j = 1$. Відповідно до п.2, перевіряється значення поточного біта e_1 коду експоненти, оскільки e_1=0, в рамках п.3, номер поточного біту екс-

поненти збільшується на одиницю: j = 2. Так як 2 ≤ 3 виконується повернення на п.2.

Згідно з умовою, значення біта експоненти e_2 рівне одиниці: e_2=1 отже поточне значення результату модулярно множиться на табличне значення T_a[2], приведене в таблиці 1: $R = R \cdot T[2] mod 83 = 1 \cdot 38 mod 83 = 38$. Згідно з п.3, виконується перехід на наступний біт коду експоненти. Оскільки, 3 ≤ 3 , повторне виконання пункту 2. В рамках цього пункту значення біту e_3 = 1, тоді, значення результату модулярної помножається до табличного T_a[3], приведеного в таблиці 1: $R = R \cdot T[3] mod 83 = 38 \cdot 33 mod 83 = 9$. Відповідно до п.3, j = 4, виконується перехід на п.4, тобто кінець процедури. Результат експоненціювання за допомогою процедури швидкого експоненціюванювання рівний 9: $R = 11^6 mod 83 = 9$.

Запропонована процедура реєстрації користувача у системі включає в себе виконання наступної послідовності дій:

1) користувач обирає велике просте n-розрядне число p;

2) користувач обирає просте число q, таке що, p – 1 націло ділиться на q;

3) користувач обирає не рівне одиниці значення числа a, що задовольняє наступну рівність: $a^q mod p = 1$;

4) користувач з використанням вищеописаної процедури, формує таблицю передобчислень T_a для обраного числа a;

5) користувач обирає довільне число s, що є меншим від q : $s < q$, в якості секретного ключа;

6) користувач, за допомогою створеної в п.4 процедури реєстрації таблиці передобчислень T_a значень модулярної експоненти постійного числа a по модулю p, обраховує значення закритого ключа v як мультиплікативну інверсію до a^s, використовуючи формулу: $v = a^{p-1-s} = a^{-s} mod p$;

7) користувач встановлює число w в 0, це число слугує в якості номера сесії;

8) користувач шифрує відкритим ключем системи значення p, v і таблицю передобчислень T_a і надсилає їй їх;

9) система розшифровує своїм секретним ключем надіслані користувачем значення p, v і таблицю передобчислень T_a і зберігає отриману інформацію у пам'яті;

10) система встановлює значення номеру сесії w' рівним нулю;

11) система з використанням вищеописаної процедури, формує таблицю передобчислень T_v для обраного числа v.

В ході виконання процедури реєстрації в пам'яті користувача зберігатимуться значення p, q, a, s, w і таблиця передобчислень T_a, а в системи значення p, v, w і таблиці передобчислень T_a і T_v.

Вищеописана процедура реєстрації може бути представлена наступним прикладом.

Відповідно до п.1 і п.2 описаної процедури реєстрації p обирається рівним 83: p = 83, а q рівне 41: q =41. В рамках п.3, користувач обирає значення a = 11, оскільки воно задовольняє умову $11^{41} mod 83 = 1$.Згідно з пунктом 4, користувач формує таблицю T_a передобчислень постійного числа a = 11, наведену в таблиці 1. В межах п.5, користувач обирає s = 21, в якості приватного ключа. Відповідно до п.6, за допомогою процедури швидкого експоненціювання і таблиці передобчислень T_a користувач обраховує значення приватного ключа $v = 11^{-21} mod 83 = 63$. Згідно п.7 процедури реєстрації, користувач встановлює значення номеру сесії в 0: w = 0. В межах п.8 користувач шифрує відкритим ключем системи значення p, v і таблицю передобчислень T_a і надсилає їй їх. В рамках п.9 система розшифровує і зберігає надіслані користувачем дані. Згідно з п.10 система встановлює значення номеру сесії в 0: w'=0. Відповідно до п.11, система формує таблицю T_v передобчислень постійного числа v = 63, наведену в таблиці 2. В ході виконання процедури реєстрації в пам'яті користувача зберігатимуться значення p = 83, q = 41,a = 11, s = 21, w = 0 і таблиця передобчислень T_a приведена в таблиці 1, а в системи значення p = 83, v = 63, w = 0 і таблиці передобчислень T_a і T_v приведені в таблиці 1 і таблиці 2 відповідно .

Запропонована процедура ідентифікації користувача у системі включає в себе виконання наступної послідовності дій:

1) користувач обирає випадкове значення r, що є меншим від q;

2) користувач, використовуючи процедуру швидкого експоненціювання і таблицю передобчислень T_a постійного числа a, обраховує значення x по формулі $x = a^r mod p$ і надсилає його системі;

3) система обирає з діапазону від 0 до 2^{t-1} значення e і надсилає його користувачеві;

4) користувач обраховує значення u, як результат хеш-перетворення над конкатенацією змінних e і w: $u = H(e||w)$;

5) користувач обраховує значення y за формулою $y = (r + s \cdot u) mod q$ і надсилає його системі;

6) система обраховує значення u', як результат хеш-перетворення над конкатенацією змінних e і w': $u' = H(e||w)$;

7) система, використовуючи процедуру швидкого експоненціювання і таблиці передобчислень T_a і T_v, постійних чисел a і v відповідно, обраховує значення x' по формулі $x' = a^y \cdot v^{u'} mod q$;

8) система порівнює значення x та x'. Якщо x рівне x', система надає дозвіл на подальшу взаємодію і перезаписує значення w' збільшивши його на одиницю.

9) після отримання дозволу на подальшу взаємодію, користувач перезаписує змінну w збільшивши його на 1.

В запропонованому методі процедура ідентифікації ілюструється наступним прикладом.

В межах п.1, в якості r обрано число 6: r = 6. Згідно з п.2, користувач обраховує значення x, використовуючи процедуру швидкого експоненціювання і таблицю передобчислень T_a , приведену в таблиці 1: $x = 11^6 mod 83 = 9$ і надсилає це значення системі. В рамках п.3, запропонованої процедури ідентифікації, система обирає e рівне 4: e = 4. Відповідно до п.3, користувач обраховує значення u, як результат хеш-перетворення над конкатенацією e і w, тобто над 4 і 0. Допустимо, що результат хеш-перетворень на конкатенацією 4 і 0 рівний 3: u = H(4||0) = 3. Користувач надсилає системі значення u. Згідно з п.5, користувач обчислює значення y по формулі: $y = (6 + 21 \cdot 3) mod 41 = 28$ і надсилає його системі. Відпо-

відно до п.6 система обчислює значення u'. як результат хеш-перетворення над конкатенацією e і w', тобто над 4 і 0. Допустимо, що результат хеш-перетворень на конкатенацією 4 і 0 рівний 3: u' = H(4||0) = 3.. В межах п.7 система, використовуючи процедуру швидкого експоненціювання і таблиці передобчислень T_a і T_v, приведених в таблиці 1 і таблиці 2 відповідно, обраховує значення $x' = 11^{28} \cdot 63^3 mod 83 = 9$. В рамках п.8, порівнявши значення $u = u'$ = 3, система дає дозвіл на подальшу взаємодію перезаписує змінну w': $w' = w' + 1 = 1$. В свою чергу, відповідно до п.9, користувач, отримавши дозвіл на подальшу взаємодію, перезаписує змінну w: $w = w + 1 = 1$.

6.4 Оцінка ефективності

Запропонований метод ідентифікації орієнтований на виконання класичного алгоритму модулярного експоненціювання починаючи з молодших з розрядів. В ході виконання алгоритму, експоненціювання виконується у вигляді n циклів. На кожному i-тому циклі, де $i \in \{1,2,\dots,n\}$ розглядається відповідний біт коду експоненти $e_i \in [0;1]$, за умови що поточний біт коду експоненти рівний одиниці, до результату модулярно додається табличне значення T[i]. Відповідно, якщо вважати появу нуля і одиниці рівно ймовірною, то середня кількість операцій модулярного додавання рівна $0.5n$. Позначивши час виконання однієї такої операції за t_a, середній час виконання модулярного експоненціювання буде рівний T_e, і може бути обрахований за формулою 6.1:

$$T_e = 0{,}5 \cdot n \cdot t_a, \tag{6.1}$$

, де t_a - час виконання однієї операції модулярного додавання;

n – кількість бітів в коді експоненти.

В запропонованому методі, процедура ідентифікації виконується під час кожного сеансу і має три операції модулярного піднесення в степінь. Тобто, сере-

дній час затрачений на одну процедуру ідентифікації рівний $3T_e$. Виконання ж самої процедури ідентифікації, в свою чергу, відбувається умовні m сеансів.

Проте запропонований метод передбачає одноразове виконання процедури реєстрації на якій відбувається побудова двох таблиць передобчислень і дві операції модулярного експоненціювання.

Процедура побудови таблиць передобчислень виконується у вигляді n циклів, на кожному з яких відбувається модулярне піднесення до квадрату. Позначимо час на виконання одного модулярного піднесення до квадрату як t_k, тоді середній час T_t на побудову двох таблиць обраховується за формулою 6.2:

$$T_t = 2 \cdot n \cdot t_k , \tag{6.2}$$

, де t_k – час виконання однієї операції модулярного піднесення до квадрату.

Загальний час на виконання всіх процедур методу обраховується за формулою 6.3:

$$T = 3T_e \cdot m + T_t = 1{,}5 \cdot n \cdot t_a + 2 \cdot n \cdot t_k + n \cdot t_a , \tag{6.3}$$

,де m – кількість сеансів.

При реалізації модулярного експоненціювання з використанням методу Монтгомері, середній час T_1 обраховується по формулі 6.4:

$$T_1 = 1.5 \cdot n \cdot t_{MM} , \tag{6.4}$$

,де $1.5n$ – середня кількість операцій модулярного множення;

t_{MM} – час на виконання однієї такої операції.

Модулярне множення Монтгомері виконується у вигляді n циклів, в кожному з яких виконуються три кроки:

На першому кроці, якщо значення поточного біта множника рівне одиниці - до суми часткових добутків додається значення множеного. Відповідно, з ймові-

рністю 0.5 відповідна операція виконується. На другому кроці, залежно від значення молодшого біта отриманого результату, додається або не додається до нього модуль. Оскільки ймовірність того що значення молодшого біта є нулем, чи одиницею рівна, відповідна операція виконується з ймовірністю 0.5. На останньому кроці зсув результату на один біт вправо відбувається завжди. Таким чином, у середньому, на одному циклі алгоритму модульного множення Монтгомері кількість операцій дорівнює двом.

Аналіз часових характеристик сучасних процесорів показує, що виконання команд додавання та зсуву займає приблизно однаковий час. Тому, у подальших розрахунках можна вважати, що час зсуву t_s n-розрядних чисел дорівнює часу додавання t_a. Виходячи з цього, час t_{MM} реалізації модульного множення Монтгомері розраховується за формулою 6.5:

$$t_{MM} = 2 \cdot n \cdot t_a , \tag{6.5}$$

, де t_a - час виконання однієї операції модулярного додавання;

n – кількість бітів в коді експоненти.

Відповідно одна операція модулярного експоненціювання з використанням методу Монтгомері рівна 6.6:

$$T_1 = 1.5 \cdot n \cdot t_{MM} = 3 \cdot n^2 \cdot t_a , \tag{6.6}$$

,де $1.5n$ – середня кількість операцій модулярного множення;

t_{MM} – час на виконання однієї такої операції.

Запропонований алгоритм ідентифікації предбачає одноразову реєстрацію коистувача в системі, в ході якої виконується дві таких операції модулярного експоненціювання і безпосередню ідентифікацію впродовж m сеансів, на кожному з яких тричі вдбувається модулярне експоненціювання. Зважаючи на це, загальний середній час на ідентифікацію буде рівний T_M і обраховується за формулою 6.7:

$$T_M = 3T_1 \cdot m + 2T_1 = 9 \cdot n^2 \cdot t_a + 6 \cdot n^2 \cdot t_a, \tag{6.7}$$

,де m – кількість сеансів.

Таким чином, коефіцієнт прискорення α виконання усіх працедур застосуванню запропонованого методу оцінюється за такою формулою 6.8:

$$\alpha = \frac{T_M}{T} = \frac{9 \cdot n^2 \cdot t_a + 6 \cdot n^2 \cdot t_a}{1{,}5 \cdot n \cdot t_a + 2 \cdot n \cdot t_k + n \cdot t_a}, \quad (6.8)$$

Коефіцієнт прискорення β виконання працедури ідентифікації оцінюється за такою формулою 6.9:

$$\beta = \frac{T_1}{T_e} = \frac{3 \cdot n^2 \cdot t_a}{0{,}5 \cdot n \cdot t_a} = 6 \cdot n, \quad (6.9)$$

Підтвердженням теоретичних розрахунків стали практичні експерименти. Вони показали, що середній час ідентифікації справді зменшується в межах, близьких до отриманого коефіцієнта β: поліпшується відгук системи, знижується затримка під час входу без втрати криптографічного рівня захисту. Таким чином, поєднання одноразових паролів із високопродуктивною процедурою прискореного експонентування забезпечує одночасне підвищення безпеки й швидкості, що відкриває нові можливості для впровадження у великих розподілених системах із вимогами до мінімальної затримки та максимального захисту.

Концепція "нульових знань" бере за основу три ключові парадигми. Згідно першої користувач має криптографічний механізм генерації коректних паролів. В розробленому методі, як і в базовому методі Шнорра, цей механізм має двокомпонентну структуру, перша з яких базується на принципово незворотній операції модулярного експоненціювання $a^r \bmod p$, де a - відома системі компонента, а r - випадкове число, що змінюється в кожному сеансі. Ключову роль в механізмі генерації коректних паролів відіграє друга складова, яка базується на формуванні паролю у вигляді суми випадкової компоненти r та добутку секретного ключа s на геш перетворення над конкатенацією номера сеансу w і надісланого системою значення e: $u = H(f||w)$ по модулю q : $y = (r + s \cdot u) \bmod q$. Включення в суму випад-

кової компоненти r не дозволяє реконструювати значення секретного ключа s. Відповідно, не знаючи s, неможливо генерувати коректний пароль.

Відповідно до другої парадигми, система має криптографічний механізм перевірки коректності паролів. При цьому в розпорядженні системи є відкритий ключ v, який являє собою мультиплікативну інверсію значення a^s по модулю p. Сутність механізму перевірки коректності паролю системою полягає в обчисленнінею значення $x' = a^y \cdot v^{u'} \bmod p$. Перетворення впродовж всієї процедури ідентифікації можна побачити у формулв 6.10.

$$x' = a^y \cdot v^{u'} \bmod p = a^{(r + s \cdot e)} \cdot a^{-s \cdot e} \bmod p = a^r \cdot a^{s \cdot e} \cdot a^{-s \cdot e} \bmod p = a^r \bmod p = x \,, \qquad (6.10)$$

,де a - відома системі компонента;

r - випадкове число, що змінюється в кожному сеансі;

s – закритий ключ;

v – відкритий ключ;

u' – значення геш перетворення

Третьою парадигмою концепції "нульових знань" декларується, що в кожному сеансі віддаленої взаємодії має використовуватися новий пароль. Як слідує із описаної вище процедури ідентифікації ця умова також виконується.

Таким чином, показано, що запропонований метод ідентифікації повною мірою відповідає парадигмам теоретичної концепції "нульових знань" і, відповідно, він є криптографічно строгим.

Головна відмінність розробленого методу криптографічно строгої ідентифікації від відомих схем, основаних на незворотних перетвореннях теорії чисел і, зокрема, схеми Шнорра полягає в блокуванні повторного використання коректних паролів користувача. Щоб довести це, припустимо, що система запам’ятала коректний пароль $<x_i, y_i>$, згенерований користувачем на і-му сеансі ідентифікації. Нехай, вона вирішила повторно використати цей пароль на поточному j-му сеансі ідентифікації (за умови що $i < j$). Запам’ятавши інформацію, і-ого сеансу система може виконати операцію несанкціонованого входу наступним чином. Першим

кроком, вона надсилає собі значення u_i замість очікуваного u_j. Тоді, пропустивши всі обрахунки, її наступним кроком буде обрахунок значення u_i', як хеш перетворення конкатенації значень x_i та x_{i-1} і порівняння його зі значенням u_i. Порівнявши значення u_i' та u_i система дозволить почати взаємодію від імені користувача. Проте, відповідний незаконний вхід можна легко виявити, оскільки, переглянувши останню операцію ідентифікації можна помітити,що в якості останнього паролю входу не було використано значення $x_{j-1,}$ тому можна легко довести, що вхід у систему був виконаний не користувачем.

Висновки до розділу 6

В результаті проведення комплексу досліджень, направлених на створення ефективних засобів криптографічно строгої ідентифікації віддалених користувачів інформаційних систем отримані наступні результати:

Проведений поглиблений аналіз сучасних методів атак на інформаційні системи показав, що найбільший захист від зовнішнього втручання забезпечують методи ідентифікації віддалений абонентів, що базуються на теоретичній концепції “нульових знань”, яка повністю виключає наявність зберігання в інформаційній системі даних, що можуть бути використані для незаконного доступу до її ресурсів. Разом з тим, існуючі методи криптографічно строгої ідентифікації використовують складні обчислювальні процедури, комп’ютерна реалізація яких потребує значних за обсягом часових ресурсів. Це обмежує оперативність доступу користувачів до ресурсів інформаційної системи, а також накладає обмеження на їх кількість. Показано, що суттєвий недолік існуючих методів криптографічно строгої ідентифікації полягає в тому, що вони не блокують повторне використання перехопленого зловмисником сеансового паролю легальних користувачів інформаційних систем.

В результаті детального вивчення існуючих методів криптографічно строгої ідентифікації в якості протипу обрано схему Шнора, оскільки вона, на відміну від інших схем, що реалізують теоретичну концепцію “нульових знань” ви-

користовує в якості відкритого ключа числа, над яким здійснюється модулярне експоненціювання, на відміну від інших схем, в яких ключ застосовується в якості показника експоненти. Проведені дослідження показали, що це можу бути ефективно використане для прискорення математичної процедури модулярного експоненціювання з використанням передобчислень.

Теоретично обґрунтовано, розроблено та експериментально досліджено метод криптографічно строгої ідентифікації віддалених абонентів інформаційних систем, відмінність якого полягає в використанні передобчислень, що залежать лише від відкритого ключа, прискорення основної роботи криптографічних механізмів для генерації сеансових паролів користувачем та їх перевірки системою, що дозволяє наказувати збільшити швидкодію процесу криптографічно строгої ідентифікації і тим самим підвищити рівень оперативності обслуговування віддалених абонентів інформаційних систем, зняти обмеження на їх кількість, а також ефективно протидіяти middle-атакам на інформаційні системи. Запропонований метод також відрізняється введенням хеш -трансформації, завдяки якій повторне використання правильних паролів блокується і тим самим збільшує рівень безпеки інформаційних систем. Доведено, що розроблений метод відповідає парадигмам концепції ідентифікації нульового знання.

Теоретично доведено та експериментально підтверджено, що розроблений метод дозволяє прискорити ідентифікацію віддалених користувачів інформаційних систем на три порядки порівняно з відомими схемами Schnorr. Показано, що запропоноване використання хеш-трансформації з'єднує наступні та попередні паролі і тим самим блокує їх повторне використання. Тим самим підвищується рівень безпеки інформаційних систем від несанкціонованого використання їх ресурсів. Розроблений метод орієнтований на використання у рамках інформаційних систем, які дистанційно надають доступ до своїх ресурсів для великої кількості користувачів у режимі реального часу.

7 ТЕСТУВАННЯ

Тестування розробленої інформаційної системи з криптографічно строгою ідентифікацією її віддалених користувачів проводилися з застосуванням створених програмних засобів, які реалізують криптографічні механізми генерації сеансових паролів на боці користувача, перевіркі правильності паролі на боці системи, а також моделювання процесів ідентифікації.

Ціль тестування полягає в наступному:

— доведення на практиці функціональної конструктивності запропонованого методу криптографічно строгої ідентифікації з блокуванням повторного використання зловмисником перехоплених паролів легальних користувачів;

— експериментальне визначення часових характеристик базових розроблених процедур: генерації сеансових паролів на стороні системи, перевірки правильності надісланих паролів на стороні інформаційної системи функціонують нормально. Найбільш критичним є експериментальна перевірка теоретично обґрунтованого підвищення швидкості перевірки правильності паролів на боці системи з використанням швидкого модулярного експоненціювання довгих чисел, розрядність яких на порядки перевищує розрядність процесора;

— експериментальне визначення рівня захищеності, який вимірюється об’ємом ресурсів для випадкового чи направленого підбору правильних сеансових паролів легальних віддалених користувачів розробленої інформаційної системи.

Тестування функціональної працездатності проводилося в різних режимах, включаючи екстремальні (раптова втрата Інтернету, раптове відключення учасників дистанційної інформаційної взаємодії). В усіх режимах інформаційна система функціонувала нормально. Іншими словами, тестування функціональної працездатності не виявило помилок в роботі як самої інформаційної системи в цілому, так і її підсистеми ідентифікації віддалених користувачів. Тестування функціональної працездатності розробленої інформаційної системи з криптографічно

строгою ідентифікацією її віддалених користувачів за запропонованим методом показало, що на практиці всі розроблені процедури: побудови таблиць передобчислень, що залежать від закритого ключа, генерації сеансових паролів на стороні системи, перевірки правильності надісланих паролів на стороні інформаційної системи функціонують нормально. Спеціально було протестовано розроблені механізми блокуванням повторного використання зловмисником перехоплених паролів легальних користувачів. В результаті тестування практично доведено, що навіть в екстремальних ситуаціях розроблені механізми блокування повторного використання паролів працюють нормально.

Тестування часових характеристик роботи інформаційної системи, зокрема її підсистеми криптографічно строгої ідентифікації віддалених користувачів з використанням запропонованого методу проводилась з застуванням спеціально розробленої програмної моделі, яка імітує часові затримки виконання окремих операцій.

В результаті проведеного тестування часових характеристик роботи інформаційної системи, зокрема її підсистеми криптографічно строгої ідентифікації віддалених користувачів з використанням запропонованого методу отримано числові дані, зведені в таблицю 7.1.

Таблиця 7.1 – Результати тестування часових характеристик

Процедура	Часова характеристика, с	
	теоретично обрахована	експериментально отримана
Генерації паролів	1,8	1,85
Перевірка паролю системою (відома схема Шнора)	1,2	1,34
Перевірка паролю системою (запропонований метод)	0,0007	0,00082

Аналіз даних, наведених в таблиці 7.1 засвідчує, що, отримані в результаті проведеного тестування експериментальні дані незначно перевищують теоретично обраховані. Експериментально підтверджено, в результаті проведеного тестування, що запропонований метод дозволяє на три порядки прискорити процес перевірки правильності сеансових паролів віддалених користувачів в порівнянні з прототипом – широко відомою схемою Шнора, за рахунок застосування передобчислень, що залежать від практично постійного відкритого ключа користувача.

Висновок до розділу 7

В результаті проведених експериментальних досліджень, направлених на практичне визначення технічних характеристик та доведення працездатності інформаційної системи з криптографічно строгою ідентифікацією, можуть бути зроблені такі висновки.

Тестування функціональної працездатності розробленої інформаційної системи за запропонованим методом показало, що на практиці всі розроблені процедури: побудови таблиць передобчислень, що залежать від закритого ключа, генерації сеансових паролів на стороні системи, перевірки правильності надісланих паролів на стороні інформаційної системи функціонують нормально. Спеціально було протестовано розроблені механізми блокуванням повторного використання зловмисником перехоплених паролів легальних користувачів.

В результаті проведеного тестування часових характеристик роботи інформаційної системи, зокрема її підсистеми криптографічно строгої ідентифікації віддалених користувачів з використанням запропонованого методу доведено, що, отримані в результаті проведеного тестування експериментальні дані незначно перевищують теоретично обраховані. Експериментально підтверджено, в результаті проведеного тестування, що запропонований дозволяє на три порядки прискорити процес перевірки правильності сеансових паролів віддалених користувачів в порівнянні з прототипом – широко відомою схемою Шнора, за рахунок застосування передобчислень, що залежать від практично постійного відкритого ключа.

ВИСНОВКИ

В результаті виконання бакалаврського проєкту націленого на розроблення інформаційної системи ідентифікації віддалених користувачів можуть бути сформульовані наступні висновки:

В сучасних умовах розширення використання інформаційних систем на сфері застосування,які вимагають підвищеного рівня безпеки, домінуючою вимогою до систем ідентифікації є забезпечення високого рівня захищеності який потенційно може бути досягнений лише в рамках застосування криптографічно строгих методів ідентифікації, що базуються на теоретичній концепції нульових знань.

Проте, разом з розширенням сфер використання, стрімким збільшенням кількості користувачів що перебувають в системі в режимі реального часу, і вимогами до обробки даних під час, безпосередньо, етапу ідентифікації їх у системі, проблема забезпечення високої швидкодії дистанційної інформаційної взаємодії стала критично важливою. Аналіз показав що існуючі методи ідентифікації віддалених абонентів, що відповідають критеріям концепції нульового розголошення не в повній мірі задовольняють вимогам сучасного стану розвитку систем віддаленої інформаційної взаємодії. Виходячи з наведеного, у сучасних умовах забезпечення надійної та ефективної віддаленої інформаційної взаємодії вимагає розробки нових протоколів ідентифікації користувачів, які забезпечать одночасно посилений криптографічний захист та підвищену швидкодію. Метою дослідження є удосконалення криптографічно строгої ідентифікації віддалених користувачів шляхом оптимізації обчислювальних процесів та запобігання повторному використанню сеансових паролів, що в свою чергу підвищує її рівень захищеності.

В результаті детального вивчення існуючих методів криптографічно строгої ідентифікації в якості протипу обрано схему Шнора, оскільки вона, на відміну від інших схем, що реалізують теоретичну концепцію “нульових знань” використовує в якості відкритого ключа числа, над яким здійснюється модулярне експоненціювання, на відміну від інших схем, в яких ключ застосовується в якості

показника експоненти. Проведені дослідження показали, що це можу бути ефективно використане для прискорення математичної процедури модулярного експоненціювання з використанням передобчислень.

Теоретично обґрунтовано, розроблено та експериментально досліджено метод криптографічно строгої ідентифікації віддалених абонентів інформаційних систем, відмінність якого полягає в використанні передобчислень, що залежать лише від відкритого ключа, прискорення основної роботи криптографічних механізмів для генерації сеансових паролів користувачем та їх перевірки системою, що дозволяє наказувати збільшити швидкодію процесу криптографічно строгої ідентифікації і тим самим підвищити рівень оперативності обслуговування віддалених абонентів інформаційних систем, зняти обмеження на їх кількість, а також ефективно протидіяти middle-атакам на інформаційні системи. Запропонований метод також відрізняється введенням хеш -трансформації, завдяки якій повторне використання правильних паролів блокується і тим самим збільшує рівень безпеки інформаційних систем. Доведено, що розроблений метод відповідає парадигмам концепції ідентифікації нульового знання.

Теоретично доведено та експериментально підтверджено, що розроблений метод дозволяє прискорити ідентифікацію віддалених користувачів інформаційних систем на три порядки порівняно з відомими схемами Schnorr. Показано, що запропоноване використання хеш-трансформації з'єднує наступні та попередні паролі і тим самим блокує їх повторне використання. Тим самим підвищується рівень безпеки інформаційних систем від несанкціонованого використання їх ресурсів.

Виходячи з того, що на боці інформаційної системи потрібно забезпечити найбільшу швидкість реалізації криптографічно строгої ідентифікації задля можливості обробки запитів великої кількості дистанційно-віддалених користувачів в режимі реального часу, а також задля запобігання ефективним middle-атакам, потрібно забезпечити максимальне використання можливостей процесору серверну. Для цього, потрібно обрати такі технології програмування, які надають змогу

ефективно організувати паралельну роботу на сучасних багатоядерних процесорах.

Оскільки передбачені запропонованим методом обчислення передбачають часте звернення до таблиць, технології розробки програмного продукту мають забезпечувати високу ефективність роботи з пам’яттю і дозволяти напряму керувати розміщенням даних таблиць по рівням комп’ютерної пам'яті, включаючи швидкодіючу кеш-пам'ять.

Тестування функціональної працездатності розробленої інформаційної системи за запропонованим методом показало, що на практиці всі розроблені процедури: побудови таблиць передобчислень, що залежать від закритого ключа, генерації сеансових паролів на стороні системи, перевірки правильності надісланих паролів на стороні інформаційної системи функціонують нормально.

В результаті проведеного тестування часових характеристик роботи інформаційної системи, зокрема її підсистеми криптографічно строгої ідентифікації віддалених користувачів з використанням запропонованого методу доведено, що, отримані в результаті проведеного тестування експериментальні дані незначно перевищують теоретично обраховані. Тому, можна стверджувати що запропонований метод дозволяє на три порядки прискорити широко відому схему Шнорра.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Boiko K., Markovskyi O., Borges J., Bardis N. Fast Zero-Knowledge Identification Method with Password Reuse Blocking // Proceedings of the 14th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT-2024). – 2024. – С. 674–677. – DOI:10.1109/DESSERT61349.2024.10416477.

2. My H., Yin Z., Chen P., Zhang X., Ma S. Zero-knowledge identity authentication for Internet of Vehicles: improvement and application // PLoS ONE. – 2020. – Т. 15, № 9. – С. 217–247.

3. Conti M. A Survey of Man in the Middle Attacks // IEEE Communications Surveys and Tutorials. – 2016. – Т. 18, № 3. – С. 2027–2051. – DOI:10.1109/COMST.2016.2548426.

4. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed.John Wiley, 1996 - 758 p.

5. Menezes A. Handbook of Applied Cryptography. — Boca Raton : CRC Press, 2001. — 780 с.

6. Battaieb S., Bidouz L., Blazy O., Gaborit P. Zero-Knowledge Reparation of the Veron and AGS Code-based Identification Schemes // Proceedings of IEEE International Symposium on Information Theory (ISIT). – 2021. – С. 55–60. – DOI: 10.1109/ISIT45174.2021.9517937.

7. Lamport L. Password Authentication with Insecure Communication // Communications of the ACM. – 1981. – Т. 24, № 11. – С. 770–772.

8. Bardis N., Doucas N., Markovskyi O. Zero-Knowledge Identification Method Based on Block Ciphers // Proceedings of the 2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO). – 2017. – DOI: 10.1109/ICCAIRO.2017.63.

9. Feige U. Zero knowledge proofs of identity/ Feige U., Fiat A., Shamir A. //In Journal of Cryptology, - 1988.- Vol.1.- №.2 . – P.77-94.

10. Guillou L.C., Quisquater J.J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory // Advances in Cryptology – EUROCRYPT ’88 : proceedings. – Berlin : Springer-Verlag, 1988. – С. 123–128.

11. Schnorr C.P. Method for Identification Subscribers and for Generating and Verificating Electronic Signatures in Data Exchange System : U.S. Patent No 4 995 083 . – 19.02.1991.

12. Markovskyi O., Al-Vrayat G.A.J.H., Doukas N., Bardis N. An Accelerate Approach for Public Key Cryptography Implementation on IoT Terminal Platforms // Proceedings of the 13th International Conference on Dependable Systems, Services and Technologies (DESSERT-2023). – 2023. – С. 434–442. – DOI:10.1109/DESSERT61349.2023.10416516.

13. Battaieb S., Bidouz L., Blazy O., Gaborit P. Zero-Knowledge Reparation of the Veron and AGS Code-based Identification Schemes // Proceedings of the IEEE International Symposium on Information Theory (ISIT). – 2021. – С. 55–60. – DOI:10.1109/ISIT45174.2021.9517937.

14. Kittichokechai K., Caire G. Secret Key-Based Identification and Authentication with a Privacy Constraint // IEEE Transactions on Information Theory. – 2016. – Т. 62, № 11. – С. 6189–6203.

15. Bardis N.G., Doukas N., Markovskyi O.P. A Method for Strict Remote User Authentication Using Non-Reversible Galois Field Transformations // MATEC Web of Conferences. – 2017. – Т. 125. – С. 243–249.

16. Asimi Y., Amghar A., Asimi A., Sadgi Y. Strong Zero-Knowledge Authentication Based on the Session Keys (SASK) // International Journal of Network Security & Its Applications. – 2015. – Т. 7, № 1. – С. 51–66.

17. Del Pino R. Efficient lattice-based zero-knowledge proofs and applications. — Paris : Université Paris Sciences et Lettres, 2018. — 110 с.

18. Stavroulakis P., Markovskyi O., Bardis N., Doucas N. Efficient Zero-Knowledge Identification Based on One-Way Boolean Transformations // Proceedings

of IEEE Globecom Workshops. – 2011. – С. 275–280. – DOI: 10.1109/GLOCOMW.2011.6162452.

19. Bardis N., Doucas N., Markovskyi O. Zero-Knowledge Identification Method Based on Block Ciphers // Proceedings of the 2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO). – 2017. – DOI:10.1109/ICCARO.2017.63.

20. Daiko I., Selivanov V., Chernyshevych M., Markovskyi O. Zero-knowledge identification of remote users by utilization of pseudorandom sequences // Information, Computing and Intelligent Systems. – 2022. – № 3. – С. 42–48.

21. Саницький А.П., Васильєва М.Д., Дайко І.В. Метод швидкої ідентифікації віддалених абонентів на основі концепції нульових знань // Наука і техніка сьогодні. – 2024. – № 3(31). – С. 791–803. – DOI:10.52058/2786-6025-2024-3(31)-791-804.

22. Марковський О.П., Дайко І.В. Метод криптографічно строгої ідентифікації на основі незворотних табличних перетворень на полях Галуа // Адаптивні системи автоматичного управління. – 2024. – Т. 1, № 44. – С. 127–141. – DOI:10.20535/1560-8956.44.2024.302429.

23. Русанова О.В., Дайко І.В. Метод криптографічно строгої ідентифікації віддалених абонентів на базі генераторів псевдовипадкових послідовностей // Проблеми управління та інформатизації. – 2023. – № 1 (77). – С. 68–79. – DOI:10.18372/2073-4751.76.18244.