КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від __ травня 2024 року, протокол №___.
Завідувач кафедри доктор фіз.-мат. наук, професор
_____Ігор АНІСІМОВ

ДИПЛОМНА РОБОТА МАГІСТРА
на тему:

«Розробка застосунку двофакторної автентифікаціїї в операційній системі Windows»

Виконав:
студент 2-го курсу магістратури
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОНП «Інформаційна безпека телекомунікаційних систем і мереж»
Гордин Павло Вадимович_____

Науковий керівник:
кандидат військових наук, доцент
Довбня Сергій Якович _____

Рецензент:
Кандидат технічних наук, СНС
Кондратюк Віктор Антонович_____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____Павло ГОРДІН

РЕФЕРАТ

Дипломна робота: 55с., 1 табл., 16 рис., 1 дод. (5с.), 21 джерел.

СПОСТЕРЕЖНІСТЬ, АВТЕНТИФІКАЦІЯ, ДВОФАКТОРНА, ІНФОРМАЦІЯ, СИСТЕМА ЗАХИСТУ.

Об’єкт дослідження - система обробки інформації в інформаційно-комунікаційних системах в яких для захисту інформації запроваджено сервіси безпеки операційних систем Windows.

Мета роботи - розробка технологічного рішення – програмного застосунку реалізації двофакторної автентифікації для інформаційно-комунікаційних систем, захист інформації в яких побудово на використанні сервісів безпеки операційних систем Windows та розробка рекомендацій щодо його використання на практиці малого та середнього бізнесу.

Розроблено систему двофакторної автентифікації для інформаційно-комунікаційних систем, захист інформації в яких забезпечується з використанням сервісів безпеки операційних систем Windows, в яких додатково використовується автономний програмний застосунок в наступній послідовності:

- Проведено аналіз сучасних програмних засобів ТЗІ і відповідних модулів автентифікації та обрано автономну систему для проектування.

- Обрано криптобібліотеки та розроблено додаткові програмні модулі генерації разового ключа.

- Розроблено рекомендації щодо впровадження цього застосунку в ІКС.

Реалізація двофакторної авторизації відрізняється від Kerberos (операційних систем Windows) в тому, що запропонований застосунок забезпечує автентифікацію на основі двох різних факторів, а саме протоколу Kerberos, який дозволяє отримувати доступ до ресурсів у розподіленій мережі та сеансового ключа (формується з особистих ключів користувачів з застосуванням окремого разового каналу). Розроблено макет застосунку мовою С++(сі плюс плюс), де на першому етапі здійснюються шифрування, на другому етапі - дешифрування даних ключа і одночасно з цим верифікація відправника та отримувача .

ЗМІСТ

ВСТУП

В умовах діючого воєнного стану в Україні особливу актуальність має забезпечення захисту інформаційно-комунікаційних систем від навмисного втручання кіберзлочинців. Це завдання виконується за такими основними напрямами:

1. Створення комплексних систем захисту інформації з підтвердженою відповідністю (в основному для державних структур та підприємств).
2. Запровадження галузевих та адаптованих профілів захисту при створення систем інформаційної безпеки та їх авторизація відповідно до вимог ДСТУ серії 27000.
3. Впровадження в різних організацій окремих програмних та програмно-апаратних засобів (в яких можна налаштовувати сервіси безпеки) - на даний час найбільш поширено.

Загальним методом (обов'язковим) захисту конфіденційної інформації є налаштування параметрів ідентифікації та автентифікації [1, 2].

Як показує оприлюднений досвід втручання та злому різних систем (наприклад Київстар [3]) загальне програмне забезпечення не може на 100% забезпечити захист відкритої та конфіденційної інформації. Тому в таких системах потрібно додаткове налаштування та/або впровадження методів багатофакторної автентифікації за напрямами - автентифікація адміністраторів, користувачів, відправника та отримувача повідомлень [4] .

На сьогодня в галузі кібербезпеки відомо ряд рішень для малого та середнього бізнесу, які допомагають забезпечити додаткові рівні безпеки корпоративної мережі. Проте важливо захищати не тільки IT-системи, а й інформаційні активи (комерційна таємниця, конфіденційна та відкрита інформація щодо бізнес процесів), які є головним ресурсом будь-якого підприємства.

Одним із першочергових кроків для безпеки критичної інформації має бути посилення спостережності в системі захисту. В першу чергу це стосується захисту облікових записів користувачів та адміністраторів системи. Зокрема запровадження двофакторної автентифікації, додатково до використання мандатної системи (паролів) розподілу доступу до онлайн-сервісів інформаційно-комунікаційних систем.

Такі рішення (програмно-апаратні застосунки) потрібні для компаній будь-якого розміру, оскільки щоденно співробітники здійснюють вхід на декілька платформ. В першу чергу двофакторну автентифікацію необхідно забезпечити для облікових записів з правами адміністратора та тих, хто має доступ до конфіденційної інформації. Це є потужним кроком до запобігання крадіжці даних і можливим фінансовим втратам.

Таким чином двофакторна автентифікація може забезпечити додатковий захист системи від втручання зловмисників.

Актуальність теми дослідження: За численними повідомленнями [3-8] в засобах масової інформації, громадяни України постійно піддаються хакерським атакам з боку ворожих кіберзловмисників. Мають місце надсилання електронних листів, повідомлень у месенджерах від начебто державних органів, банків, служби безпеки тощо з рекомендаціями перейти за вказаними у листах/повідомленнях посиланнями. Після завантаження вкладеного файлу зловмисники мають змогу отримати доступ до персональних даних, що містяться на електронному пристрої користувача (контактів телефонної книги, файлів персонального комп'ютера тощо).

Тобто є нагальна потреба підвищення рівня спостережності в базових (діючих) системах захисту інформації, а саме забезпечення багаторівневої автентифікація адміністраторів, користувачів, відправника та отримувача повідомлень.

Об'єкт дослідження - система обробки інформації в інформаційно-комунікаційних системах в яких для захисту інформації запроваджено сервіси безпеки операційних систем Windows.

Мета роботи - розробка технологічного рішення – програмного застосунку реалізації двофакторної автентифікації для інформаційно-комунікаційних систем, захист інформації в яких побудово на використанні сервісів безпеки операційних систем Windows та розробка рекомендацій щодо його використання на практиці малого та середнього бізнесу.

Предметом дослідження є програмний застосунок двофакторної аутентифікаціїї, для більшого захисту в Windows систем . Науково-прикладний

результат буду у формі коду. Можливості використання двофакторної моделі май великий спектр можливості які збудуть забезпечувати конфіденційність , цілісніть та захисту обміну даними**.**

Наукова новизна: Отримання науково-прикладного результату, а саме програмного застосунку та рекомендацій щодо його використання для забезпечення двофакторної автентифікації в системах захисту інформації інформаційно-комунікаційних систем з використанням ОС Windows.

Методологія та методи дослідження: Спрямована на запровадження нових технологій та істотне вдосконалення тих що вже введені в дію, та використовуються в операційній системі Windows, аналіз можливості використання технологіїї двофакторної автентифікації .

1. Послуга автентифікації в системах захисту інформації автоматизованих систем

1.1. Поняття послуг автентифікації в системі критерія спостережності системи захисту інформації в автоматизованих системах

Інформаційно-комунікаційні системи (ІКС) з використанням засобів криптозахисту інформації (КЗІ) створюються для забезпечення безпеки обробки, передачі та зберігання конфіденційної інформації.

В даному розділі розглядаються такі основні принципи їх функціонування:

- Шифрування даних;
- Автентифікація і авторизація;
- Захист ключів;
- Захист від атак та вразливостей;
- Управління ключами і сертифікатами.

Опис принципів та методів наведено в розділі 1.1 Додатку А.

Аналізу підлягає система обробки інформації в інформаційно-комунікаційних системах (далі – ІКС), загальну схему якої наведено на рисунку 1.1.

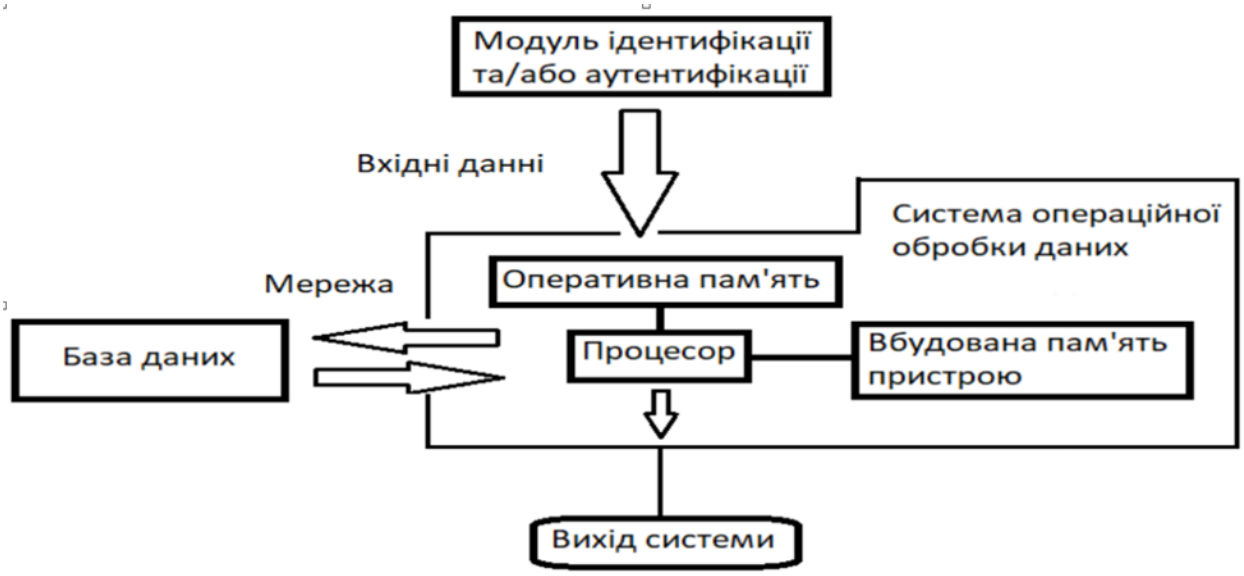


Рис. 1.1. Система обробки інформації в ІКС

Аналіз методів автентифікації і авторизації в забезпеченні безпеки інформаційних систем наведено в розділі 1.2 Додатку А.

Таким чином в системах захисту інформації автоматизованих систем може бути реалізовано декілька механізмів автентифікації, а саме:

- Автентифікація користувача системи;
- Автентифікація вузла доступу до ІКС;
- Автентифікація каналу передачі інформації;
- Автентифікація відправника інформації;
- Автентифікація отримувача інформації.

1.2. Особливості забезпечення автентифікації сервісами безпеки операційної системи Windows

Результат аналізу [4-7] щодо реалізації механізмів автентифікації в найбільш поширених ОС Windows 10, 11 pro наведено в таблиці 1.

Таблиця 1.

Параметри автентифікації	Опис реалізації	переваги (Забезпечує)	Недоліки (Не дозволяє)	Висновок
При обміні	Протокол Kerberros мережевий протокол автентифікації, що дозволяє передавати дані через незахищені мережі для безпечної ідентифікації	Дозволяє передавати дані через незахищені мережі для безпечної ідентифікації	Не достатня захищеність як для мережевого протоколу	мережеві дані можна перехопити або вивести з ладу серверні дані в мережі.
Користувача та робочої станції	ОС Windows налаштування логінів та паролів, розподіл доступу	Оновлення системи та драйверів периферійних пристроїв	Просто проводить різні оновлення	При проведенні оновлення ОС та драйверів, можуть бути відмінені налаштування послуг безпеки

Проведений аналіз, показує що ОС Windows 10, 11 забезпечує послуги

безпеки: Ідентифікація і автентифікація, Ідентифікація і автентифікація при обміні, але не забезпечує таки важливі послуги, а саме Автентифікація відправника, автентифікація одержувача.

1.3. Методи реалізація автентифікації програмно-апаратними засобами технічного захисту інформації

Для забезпечення багатофакторної автентифікації в Україні застосовуються розробки відчизняних виробників. Для операційних систем Windows додатково встановлюються програмні засоби захисту інформації від несанкціонованого доступу та криптографічного захисту інформації, наприклад Тайфун-WEB та Гриф-4. Аналіз литератури [10,11], надає можливість визначити які методи та засоби забезпечення послуг автентифікації в них реалізовані. Загальна характеристика, переваги та недоліки наведено в таблиці 2.

Таблиця 2.

Complex grif	Typhon-web	ОС Windows
Забезпечує автентифікацію користувачів (на робочих станціях) (за вибором однофакторна/двофакторна)	Взаємна автентифікація клієнта та сервера із використанням симетричних криптографічних алгоритмів.	SRM (Security Reference Monitor – монітор безпеки) - забезпечує дотримання політики безпеки на локальному комп'ютері. (однофакторна автентифікація)
Забезпечує створення достовірного каналу використовуваного при початковій ідентифікації.	Захист конфіденційності та цілісності інформації, що передається між клієнтом та сервером з використанням алгоритму симетричного шифрування. (автентифікація вузла доступу)	IPSec (IP Security) – набір протоколів для забезпечення захисту даних, що передаються з використанням міжмережевого протоколу IP. Автентифікація вузла доступу.
Забезпечують автентифікацію користувачів на підставі введення ними паролів.	Розмежування доступу користувачів до інформації ресурсів у вигляді статичних веб сторінок , що зберігаються на сервері.	Device Guard - надає сервіс HVCI (Hypervisor Code Integrity) для посилення гарантій підписування коду

Таким чином, операційні системи Windows забезпечують ФБП (функціональні послуги безпеки) спостережності та автентифікації **НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1** (розкриття позначень наведено в розділі А.3 додатку А).

Програмні засоби ТЗІ додатково забезпечують реалізацію послуг **НЦ-1, НТ-2, НВ-2.**

Але при цьому використовується тільки мережа передача даних (інтернет) трафік якої може бути перехоплено, а інформація спотворена або замінена на хибну.

Тому запропоновано використання автономного програмного застосунку, який по додатковому каналу забезпечує автентифікацію відправника та отримувача інформації та дозволяє досягнути двофакторну автентифікацію на базі ФБП ОС Windows + АЗПГ (автономний застосунок Павла Гордіна) а саме:

НИ-1,НИ-2, НК-1, НВ-1 + НИ-3, НК-2, НА-1, НП-1

Windows забезпечує :

НИ-1 Зовнішню ідентифікацію і автентифікацію;

НИ-2 Одиночну ідентифікацію і автентифікацію;

НК-1 Однонаправлений достовірний канал;

НВ-1 Автентифікацію вузла.

В наступному розділі розглядається програмний застосунок та методи його використання, які дозволяють досягнути наступних послуг безпеки:

НИ-3 Множину ідентифікацію;

НК-2 Двонаправлений достовірний канал;

НА-1 Базову автентифікацію відправника;

НП-1 Базову автентифікацію користувача.

2. Розробка автономного методу двофакторної автентифікації в інформаційно-комунікаційних системах з використанням операційних систем Windows

2.1 Обрання методів та засобів підвищення рівня спостережності до двофакторної автентифікації

На підставі аналізу переваг та недоліків двофакторної автентифікації, було обрано криптографічний алгоритм RSA як додатковий до методів та алгоритмів OAuth, Kerberos, OpenID, які використовуються в ОС Windows.

Опис криптографічних алгоритмів, які використовуються з метою автентифікації наведено в таблиці А.1 додатку А.

Загальна схема генерації особистих ключів користувачів та формування сеансового ключа наведена на рисунку 2.1.

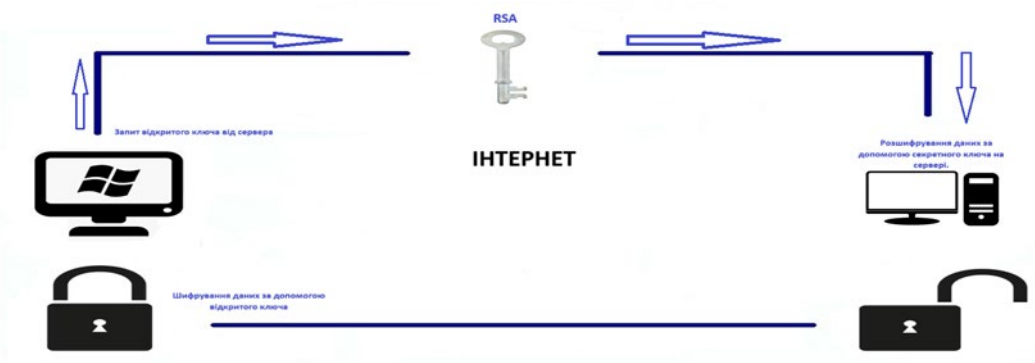


Рис. 2.1 Схема формування сеансового ключа

В контексті інформаційно-комунікаційних систем (ІКС), додатковий механізм автентифікації на основі RSA реалізований для забезпечення безпеки доступу до системи, з'ємного носія RSA (MicroCD, token, USB flash, тощо), що генерують одноразові ключі. Користувачам виділяються апаратні або програмні ключі, які використовуються для автентифікації. По додатковому каналу мобільного зв'язку користувачі, здійснюють обмін приватними (відкритими) ключами. Цей метод забезпечує двосторонню автентифікацію клієнт - сервер, клієнт - клієнт.

Для реалізації алгоритму генерації особистих ключів користувачів було обрано та додатково підключено кріптографічні бібліотеки, показані в таблиці 3.

Таблиця 3.

Позначення	Опис (призначення)
Include<iosteam>	Оголошує об'єкти, що керують читанням із стандартних потоків та записом у них. заголовок, для виконання даних програми C++
Include<stdio.h>	Заголовний файл стандартної бібліотеки мови Сі, що містить визначення макросів, констант та оголошення функцій і типів, призначених для виконання операцій введення та виведення.
Include<stdlib.h>	Заголовний файл стандартної бібліотеки мови Сі, який містить у собі функції, що займаються виділенням пам'яті, контролем процесу виконання програми, перетворенням типів та інші.
Include<exception>	Структурована обробка винятків (SEH) - це розширення корпорації Майкрософт для C і C++ для обробки певних виняткових ситуацій коду, таких як помилки обладнання.
Include<string>	Клас з методами та змінними для організації роботи з рядками у мові програмування C++
Include<memory>	Концепція в розробці програмного забезпечення, метою якої є запобігти виникненню програмних помилок, що призводять до уразливостей пов'язаних з доступом до оперативної пам'яті комп'ютера, таким як переповнення буфера, завислі вказівники тощо

Ці бібліотеки дозволять працювати з виведенням та введенням тексту, з математичними формулами та функціями, які потрібні для реалізації RSA, а також з рядками, підрахунком часу, двома головними файлами, які містять всі необхідні дані для роботи алгоритму шифрування RSA функції. Крім того створенно два нових класи BigInteger та RSABigInteger, які реалізують генерацію випадкового (простого) числа та ключа.

2.2. Розробка додаткових програмних модулів генерації разового (сеансового) ключа

Принцип формування та обміну ключами для клієнт-серверної структури ІКС наведено на рисунку 2.1, особливістю структури клієнт-клієнт є наявність додаткового каналу зв'язку між ними.

Для розробки програмного застосунку обрано кріптобібліотеки. Програмний код двох модулів BigInteger та RSABigInteger написаний на мові C++.

Додано два нових класи (розроблено особисто).

На рисунку А.5 наведено порядок формування разового (сеансового) відкритого ключа, шляхом виділення по одному байту з двох послідовностей та математичну операцію над ними.

У програмі виконано спрощення роботи з нею - операції з числами. Це потрібно для спрощення реалізації програми і для того, щоб позбавитися необхідності створення окремого алфавіту для роботи з нею. Приклад того, як це виглядає, представлений на рисунку А.6.

Таким чином, не потрібно використовувати конвертер для переведення цифр у літери, що прискорює роботу всієї програми. Але для створення великих чисел введено два класи (генерації довгих (більш 56 бітових) ключів) - BigInteger та RSABigInteger, представлені на рисунках 2.2, 2.3.

```
#ifndef RSABIGINTEGER_H
#define RSABIGINTEGER_H
#include "BigInteger.h"

class RSABigInteger
{
    public:
        RSABigInteger(int nSize);
        virtual ~RSABigInteger();

        void CalculateD(BigInteger& e, BigInteger& phi, BigInteger& d);
        void init(BigInteger&p, BigInteger& q);
        void eGeneration(BigInteger& phi,BigInteger& result);
        void encryption(BigInteger& msg, BigInteger& code);
        void decryption(BigInteger& code, BigInteger& msg);
        void randomNGeneration(BigInteger& randResult, int n);
        void primeNumberGeneration(BigInteger& randPrime, int n);

    private:
        int SIZE;
        BigInteger N;
        BigInteger d;
        BigInteger e;
};

#endif // RSABIGINTEGER_H
```

```
#ifndef BIGINTEGER_H
#define BIGINTEGER_H

class BigInteger
{
    public:
        int nSize;
        unsigned int *digit;
        BigInteger();
        BigInteger(int n);
        BigInteger(const BigInteger &obj);
        ~BigInteger();

        void addBigInteger(BigInteger& a, BigInteger& b);
        void subBigInteger(BigInteger& a, BigInteger& b);
        void multBigInteger(BigInteger& a, BigInteger& b);
        void copyBigInteger(BigInteger& a, int index);
        void expoModNBigInteger(BigInteger& x, BigInteger& y, BigInteger& N, BigInteger& result);
        void setSize(int n);
        int msbBigInteger();
        void clearBigInteger();
        void showDigits();
        void setDigits(int index);
};

int Compare(BigInteger& first, BigInteger& second);
int divBigInteger(BigInteger& u, BigInteger& v, BigInteger& q, BigInteger& r);
void gcdBigInteger(BigInteger& a, BigInteger& b, BigInteger& result);

#endif // BIGINTEGER_H
```

Рис. 2.2. RSABigInteger

Рис. 2.3 BigInteger

Функції, які використовуються в програмі, перераховані на рисунках А.5 і А.6.

Спочатку відбувається генерація двох простих чисел p та q. Для цього в класі RSABigInteger запускається функція primeNumberGeneration, яка генерує випадкове велике число і перевіряє його на простоту. Потім генерується кілька об'єктів класу BigInteger, частина з яких використовується тимчасово. Фрагмент коду міститься на рисунку 2.4.

```
void RSABigInteger::primeNumberGeneration(BigInteger& randPrime, int n)
{
    BigInteger valueOne(randPrime.nSize);
    valueOne.digit[0] = 1;
    BigInteger valueTwo(randPrime.nSize);
    valueTwo.digit[0] = 2;
    BigInteger valueThree(randPrime.nSize);
    valueThree.digit[0] = 3;

    BigInteger tempPrime(randPrime.nSize);
    BigInteger tempExpoDummy(randPrime.nSize);
    BigInteger ExpoDummy(randPrime.nSize);

    BigInteger tempRemainder(randPrime.nSize);
    BigInteger tempPrimeMinusOne(randPrime.nSize);
    randomNGeneration(tempPrime,n);

    while(1)
    {
        tempPrimeMinusOne.clearBigInteger();
        tempRemainder.clearBigInteger();
        ExpoDummy.clearBigInteger();
        tempExpoDummy.clearBigInteger();
        tempPrimeMinusOne.subBigInteger(tempPrime, valueOne);

        ExpoDummy.expoModNBigInteger(valueTwo, tempPrimeMinusOne, tempPrime, tempRemainder);

        if(tempRemainder.msbBigInteger()==0 && tempRemainder.digit[0]==1)
        {
            cout<<"Prime Number Generating ... Wait a little bit\n";
            tempRemainder.clearBigInteger();
            tempExpoDummy.expoModNBigInteger(valueThree, tempPrimeMinusOne, tempPrime, tempRemainder);
            if(tempRemainder.msbBigInteger()==0 && tempRemainder.digit[0]==1)
            {
                break;
            }
        }
        tempPrime.clearBigInteger();
        randomNGeneration(tempPrime,n);
    }
    randPrime.copyBigInteger(tempPrime,0);
}
```

Рис. 2.4 Генерація випадкого великого числа

Далі здійснюється операція виводу числа на екран. Приклад коду наведено

на рисунку 2.5.

```
void BigInteger::showDigits()
{
    int nonZeroDigitFlag =0;
    for(int i=(nSize-1);i>=0; i--)
    {
        if(digit[i]!=0)
        {
            nonZeroDigitFlag=1;
        }
        if(nonZeroDigitFlag==1)
        {
            printf("%u ",digit[i]);
        }
    }

    if(nonZeroDigitFlag ==0)
    {
        printf("0");
    }
    cout << endl;
}
```

Рис. 2.5. Вивод випадкового числа

По закінченні генерації випадкових чисел, здійснюється формування даних для роботи алгоритму RSA, таких як N, d, e. Фрагмент коду представлено на рисунку 2.6.

```
void RSABigInteger::init(BigInteger&p, BigInteger& q)
{
    N.multBigInteger(p,q);
    BigInteger one(p.nSize);
    one.digit[0] = 1;
    BigInteger phi(p.nSize);

    BigInteger tempP(p.nSize), tempQ(p.nSize);

    tempP.subBigInteger(p,one);
    tempQ.subBigInteger(q,one);

    phi.multBigInteger(tempP,tempQ);
    cout<<"\nGenerated 'phi' :"<<endl;
    phi.showDigits();
    eGeneration(phi,e);
    cout<<"\nGenerated 'e' :"<<endl;
    e.showDigits();
    CalculateD(e,phi,d);
    cout<<"\nGenerated 'd' :"<<endl;
    d.showDigits();
}
```

Рисунок 2.6. Генерація и виведення чисел

Але для генерації d та e програмою використовуються спеціально зроблені для цього функції EGeneration та CalculateD. EGeneration шукає найбільший спільний дільник функції. Для цього в функцію повідомляється (N) і результат, в яку заноситиметься e. Фрагмент коду EGeneration представлений рисунку 2.7.

```
void RSABigInteger::init(BigInteger&p, BigInteger& q)
{
    N.multBigInteger(p,q);
    BigInteger one(p.nSize);
    one.digit[0] = 1;
    BigInteger phi(p.nSize);

    BigInteger tempP(p.nSize), tempQ(p.nSize);

    tempP.subBigInteger(p,one);
    tempQ.subBigInteger(q,one);

    phi.multBigInteger(tempP,tempQ);
    cout<<"\nGenerated 'phi' :"<<endl;
    phi.showDigits();
    eGeneration(phi,e);
    cout<<"\nGenerated 'e' :"<<endl;
    e.showDigits();
    CalculateD(e,phi,d);
    cout<<"\nGenerated 'd' :"<<endl;
    d.showDigits();
}
```

Рис.2.7 Обрахування e

Для обчислення числа d у функцію CalculateD вводиться значення функції, і число e. Далі вираховується значення d. Після всіх підрахунків функція копіює значення d в переданий до неї заздалегідь BigInteger d. Фрагмент коду генерації d представлений на рисунку 2.8.

```
void RSABigInteger::CalculateD(BigInteger& e, BigInteger& phi, BigInteger& d)
{
    int i =0;
    BigInteger temp1(phi.nSize),temp2(phi.nSize),quotient(phi.nSize),remainder(phi.nSize);
    BigInteger one(phi.nSize);
    one.digit[0] = 1;
    BigInteger k(phi.nSize);
    while(true)
    {
        i++;
        k.digit[0] = i;
        temp1.multBigInteger(k,phi);
        temp2.addBigInteger(temp1,one);
        divBigInteger(temp2,e,quotient,remainder);
        if(remainder.msbBigInteger() == 0 && remainder.digit[0] == 0)
        {
            d.copyBigInteger(quotient,0);
            break;
        }
    }
}
```

Рис. 2.8. Генерація d

Після створення та генерації всіх потрібних змінних програма генерує випадкову змінну RSABigInteger, що складається з випадкової послідовності цифр. Ця послідовність цифр потім буде зашифрована та розшифрована із застосуванням алгоритму RSA. Для цього викликаються функції encryption та decryption, які використовують функцію expoModNBigInteger для шифрування та

дешифрування повідомлень. Результат наведено на рисунках 2.9 та 2.10.

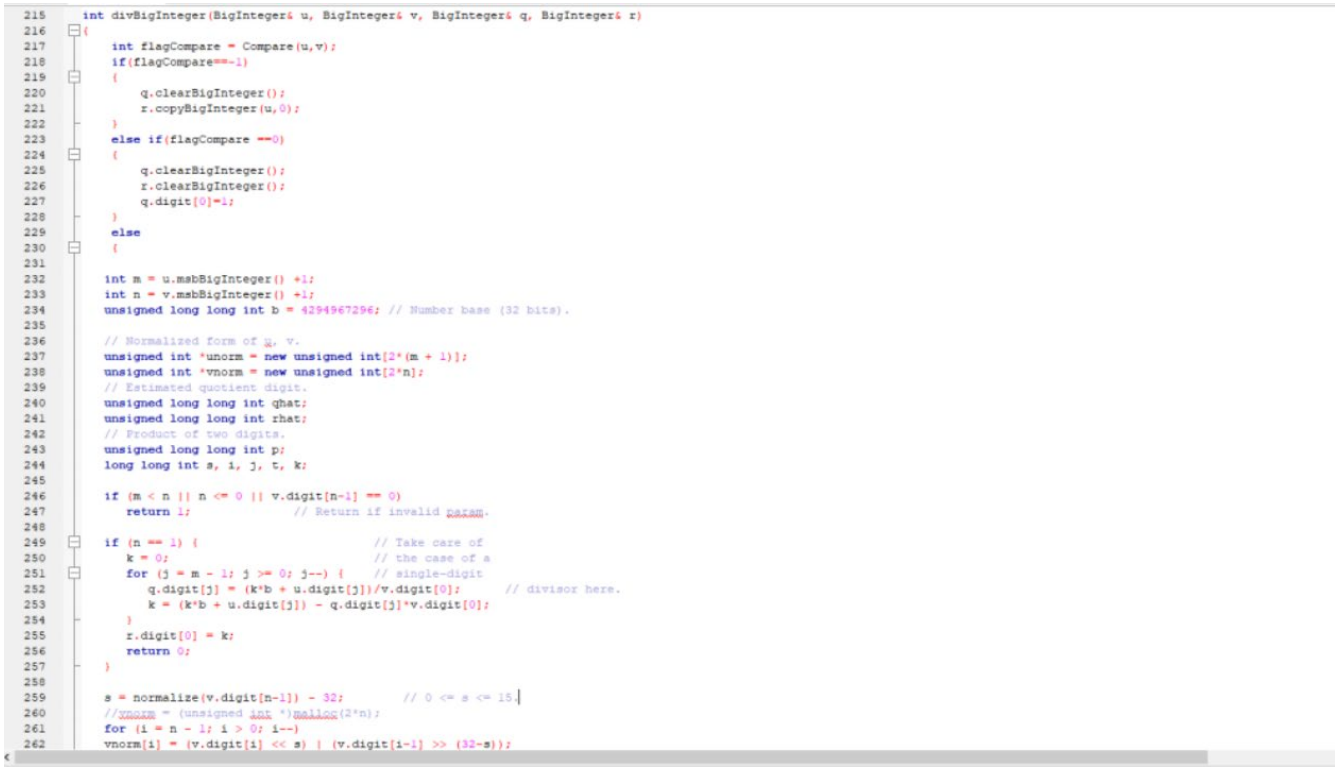
```
void RSABigInteger::encryption(BigInteger& msg, BigInteger& code)
{
    BigInteger temp(SIZE);
    temp.expoModNBigInteger(msg, e, N, code);
}

void RSABigInteger::decryption(BigInteger& code, BigInteger& msg)
{
    BigInteger temp(SIZE);
    temp.expoModNBigInteger(code, d, N, msg);

}
```

Рис. 2.9. Функції encryption и decryption

```
void BigInteger::expoModNBigInteger(BigInteger& x, BigInteger& y, BigInteger& N, BigInteger& result)
{
    if (y.msbBigInteger() == 0 && y.digit[0] ==0)
    {
        result.digit[0] = 1;
        for (int i = 1; i < result.nSize; i++)
        {
            result.digit[i] = 0;
        }
    }
    else
    {
        BigInteger temp(nSize);
        BigInteger reminder(nSize);

        BigInteger value2(nSize);
        value2.digit[0]=2;
        divBigInteger(y,value2, *this, reminder);

        temp.copyBigInteger(*this, 0);
        expoModNBigInteger(x, temp,N, result);

        multBigInteger(result, result);

        temp.copyBigInteger(*this, 0);

        if (y.digit[0] % 2 != 0)
        {
            multBigInteger(temp, x);
            temp.copyBigInteger(*this, 0);
        }
        BigInteger q(nSize), r(nSize);
        divBigInteger(temp, N,q,r);
        result.copyBigInteger(r,0);
    }

    return;
}
```

Рис. 2.10. Функція expoModNBigInteger

У функцію expoModNBigInteger створюється оригінальне повідомлення, ключі та порожній BigInteger для запису в нього результату. Також програма використовує інші функції класу BigInteger, таку як divBigInteger. Фрагмент коду divBigInteger представлений рисунку 2.11.



```
int divBigInteger(BigInteger& u, BigInteger& v, BigInteger& q, BigInteger& r)
{
    int flagCompare = Compare(u,v);
    if(flagCompare==-1)
    {
        q.clearBigInteger();
        r.copyBigInteger(u,0);
    }
    else if(flagCompare ==0)
    {
        q.clearBigInteger();
        r.clearBigInteger();
        q.digit[0]=1;
    }
    else
    {

   int m = u.msbBigInteger() +1;
   int n = v.msbBigInteger() +1;
   unsigned long long int b = 4294967296; // Number base (32 bits).

   // Normalized form of u, v.
   unsigned int *unorm = new unsigned int[2*(m + 1)];
   unsigned int *vnorm = new unsigned int[2*n];
   // Estimated quotient digit.
   unsigned long long int qhat;
   unsigned long long int rhat;
   // Product of two digits.
   unsigned long long int p;
   long long int s, i, j, t, k;

   if (m < n || n <= 0 || v.digit[n-1] == 0)
      return 1;             // Return if invalid param.

   if (n == 1) {                        // Take care of
      k = 0;                            // the case of a
      for (j = m - 1; j >= 0; j--) {    // single-digit
         q.digit[j] = (k*b + u.digit[j])/v.digit[0];      // divisor here.
         k = (k*b + u.digit[j]) - q.digit[j]*v.digit[0];
      }
      r.digit[0] = k;
      return 0;
   }

   s = normalize(v.digit[n-1]) - 32;        // 0 <= s <= 15.
   //vnorm = (unsigned int *)malloc(2*n);
   for (i = n - 1; i > 0; i--)
   vnorm[i] = (v.digit[i] << s) | (v.digit[i-1] >> (32-s));
```

Рис. 2.11. bigDivInteger

Таким чином розроблено програмний застосунок, який забезпечує виконання наступних операцій:

- Автоматичну генерацію випадкових простих чисел;
- генерацію особистих та сеансових (відкритого та закритого) ключів;
- шифрування та дешифрування повідомлень.

Шифрування та дешифрування здійснюються одночасно. Розроблений алгоритм забезпечує додаткову автентифікацію користувачів (відправника та отримувача інформації).

2.3. Рекомендації застосування автономної системи додаткової автентифікації в ІКС з використанням ОС Windows

Наведені в даному розділі рекомендації спрямовані на практичне досягнення двофакторної авторизації в ІКС з використанням операційної системи Microsoft Windows 10 Professional.

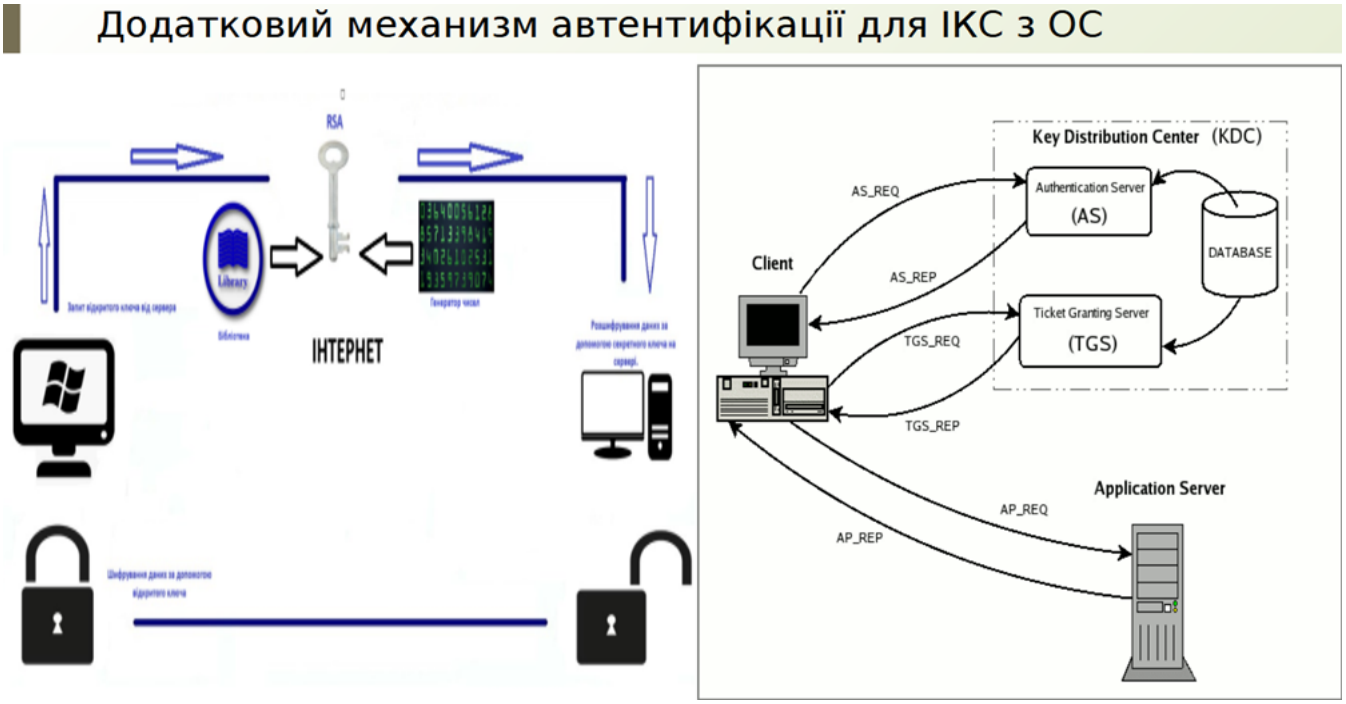


Рис 2.12

Загальний порядок використання програмного засобу:

1. Кожному користувачу видається носій програмного застосунку, який можна під’єднувати до мобільних засобів зв’язку та робочих станцій автоматизованих систем з використання ОС Windows.

2. Користувач запускає застосунок на генерацію разового ключа та формує push повідомлення, яке відправляється на сервер або іншому клієнту автоматизованої системи.

3. При отримані зворотного push повідомлення від сервера або іншого клієнта воно зберігається та вноситься в програмний застосунок.

4. З’ємні носії користувачами підключаються до робочих станцій автоматизованої системи для використання сеансового ключа при шифруванні та дешифруванні повідомлень.

На основі згенерованого та отриманого push повідомлення, здійснюється формування сеансового разового ключа.

В контексті інформаційно-комунікаційних систем (ІКС), додатковий механізм автентифікації на основі RSA реалізований для забезпечення безпеки доступу до системи, з’ємного носія RSA (MicroCD, token, USB flash, тощо), що генерують одноразові ключі. Користувачам виділяються апаратні або програмні ключі, які використовуються для автентифікації. По додатковому каналу мобільного зв’язку користувачі, здійснюють обмін приватними (відкритими) ключами. Цей метод забезпечує двосторонню автентифікацію клієнт - сервер, клієнт - клієнт.

ВИСНОВКИ

В ході виконання роботи здійснено розробку технологічного рішення – програмного застосунку реалізації двофакторної автентифікації для інформаційно-комунікаційних систем, захист інформації в яких побудово на використанні сервісів безпеки операційних систем Windows та розробка рекомендацій щодо його використання на практиці малого та середнього бізнесу, а саме:

- Проведено аналіз сучасних програмних засобів ТЗІ і відповідних модулів автентифікації та обрано автономну систему для проектування.

- Обрано криптобібліотеки та розроблено додаткові програмні модулі генерації разового ключа.

- Розроблено рекомендації щодо впровадження цього застосунку в ІКС.

Запропонований у роботі автономний програмний застосунок та отримані результати дозволяють покращити механізм автентифікації Windows. В ході виконання дипломної роботи магістра був запропонований автономний, додатковий метод автентифікації а також був реалізований програмний продукт, який відрізняється від наявних криптографічних бібліотек, додаванням додаткових класів.

Програмно-апаратна реалізація застосунку може підключатися до мобільних засобів зв’язку та робочих станцій автоматизованих систем, або знаходитись віддалено на сервері.

Перелік джерел посилання

1. Г.Ф. Конахович та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.

2. Г.М. Гулак та інші. Основи криптографічного захисту інформації.-К.: ІММ НАНУ, 2011.-200 с.

3. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. *Навчальний посібник*. – Вінниця: ВНТУ, 2009. – 268 с.

4. С.Я. Довбня, П.П. Наталенко. Основи використання, адміністрування та забезпечення захисту інформації в автоматизованих системах: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2017. – 164 с.

5. С.Я. Довбня. Підготовка користувачів та адміністраторів ЗАТК "Персонал-Командування" з технічного захисту інформації: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2018. – 280 с.

6. Виноградов І.М. Основа теорії чисел: 1949.-180с.

7) [Електронний ресурс] – Режим доступу до ресурсу: https://www.jstor.org/

8) [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/

9) [Електронний ресурс] – Режим доступу до ресурсу: https://scholar.google.com.ua/

10) [Електронний ресурс] – Режим доступу до ресурсу: https://books.google.com/ngrams

11. Коутинхо С.А., Ланцо С.К Ведення в теорію чисел. Алгоритм RSA, 2001

12. Макаров А.С. Теорія практики хакерских атак 2015

13. Мао В: Сучасна криптографія теорія і практика. 2005.-768с.

14. Орлов В, В., Алексеев А.П Стенографічні і криптографічні методи захисту інформаціїї 2010 -288с.

15. Шилдт Г. С++ Руководство для початківців 2005.-67с.

16. Welch P., Codes and Cryptography, London: Oxford university press, 1988-

272с.

17. Skobic V, Dokic B., Ivanovic Z., Hardware Modules of the RSA//serdian journal of electrical engineering.2014.,-121с.

18. https://authy.com/what-is-2faa/12.03.2024

19. А.Сулавко.А Еременко с 20-25. Двофакторна аутентифікація користувачів комп'ютерних систем на віддаленому сервері за клавіатурним почерком

20.https://www.techtarget.com/searchsecurity/definition/two-factor-authentication/12.03.2024

21.https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa/12.03.2024

ДОДАТОК А

Опис методів забезпечення автентифікації в інформаційно-комунікаційних системах

А.1. Методи захисту інформації

Поняття	Опис
Шифрування	Процес перетворення даних у зашифрований вигляд для забезпечення конфіденційності
Дешифрування	Зворотний процес, коли зашифровані дані повертаються до вихідного вигляду
Ключ	Секретна інформація, що використовується в алгоритмі шифрування для перетворення даних
Криптографічний протокол	Сукупність кроків та правил для виконання безпечних криптографічних операцій
Протокол SSL/TLS	Протоколи забезпечують шифрування даних під час передачі через Інтернет, забезпечуючи безпечне з'єднання.
Ключеве управління	Процес генерації, зберігання та керування ключами шифрування для забезпечення безпеки
Криптографічні засоби	Інструменти, методи та алгоритми для реалізації криптографічного захисту інформації

Шифрування даних: криптографічні алгоритми використовуються для шифрування конфіденційної інформації перед її передачею через мережу або зберігання на носіях даних. Це забезпечує конфіденційність даних, оскільки навіть якщо дані отримає несанкціонована особа, вони будуть незрозумілими без відповідного ключа.

КЗІ дозволяють встановлювати процеси аутентифікації користувачів та перевірки їх прав доступу до різних ресурсів. Це забезпечує, що тільки авторизовані користувачі мають доступ до конфіденційної інформації, а також дозволяє відстежувати дії користувачів для забезпечення аудитування.

Ключі шифрування і підпису є критично важливими компонентами КЗІ. Система повинна забезпечити їх безпеку від несанкціонованого доступу, наприклад, шляхом використання криптографічних модулів або застосування

методів апаратного захисту. КЗІ повинні бути розроблені з урахуванням потенційних загроз безпеці, таких як атаки з використанням вразливостей програмного забезпечення, соціально-інженерні атаки або криптоаналіз. Це може включати регулярне оновлення програмного забезпечення та використання стійких криптографічних алгоритмів. КЗІ мають вбудовані механізми для управління ключами шифрування і підпису, а також цифровими сертифікатами. Це включає генерацію, зберігання, розподіл, відновлення та відкликання ключів і сертифікатів. Загалом, ІКС з використанням КЗІ створюють комплексну систему захисту інформації, яка забезпечує конфіденційність, цілісність та доступність даних, а також захист від різних видів загроз безпеці.

Принципи сучасної криптографії базуються на забезпеченні конфіденційності, цілісності та автентифікації інформації шляхом використання математичних алгоритмів. Ось деякі ключові принципи:

Конфіденційність: криптографічні алгоритми забезпечують захист інформації від несанкціонованого доступу. Це досягається шляхом застосування алгоритмів шифрування, які перетворюють зрозумілий текст у незрозумілий (шифртекст).

Цілісність: криптографічні методи дозволяють перевіряти цілісність даних, тобто визначати, чи були дані змінені під час передачі. Це досягається за допомогою хеш-функцій, які генерують унікальний "відбиток" для даних.

Автентифікація: криптографія також дозволяє перевіряти автентичність користувача або джерела інформації. Це виконується за допомогою цифрових підписів або аутентифікаційних протоколів.

Необхідність ключа: У сучасних криптографічних системах ключі грають критичну роль. Вони використовуються для шифрування та розшифрування даних, підпису або перевірки цілісності. Забезпечення безпеки ключів є важливою складовою цих систем

Стійкість до атак: сучасні криптографічні алгоритми розроблені з урахуванням стійкості до різних видів криптоаналізу, таких як атаки з використанням силового перебору, атаки на основі знання частини даних і т.д.

Ефективність: Криптографічні алгоритми повинні бути достатньо швидкими для застосування у реальному часі і мати мінімальний вплив на продуктивність системи, де вони використовуються.

Ці принципи формують основу для розробки та застосування сучасних криптографічних систем, які забезпечують безпеку в інформаційному просторі.

А.2 Захист від несанкціонованого доступу

Автентифікація дозволяє перевірити, що користувач є тим, за кого він себе видає, тоді як авторизація визначає, які дії або ресурси має право виконувати або отримувати цей користувач. Це допомагає уникнути несанкціонованого доступу до конфіденційної інформації або функціоналу системи.

Забезпечення конфіденційності: Якщо аутентифікація не була б проведена належним чином, то втрачається контроль над тим, хто має доступ до конфіденційної інформації. Це може призвести до витоку даних або порушення конфіденційності.

Забезпення цілісності даних: Часто аутентифікація також включає в себе перевірку цілісності даних, щоб упевнитися, що дані не були змінені під час передачі або зберігання.

Аудит та відповідність : Аутентифікація і авторизація дозволяють стежити за діями користувачів і забезпечувати відповідність з правилами і політиками безпеки. Це важливо для аудитування та виявлення порушень безпеки.

Зменшення ризику: Правильна аутентифікація і авторизація допомагають зменшити ризик порушення безпеки, так як вони обмежують доступ до системи та її ресурсів тільки авторизованим користувачам.

А.3. Поняття послуг автентифікації в системі критерія спостережності системи захисту інформації в автоматизованих системах

КД — довірча конфіденційність;

КА — адміністративна конфіденційність;

КО — повторне використання об'єктів;

КК — аналіз прихованих каналів;

КВ — конфіденційність при обміні;

ЦД — довірча цілісність;

ЦА — адміністративна цілісність;

ЦО — відкат;

ЦВ — цілісність при обміні;

ДР — використання ресурсів;

ДВ — стійкість до відмов;

ДЗ — гаряча заміна;

ДВ — відновлення після збоїв;

НР — реєстрація;

НИ — ідентифікація і автентифікація;

НК — достовірний канал;

НО — розподіл обов'язків;

НЦ — цілісність КЗЗ;

НТ — самотестування;

НВ — автентифікація при обміні;

НА — автентифікація відправника;

НП — автентифікація одержувача.

Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими

послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Забезпечує критерііїї	Критерії реєстрацііїї в Windows
НР-1 зовнішній аналіз	Політика реєстрацііїї, що реалізується КЗЗ,повина визначати перелік подій, що реєструються.КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.
НР-2 захищений журнал	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події .КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту.КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Реєстрація комплексу захисту інформації (КЗІ), що включає в себе технічні, організаційні та правові заходи для захисту конфіденційної інформації. Процедури реєстрації такого комплексу можуть відрізнятися в залежності від країни та її законодавства

Зазвичай реєстрація КЗІ(Комплекс захисту інформації) може включати такі кроки:

- Аналіз потреб: Визначення обсягу і типу інформації, яку необхідно захищати, та визначення потрібних заходів для забезпечення безпеки.
- Підготовка документації: Створення політик, процедур і правил, пов'язаних з захистом інформації. Це може включати політику доступу до інформації, процедури реагування на інциденти безпеки, тощо.
- Технічні заходи: Впровадження технічних засобів захисту інформації, таких як файрволи, антивірусне програмне забезпечення, системи контролю доступу тощо.
- Навчання та свідомість персоналу: Навчання співробітників щодо правил безпеки і захисту інформації, а також створення культури безпеки в організації.
- Аудит і пітримка: Регулярне проведення аудитів безпеки для перевірки ефективності заходів і внесення необхідних змін для підтримки безпеки..У багатьох країнах можуть існувати спеціальні вимоги до реєстрації КЗІ, зокрема щодо збору та обробки конфіденційної інформації.

Реєстрація операційної системи Windows зазвичай не є процесом, який потребує введення критеріїв у звичайному розумінні. Зазвичай, коли ви встановлюєте Windows на вашому комп'ютері, ви повинні ввести ключ продукту або активаційний ключ, який ви отримали разом із ліцензійними матеріалами.

Однак, є кілька загальних критеріїв, які можна вказати щодо реєстрації Windows:

1.Легальність ліцензії: Ви повинні мати легальну ліцензійну копію операційної системи Windows. Використання піратських копій не тільки незаконне, а й може призвести до проблем з безпекою та стабільністю системи.

2. Введення ключа продукту: Під час установки або активації Windows вам буде запропоновано ввести ключ продукту. Це є необхідним кроком для активації вашої копії Windows

3. Активація: Після введення ключа продукту, ви повинні активувати свою копію Windows за допомогою Інтернету або шляхом телефонної активації. Цей крок підтверджує вашу легальність користування продуктом.

Зазвичай ці критерії достатньо для реєстрації Windows. Важливо відзначити, що правила активації та реєстрації можуть змінюватися в залежності від версії Windows та регіона.

Аналіз зовнішнього середовища (ЗС) є важливою складовою стратегічного управління для будь-якої організації, включаючи НР-1. Зовнішній аналіз передбачає оцінку факторів, які можуть впливати на діяльність організації, але перебувають поза її контролем. Ось деякі аспекти, які можна включити в зовнішній аналіз НР-1:

Технологічне середовище: Включає технологічні інновації, технологічні зміни та технологічний прогрес, які можуть створювати нові можливості або загрози для НР-1. Наприклад, розвиток нових енергоефективних технологій. Захищені журнали є важливими засобами для збереження конфіденційної інформації та захисту від несанкціонованого доступу.

Ось деякі особливості і переваги захищених журналів, які можуть відноситися до НР-2:

1. Конфіденційність: Захищені журнали забезпечують конфіденційність інформації, що в них зберігається, за допомогою шифрування або інших заходів безпеки. Це дозволяє уникнути несанкціонованого доступу до важливих даних.

2. Цілісність даних: Захищені журнали забезпечують цілісність даних, що в них зберігається, шляхом використання методів перевірки цілісності та контролю доступу.

3. Аудит і відслідковування: Деякі захищені журнали можуть надавати можливість вести аудит і відслідковувати дії користувачів, які мають доступ до журналу. Це дозволяє виявити та відстежувати потенційні порушення безпеки.

4. Резервне копіювання і відновлення: Деякі захищені журнали можуть мати вбудовані засоби резервного копіювання та відновлення даних, що забезпечують безпеку та надійність зберігання інформації.

5. Широкі можливості налаштування: Захищені журнали часто надають широкі можливості налаштування, що дозволяє забезпечити відповідність конкретним вимогам безпеки організації.

6. Законні вимоги: Захищені журнали можуть допомогти виконати вимоги щодо зберігання і аудиту інформації відповідно до законодавства або стандартів безпеки.

Зовнішній аналіз для НР-2, організації, яка працює з захищеними журналами:

1. Технологічні тенденції: Оцінка технологічних тенденцій у сфері захищених журналів, включаючи розвиток шифрування, методів аутентифікації та інших технологій безпеки.

2. Конкуренція: Аналіз конкурентів, які також працюють у сфері захищених журналів, їхніх стратегій, продуктів та послуг, а також їхніх сильних та слабких сторін.

3. Законодавство та регуляція: Оцінка законодавчих вимог та регуляторного середовища, що стосуються зберігання та обробки конфіденційної інформації. Це може включати вимоги до захисту даних, стандарти безпеки тощо.

4. Попит на захищені журнали: Аналіз попиту на захищені журнали серед клієнтів та ринкові тенденції у цьому сегменті.

5. Міжнародні фактори: Врахування міжнародних факторів, які можуть впливати на ринки та регуляторне середовище, особливо якщо НР-2 працює або має клієнтів за межами своєї країни.

6. Тенденції ринку: Аналіз загальних тенденцій у сфері інформаційної безпеки та збереження конфіденційної інформації, включаючи популярність захищених журналів серед різних сегментів ринку.

7. Економічне середовище: Оцінка економічних факторів, таких як доступність капіталу та здатність ринку підтримувати витрати на розробку та впровадження нових технологій безпеки.

Ці аспекти допоможуть НР-2 отримати глибше розуміння зовнішнього середовища та підготувати стратегії для забезпечення конкурентоспроможності та успіху в її сегменті ринку.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації.

Запезпечує критерії	Критерііі в Windows	Критерііі автономного застосунку Павла Гордіна
НИ - 1 Зовнішня ідентифікація і автентифікація	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.	-
НИ - 2 Одиночна ідентифікація і автентифікація	Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.автентифікувати цього користувача з використанням захищеного механізму .	-
НИ - 3 Множина ідентифікація та автентифікація.	-	Автентифікувати цього користувача з використанням захищених механізмів двох або більше типів.

"НИ - 1" може вказувати на "Нормативний документ з інформаційної безпеки № 1", який може містити вказівки щодо зовнішньої ідентифікації і автентифікації.

Зазвичай, зовнішня ідентифікація означає процес визначення особи на основі зовнішніх ознак, таких як ім'я, фотографія, а також можливо біометричні дані. Автентифікація, у свою чергу, відбувається, коли особа підтверджує свою ідентичність, наприклад, за допомогою пароля, PIN-коду або біометричних даних. В контексті інформаційної безпеки, ці процеси є ключовими для забезпечення доступу до систем і даних тільки для авторизованих користувачів.

Аналіз "НИ - 1" щодо зовнішньої ідентифікації і автентифікації потрібно взяти до уваги кілька ключових аспектів:

Область застосування: Документ повинен чітко визначити, на які системи та дані він поширюється, а також на який період часу. Це допоможе зрозуміти, де саме будуть застосовуватися вказівки щодо зовнішньої ідентифікації і автентифікації.

1.Вимоги до ідентифікації: Документ повинен визначити, які конкретні методи індентифікації будуть використовуватися (наприклад, ім'я користувача, електронна пошта, номер телефону, фотографія, біометричні дані тощо) і які вимоги до їхньої безпеки.

2.Вимоги до автентифікації: Документ повинен описати методи автентифікації, такі як паролі, PIN-коди, біометричні сканери, а також встановити вимоги до їхньої складності і безпеки.

3.Механізми захисту: Документ має включати в себе рекомендації щодо захисту інформації під час процесів ідентифікації та автентифікації, включаючи шифрування, двофакторну аутентифікацію, контроль доступу тощо.

4.Управління доступом: Документ також має визначити процедури управління доступом, включаючи створення, видалення та управління обліковими записами користувачів, а також контроль за їхніми привілеями.

5.Аудит та моніторинг: Важливим аспектом є наявність в документі вимог щодо аудиту та моніторингу процесів ідентифікації та автентифікації для виявлення спроб несанкціонованого доступу або порушень безпеки.

6.Відповідність і стандарти: Документ повинен відповідати відповідним законодавчим актам, стандартам безпеки та нормативам, які стосуються обраних методів зовнішньої ідентифікації та автентифікації.

7.Аналіз "НИ - 1" з цих точок зору допоможе забезпечити, що він відповідає вимогам безпеки та забезпечить надійний захист інформації.

"НИ - 2" "Одиночна ідентифікація і автентифікація" вказує на процес визначення та підтвердження ідентичності конкретного користувача. Це може включати в себе введення пароля, використання біометричних даних (таких як відбитки

пальців або розпізнавання обличчя), використання токенів або інших методів для забезпечення доступу до системи або інформації.

Аналіз НИ-2 з питань одиночної ідентифікації і автентифікації важливий для розуміння стандартів та вимог до захисту інформації в Україні. Ось деякі аспекти, які можна включити до такого аналізу:

1. Вимоги до ідентифікації та автентифікації: Аналізуйте конкретні вимоги, які стандарт встановлює для процесів ідентифікації та автентифікації користувачів. Це може включати в себе методи, технології та процедури.

2. Безпека: Оцініть, наскільки ефективно стандарт враховує вимоги безпеки. Чи передбачає він заходи захисту від різних загроз, таких як злам або несанкціонований доступ?

3. Сумісність із міжнародними стандартами: НИ — 2 відповідає міжнародним стандартам безпеки інформації. Наприклад ISO/IEC 27001

5. Актуальність: Переконатися, що стандарт враховує сучасні технології та загрози. Чи оновлюється він відповідно до змін в інформаційній безпеці.

6. Впровадження та дотримання: Наскільки ефективно організації впроваджують та дотримуються цих вимог. Чи існують проблеми з впровадженням або виконанням стандарту.

7. Можливості для поліпшення: На основі аналізу визначите можливість покращення стандарту. Це може бути зміна або доповнення вимог, щоб врахувати нові технології або загрози.

Аналіз НИ - 2 допоможе зрозуміти ефективність та актуальність з питань одиночної ідентифікації і автентифікації .

"НИ - 3" це "Множина ідентифікація та автентифікація" вказує на те, що стандарт встановлює вимоги не лише до одиночної ідентифікації і автентифікації користувачів, але й до ситуацій, коли існує необхідність визначити та підтвердити ідентичність групи користувачів або суб'єктів.

Аналіз НИ - 3 може включати такі аспекти:

1. Обсяг застосування: Розглядайте, на які види інформації та систем поширюється стандарт. Чи охоплює він різні групи користувачів або суб'єктів, які можуть мати різні рівні доступу.

2. Вимоги до ідентифікації та автентифікації груп: Аналізуйте, які конкретні вимоги стандарт встановлює для процесів ідентифікації та автентифікації груп користувачів або суб'єктів. Це може включати в себе методи та технології, придатні для масштабного управління доступом.

3. Безпека масштабних ідентифікаційних процесів: Оцініть, наскільки ефективно стандарт враховує безпеку масштабних ідентифікаційних процесів, враховуючи можливі ризики, пов'язані з масовою ідентифікацією користувачів або суб'єктів.

4. Взаємодія з іншими стандартами: Переконатися НИ - 3 сумісна з іншими вітчизняними та міжнародними стандартами безпеки.

5. Актуальність та майбутні вимоги: Врахуйте зміни в технологіях та практиках безпеки, щоб забезпечити актуальність стандарту. Це може включати в себе майбутні вимоги до ідентифікації та автентифікації з урахуванням швидко розвиваючихся технологій.

Аналіз НИ- 3 з питань множинної ідентифікації та автентифікації допоможе забезпечити ефективний та безпечний доступ до інформації для груп користувачів або суб'єктів.

Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Забезпечує критеріїї	Критерії Windows	Критеріїї автономного застосунку Павла Гордіна
НК-1 Однонаправлений достовірний канал	Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	-

НК-2 Днонаправлений достовірний канал	-	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ.Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача

"НК-1". Однонаправлений достовірний канал означає, що це канал передачі даних, який працює у одному напрямку та забезпечує достовірність передачі. Аналіз "НК-1 Однонаправленого достовірного каналу" може включати оцінку його ефективності, надійності та можливостей передачі даних. Для проведення такого аналізу можуть використовуватися наступні критерії:

1. Достовірність передачі даних: Оцінка того, наскільки надійно канал передає дані без помилок або втрат.

2. Пропускна здатність: Максимальна швидкість передачі даних через канал. Важливо визначити, чи відповідає пропускна здатність вимогам конкретного застосування.

3. Затримка: Час, необхідний для передачі сигналу від джерела до приймача. Низька затримка важлива для додатків реального часу.

4. Вартість: Оцінка витрат на розгортання та підтримку каналу в порівнянні з іншими альтернативами.

5. Споживана енергія: Для бездротових каналів важливо визначити, скільки енергії споживається під час передачі даних.

6. Наявність інтеграції з іншими системами: Як добре "НК-1" інтегрується з іншими технологіями та пристроями у вашій системі зв'язку.

7. Стійкість до перешкод: Здатність каналу працювати ефективно в умовах перешкод, таких як шум, спотворення сигналу або інтерференція.

8. Масштабованість: Можливість розширення каналу для обробки більшого

обсягу даних чи підключення додаткових пристроїв.

Аналіз "НК-1 Однонаправленого достовірного каналу" повинен базуєтся на конкретних потребах і вимогах системи зв'язку або проекту, а також на порівнянні з альтернативними рішеннями.

НК -2 Двонаправлений канал зв'язку - це канал передачі даних, який дозволяє обміну інформацією між двома або більше пристроями в обох напрямках одночасно. Це означає, що дані можуть передаватися як від відправника до отримувача, так і від отримувача до відправника, одночасно або за потреби. Двонаправлені канали зв'язку широко використовуються в різних системах зв'язку, таких як мережі зв'язку, мобільні телефони, бездротовий Інтернет, радіозв'язок та інші. Вони дозволяють ефективно обмінюватися інформацією між пристроями без значного затримання.

Двонапрямлений зв'язок - це концепція в теорії комунікації, що передбачає обмін інформацією між двома або більше сторонами, де кожна з них може виступати як передавач і як приймач інформації одночасно. Аналіз цього типу зв'язку включає в себе оцінку ефективності комунікації між учасниками, способів, якими інформація передається та розуміється, а також впливу цього зв'язку на взаємини між учасниками.

Ось деякі аспекти, які можна розглядати при аналізі двонапрямленого зв'язку:

1. Ефективність передачі інформації: Як добре інформація передається від одного учасника до іншог. Чи існують перешкоди для зрозуміння

2. Активне слухання: Чи демонструють учасники здатність активно слухати один одного? Чи реагують вони на отриману інформацію?

3. Взаємодія: Чи сприяє зв'язок взаєморозумінню та співпраці між учасниками? Чи існують конфлікти або недорозуміння?

4. Задоволення потреб: Чи вдається задовольнити потреби обох учасників у зв'язку? Чи відчувають вони, що їхні думки та почуття враховуються?

5. Побудова відносин: Як зв'язок впливає на відносини між учасниками Чи сприяє він покращенню взаєморозуміння та довіри.

6. Застосування отриманої інформації: Чи використовується отримана інформація для досягнення спільних цілей або вирішення проблем.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Забезпечує критерії	Критеріїї Windows
НО-3 Розподіл обов’язків на основі привілеїв	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Політика розподілу обов'язків повинна визначати множину ролей користувачів ,користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

У Windows існує концепція облікових записів користувачів і груп, яка дозволяє адміністраторам призначати різні рівні доступу та привілеїв для користувачів і програм. Розподіл обов'язків на основі привілеїв може включати наступні кроки:

1. Створення груп користувачів: Групи дозволяють об'єднувати користувачів зі схожими потребами у керуванні даними і ресурсами. Наприклад, група "Адміністратори" може мати повний доступ до всіх системних ресурсів, тоді як група "Користувачі" може мати обмежений доступ.

2. Призначення привілеїв для груп: Після створення груп ви можете надавати їм певні привілеї. Наприклад, ви можете дозволити групі "Адміністратори" встановлювати програми або змінювати налаштування системи, тоді як група "Користувачі" може мати обмежений доступ до цих функцій.

3. Створення облікових записів користувачів і призначення їх до групи Створіть облікові записи користувачів для кожної особи, яка буде використовувати систему, і призначте їх до відповідних груп.

4. Аудит доступу і змін: Використовуйте функції аудиту Windows, щоб відслідковувати, які користувачі отримують доступ до ресурсів і які зміни вони вносять.

5. Регулярне оновлення прав доступу: Періодично переглядати та оновлювати права доступу користувачів та груп, особливо якщо відбуваються зміни в організаційній структурі або потребах безпеки.

6. Використання політик безпеки: Windows також підтримує групові політики, які дозволяють адміністраторам централізовано керувати налаштуваннями безпеки для груп користувачів і комп'ютерів у мережі.

Ці кроки допоможуть вам ефективно розподілити обов'язки на основі привілеїв у вашій системі Windows, забезпечуючи відповідний рівень доступу для кожного користувача чи групи користувачів.

Аналіз НО-3 розподілу обов'язків на основі привілеїв в Windows може бути важливим кроком для забезпечення ефективного управління доступом до ресурсів системи і забезпечення безпеки інформації.

Ось деякі аспекти, які можна врахувати під час аналізу:

1. Потреби бізнесу або організації: Перш ніж розпочати розподіл обов'язків, важливо зрозуміти потреби вашого бізнесу або організації. Які типи даних та ресурсів необхідно захищати Які функції або завдання потрібно виконувати різним користувачам.

2. Огляд існуючих привілеїв: Проведіть огляд поточного розподілу привілеїв і доступу в системі Windows. Які групи користувачів вже існують? Які привілеї призначені для кожної групи?

3. Ідентифікація ключових ролей: Визначте ключові ролі або позиції в вашій організації і з'ясуйте, які привілеї кожна з цих ролей повинна мати. Наприклад, адміністратор мережі, користувачі відділу продажів, розробники програмного забезпечення тощо.

4. Розробка матриці доступу: Створіти матрицю доступу, в якій відображені різні ролі користувачів і відповідні привілеї для кожної ролі. Це може допомогти візуалізувати, як поточні привілеї відповідають потребам організації і чи є вони відповідними з точки зору безпеки.

5. Виконання аудиту безпеки: Проведіть аудит безпеки для ідентифікації можливих проблем безпеки або неправильного використання привілеїв. Це може включати перегляд журналів подій, перевірку прав доступу до файлів і папок, а також аналіз прав доступу до системних ресурсів.

6. Впровадження змін і моніторинг: Після виявлення можливих областей для покращення виконайте необхідні зміни у розподілі обов'язків та привілеїв. Після цього регулярно моніторте систему, щоб переконатися, що розподіл обов'язків відповідає поточним потребам та нормам безпеки.

Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Забезпечує критерії	Критерії Taifun Web	Критерії автономного застосунку Павла Гордіна
НЦ-1 КЗЗ з контролем цілісності	Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.	-
НЦ-2 КЗЗ з гарантованою цілісністю	-	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту,

		що використовуються для реалізації розподілення доменів КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування

НЦ -1 Контроль захисту засобів з контролем цілісності - це процес перевірки, який забезпечує, що інформаційні засоби (наприклад, програмне забезпечення, дані, мережі тощо) залишаються цілими і захищеними від несанкціонованого доступу, змін або втрати.

Ця концепція включає в себе різні аспекти, такі як:

1. Перевірка цілісності даних: Це означає перевірку, щоб упевнитися, що дані не були змінені без дозволу або без знання власника. Це може включати застосування криптографічних методів або контрольних сум для перевірки цілісності файлів.

2. Заходи безпеки доступу: Це включає в себе методи контролю доступу, такі як паролі, біометричні дані, двофакторна аутентифікація тощо, щоб забезпечити, що лише уповноважені користувачі можуть отримувати доступ до системи або даних.

3. Моніторинг систем та виявлення вторгнень: Це означає постійний нагляд за системою з метою виявлення будь-яких підозрілих або несанкціонованих дій, які можуть позначити на порушення безпеки.

4. Резервне копіювання та відновлення: Забезпечення наявності резервних копій даних і процедур відновлення даних у випадку втрати або пошкодження оригіналів.

5. Шифрування даних: Застосування методів шифрування для захисту конфіденційності даних під час їх транспортування або зберігання.

6. Оновлення та патчі безпеки: Регулярне оновлення програмного забезпечення та встановлення патчів для виправлення виявлених вразливостей і підвищення рівня захисту.

Ці заходи спільно допомагають забезпечити, що інформаційні засоби залишаються цілими і захищеними від потенційних загроз безпеки.

Аналіз НЦ -1 контролів захисту засобів з контролем цілісності включає оцінку ефективності і потужності вже наявних заходів захисту та ідентифікацію можливих слабких місць. Ось деякі кроки, які можуть бути включені в аналіз таких контролів:

1. Огляд політик і процедур: Перевірте, які політики і процедури встановлені для контролю цілісності даних та засобів. Це включає в себе перевірку правил доступу, процедур резервного копіювання, контрольних точок і так далі.

2. Оцінка технічних заходів безпеки: Оцініть наявні технічні засоби, які застосовуються для контролю цілісності даних, такі як механізми шифрування, системи виявлення вторгнень, контроль цілісності файлів тощо.

3. Проведення внутрішніх та зовнішніх тестів з вразливості: Виконання тестів на проникнення та аудитів безпеки, щоб ідентифікувати можливі слабкі місця в системі та контрольних заходах.

4. Оновлення та підтримка: Перевірте, чи оновлюється та підтримується програмне забезпечення, обладнання та інші засоби безпеки на регулярній основі для забезпечення відповідності останнім стандартам безпеки.

5. Аналіз інцидентів безпеки: Вивчіть інциденти безпеки, які сталися в минулому, і з'ясуйте, чому вони сталися, щоб уникнути їх у майбутньому.

6. Оцінка дотримання стандартів безпеки: Перевірте, чи дотримується ваша організація відповідних стандартів безпеки (наприклад, ISO 27001) і чи існують проблеми з відповідністю.

НЦ -2 Контроль засобів захисту з гарантованою цілісністю - це підхід до захисту інформації та систем, що забезпечує високий рівень впевненості в тому, що дані і ресурси залишаються недоторканими, неспотвореними і незмінними в умовах різних загроз і ризиків.

Ось деякі основні аспекти контролю засобів захисту з гарантованою цілісністю:

1. Криптографія: Використання сильних алгоритмів шифрування для захисту конфіденційності, цілісності і автентичності даних під час їх транспортування або зберігання.

2. Методи аутентифікації: Використання сильних методів аутентифікації, таких як біометрія, одноразові паролі, двофакторна аутентифікація тощо, щоб переконатися, що лише правильні користувачі мають доступ до системи.

3. Моніторинг та виявлення вторгнень: Регулярний моніторинг систем для виявлення підозрілих або несанкціонованих дій, які можуть вказувати на порушення цілісності даних або ресурсів.

4. Централізований контроль доступу: Встановлення централізованих систем контролю доступу, які дозволяють точно налаштовувати, хто має доступ до яких ресурсів і яким чином.

5. Регулярні аудити та оцінки безпеки: Проведення регулярних аудитів і оцінок безпеки, щоб переконатися, що контроль захисту засобів з гарантованою цілісністю ефективний і відповідає поточним стандартам безпеки.

6. Фізичні заходи безпеки: Забезпечення фізичної безпеки серверних приміщень, обладнання та інших критичних ресурсів для запобігання несанкціонованому доступу або втраті даних.

Аналіз НЦ - 2 контролю засобів захисту з гарантованою цілісністю - це процес оцінки ефективності та надійності заходів безпеки, спрямованих на забезпечення цілісності даних та ресурсів. Основні кроки аналізу включають такі дії:

1. Огляд політик і стандартів: Перегляд і оцінка політик безпеки, процедур та стандартів, що застосовуються в організації, для забезпечення відповідності сучасним вимогам і нормативам безпеки.

2. Оцінка систем безпеки: Аналіз наявних технічних засобів безпеки, таких як системи контролю доступу, системи виявлення вторгнень, системи моніторингу та аудиту, щоб переконатися в їх ефективності.

3. Тестування вразливостей: Проведення тестування на проникнення та оцінка вразливостей системи для виявлення потенційних слабких місць у контролі захисту та їх подальшого виправлення.

4. Аналіз інцидентів безпеки: Вивчення інцидентів безпеки, які сталися в минулому, щоб зрозуміти причини порушень цілісності даних та ресурсів і прийняти заходи для їх попередження в майбутньому.

5. Оцінка дотримання стандартів і вимог безпеки: Перевірка відповідності встановленим стандартам і вимогам безпеки, таким як GDPR, HIPAA, ISO 27001 тощо, і вживання заходів для виправлення будь-яких виявлених невідповідностей.

6. Аудит контрольних заходів: Проведення регулярних аудитів безпеки для перевірки ефективності та правильності застосування контрольних заходів і виявлення можливих проблем або недоліків.

Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Забезпечує критеріїї	Критерії Windows
НТ-2 Самотестування на старті	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження.

Більшість комплексів антивірусної захисту, таких як Norton, McAfee, а також вбудований Windows Defender, мають можливості самодіагностики, які можуть запускатися під час завантаження системи. Ці функції можуть виявляти

проблеми з безпекою та проводити сканування системи на виявлення вірусів або шкідливих програм ще до того, як операційна система повністю завантажиться.

Аналіз самотестування комплексу систем захисту на початковому етапі завантаження комп'ютера може виявити різні проблеми, включаючи:

1. Виявлення вірусів та шкідливих програм: Система може провести сканування файлів і виявити наявність вірусів або шкідливих програм на комп'ютері. Це дозволить вам прийняти відповідні заходи для їх вилучення та очищення системи.

2. Перевірка цілісності системних файлів: Самотестування може перевірити цілісність важливих системних файлів, щоб виявити можливі пошкодження або зміни. Це важливо для забезпечення стабільності операційної системи.

3. Перевірка ефективності антивірусного движка: Тестування може оцінити ефективність антивірусного движка і його здатність виявляти нові загрози. Це дозволить користувачеві переконатися, що їх система захищена від сучасних загроз.

4. Аналіз стану засобів безпеки: Система може перевірити наявність активних засобів безпеки, таких як файрвол, антивірусне програмне забезпечення та антишпіонське програмне забезпечення, і переконатися, що вони працюють належним чином.

5. Повідомлення про проблеми і поради щодо виправлення: Система може надати користувачеві повідомлення про будь-які виявлені проблеми та надати поради щодо їх вирішення.

Загалом, аналіз самодіагностики на старті комплексу систем захисту дозволяє забезпечити високий рівень безпеки комп'ютера та захистити його від різноманітних загроз і атак.

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість

ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

Забезпечує критеріїї	Критеріїї Windows	Критерії Taifun Web
НВ-1 Автентифікація вузла	Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації	-
НВ-2 Автентифікація джерела даних	-	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується.

НВ-1 Автентифікація вузла — це процес перевірки ідентичності конкретного комп'ютера (вузла) в комп'ютерній мережі. Це важливий етап забезпечення безпеки мережі, оскільки дозволяє контролювати доступ до ресурсів і забезпечувати конфіденційність та цілісність даних.

Існує кілька методів автентифікації вузла:

1. MAC-адреса: Кожний мережевий адаптер має унікальну фізичну адресу, відому як MAC-адреса. Автентифікація може ґрунтуватися на перевірці MAC-адреси вузла.

2. IP-адреса: Автентифікація може виконуватися на основі IP-адреси вузла.

3. SSL-сертифікати: Вузли можуть автентифікуватися за допомогою SSL-сертифікатів, які гарантують їхню ідентичність в мережі.

4. Kerberos: Це протокол аутентифікації, що дозволяє вузлам довіряти один одному за допомогою спільного довіреного центру.

5. LDAP або Active Directory: У великих мережах використовуються каталоги даних, такі як LDAP або Active Directory, для централізованої автентифікації вузлів.

6. Biometric Authentication: Деякі системи можуть використовувати біометричні дані, такі як сканування відбитків пальців або розпізнавання обличчя, для автентифікації вузлів.

Кожен метод має свої переваги і недоліки, і вибір конкретного методу залежить від потреб конкретної мережі та рівня безпеки, який потрібно забезпечити.

Аналіз HB-1 автентифікації вузла в мережі може охоплювати кілька аспектів, які допоможуть зрозуміти її ефективність та безпеку. Ось деякі ключові пункти, які можна включити у такий аналіз:

1. Методи автентифікації: Визначте, які саме методи автентифікації використовуються в вашій мережі. Це може бути базова аутентифікація за допомогою паролів, сертифікати SSL/TLS, використання біометричних даних, використання мережевих ключів або інші методи.

2. Слабкі місця: Виявіть можливі слабкі місця в автентифікаційному процесі. Це може бути недостатня складність паролів, вразливості протоколів аутентифікації або недостатня захист від атак, таких як перехоплення сесій.

3. Моніторинг і аудит: Перевірте, чи ведеться адекватний моніторинг та аудит автентифікаційних подій. Це дозволить вчасно виявляти ненормальну активність та атаки на автентифікаційні механізми.

4. Централізоване керування доступом: Оцініть, чи використовується

централізована система керування доступом, така як Active Directory або LDAP, для управління автентифікацією вузлів в мережі.

5. Міцність аутентифікаційних механізмів: Визначте, наскільки міцні аутентифікаційні механізми, які використовуються в мережі, і чи є можливість виконання атак, таких як брутфорс паролів або атаки з використанням слабкостей протоколів.

6. Загрози та ризики: Проаналізуйте потенційні загрози та ризики, пов'язані з автентифікацією вузлів в мережі, і розробіть стратегії для їх запобігання або виявлення.

НВ - 2 Автентифікація джерела даних - це процес перевірки правдивості чи автентичності джерела, звідки надходять дані. Це важливий аспект в інформаційній безпеці та кібербезпеці, оскільки неправильні дані можуть призвести до небажаних наслідків, таких як зловживання, маніпуляції або втрата конфіденційності.

Існують різні методи автентифікації джерела даних, включаючи:

1. Цифровий підпис: Дані підписуються за допомогою приватного ключа, а потім перевіряються за допомогою відповідного публічного ключа.

2. Автентифікація на основі токенів: Джерела даних можуть отримувати токени, які вони використовують для автентифікації при кожному взаємодії з системою.

3. IP-фільтрація: Перевірка IP-адреси джерела даних на відповідність списку довірених або недовірених джерел.

4. SSL-сертифікати: Забезпечують безпеку транспортування даних між джерелом та отримувачем.

5. Біометрична аутентифікація: Використання біометричних даних, таких як відбитки пальців чи розпізнавання обличчя, для підтвердження особи, що відправляє дані.

6. Автентифікація з використанням протоколів аутентифікації: Наприклад,

протокол OAuth для автентифікації користувачів за допомогою сторонніх сервісів.

Аналіз НВ - 2 Аналіз автентифікації джерела даних включає в себе оцінку та перевірку різних аспектів, що впливають на надійність та безпеку збирання інформації. Ось деякі ключові елементи, які слід враховувати при аналізі автентифікації джерела даних:

1. Методи автентифікації: Оцінити, які методи автентифікації використовуються для перевірки автентичності джерела даних. використовуються надійні методи, такі як цифровий підпис або багатофакторна аутентифікація

2. Захист від підробки: Перевірте, які заходи захисту використовуються для запобігання підробці даних або ідентифікаторів джерела. Наприклад, чи використовуються токени або цифрові підписи для перевірки цілісності даних?

3. Управління доступом: Розгляньте, як керується доступ до джерела даних. Чи існують правила або політики, що регулюють, хто має доступ до даних та як цей доступ контролюється

4. Моніторинг інцидентів: Перевірте, які заходи прийняті для виявлення та реагування на можливі порушення безпеки або інциденти з автентифікацією джерела даних.

5. Захист проти атак: Оцініть, які заходи захисту застосовуються для запобігання атакам на автентифікацію, таким як перехоплення токенів, фішинг або використання підроблених цифрових підписів.

6. Аудит автентифікації: Розгляньте, чи проводиться аудит процесів автентифікації для виявлення слабких місць або можливих вразливостей у системі.

Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто

той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ран жируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Забезпечує критерііï	Критерііï автономного застосунку Павла Гордіна
НА- 1 Базова автентифікація відправника	Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем . Встановлення автентифікаціїї має виконуватись на підставі затвердженого протоколу автентифікації.

НА - 1 Базова автентифікація відправника - це метод аутентифікації, який використовується для перевірки ідентичності користувача під час надсилання запитів до сервера. Під час базової автентифікації, клієнтська програма надсилає на сервер ідентифікатор та пароль у вигляді заголовка HTTP. Наприклад, заголовок може виглядати так: Хоча базова автентифікація широко використовується, варто пам'ятати, що вона не є найбільш безпечним методом, оскільки дані надсилаються у відкритому вигляді, і можуть бути легко зламані. Тому рекомендується використовувати HTTPS замість HTTP для захисту конфіденційності даних під час автентифікації.

Аналіз НА -1 Базова автентифікація відправника є одним з найпростіших методів аутентифікації в мережі. Ось деякі переваги та недоліки цього підходу:

Переваги:

1. Простота реалізації: Цей метод досить легко впроваджується як на стороні клієнта, так і на стороні сервера. Немає необхідності встановлювати додаткові засоби аутентифікації.

2. Широке застосування: Базова автентифікація підтримується більшістю

серверів та клієнтських програм, що робить її доступною для використання в різних середовищах.

Недоліки:

1. Відсутність шифрування: У базовій автентифікації дані (ідентифікатор і пароль) передаються у відкритому вигляді, тому вони можуть бути перехоплені зловмисником. Це робить цей метод небезпечним для використання у відкритих мережах, таких як Інтернет.

2. Вразливість до атак перехоплення: Під час передачі даних, навіть через HTTPS, є ризик атаки перехоплення, коли зловмисник може отримати доступ до ідентифікаторів та паролів користувачів.

3. Відсутність варіантів переаутентифікації: Під час використання базової автентифікації неможливо підтвердити ідентичність користувача знову без повного повторного введення ідентифікатора та пароля.

Загалом, базова автентифікація відправника є простим і зручним методом для використання у внутрішніх мережах або в ситуаціях, де конфіденційність даних не є критичною.

Автентифікація отримувача

Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ран жируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Забезпечує	Критерії автономного застосунку Павла Гордіна

критерії	
НП-1Базова автентифікація користувача	Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем. Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації

НП -1 Базова автентифікація користувача (Basic User Authentication) - це метод аутентифікації, який використовується для перевірки ідентифікації користувача під час доступу до веб-ресурсів або захищених областей в Інтернеті. У цьому методі користувач повинен надати ідентифікатор (зазвичай це ім'я користувача) і пароль для підтвердження своєї ідентичності.Принцип роботи базової автентифікації користувача дуже простий.

1. Користувач намагається отримати доступ до захищеного ресурсу, наприклад, веб-сторінки або API.

2. Сервер запитує від користувача ідентифікатор і пароль.

3. Користувач надсилає ідентифікатор і пароль на сервер.

4. Сервер перевіряє правильність наданих даних. Якщо ідентифікатор і пароль вірні, то користувач отримує доступ до ресурсу.

5. Якщо ідентифікатор або пароль неправильні, сервер повертає помилку аутентифікації.

Основна перевага базової автентифікації користувача - це її простота в реалізації як на стороні клієнта, так і на стороні сервера. Однак, цей метод не забезпечує високого рівня безпеки, оскільки дані (ідентифікатор і пароль) передаються у відкритому вигляді і можуть бути легко перехоплені. Тому рекомендується використовувати HTTPS замість HTTP для захисту конфіденційності даних під час автентифікації.

Аналіз НП - 1 базової автентифікації користувача дасть змогу розібрати переваги та недоліки цього методу:

Переваги:

1. Простота реалізації: Один із головних плюсів базової автентифікації полягає в її простоті. Вона легко впроваджується як на стороні сервера, так і на стороні клієнта, не вимагаючи значних зусиль для налаштування.

2. Широке застосування: Базова автентифікація підтримується більшістю веб-серверів і є стандартом для HTTP, що дозволяє її використовувати в різних середовищах без додаткових зусиль.

Недоліки:

1. Відсутність шифрування: Основна недолік базової автентифікації полягає в тому, що дані (ідентифікатор і пароль) передаються у відкритому вигляді, не зашифровані. Це робить їх вразливими для перехоплення атакуючими.

2. Низький рівень безпеки: У зв'язку з відсутністю шифрування дані, введені користувачем, можуть бути легко перехоплені зловмисниками, особливо у відкритих мережах.

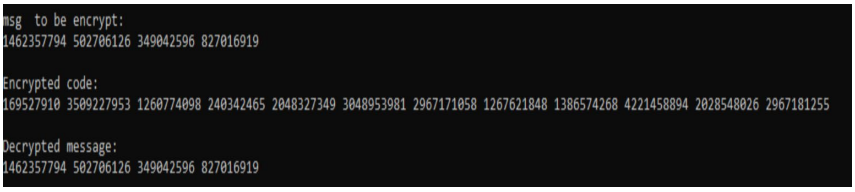
3. Відсутність можливостей переаутентифікації: Базова автентифікація не має механізмів для переаутентифікації користувача без повного повторного введення ідентифікатора і пароля.

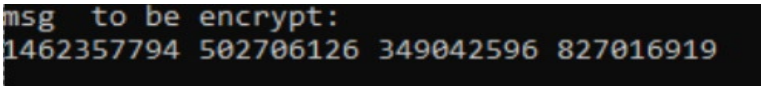
4. Брак захисту від атак перехоплення: Маніпулювання та перехоплення данних, навіть якщо вони передаються через HTTPS, можуть бути виконані з використанням базової автентифікації.

Таблиця А.1

Види криптографії	**Опис**	**Приклади методів і алгоритмів**
Симетрична	Використовує один ключ для шифрування та розшифрування даних	AES, DES, 3DES, Blowfish
Асиметрична	**Використовує пару ключів:**	**RSA, ECC**

Види криптографії	Опис	Приклади методів і алгоритмів
(RSA)	**публічний та приватний. Публічний ключ використовується для шифрування, а приватний для розшифровки**	
Хэшування	Перетворює дані на фіксовану довжину хеша. Хеші використовуються для перевірки цілісності даних	MD5, SHA-256, SHA-3
Цифрові підписи	Використовується для автентифікації відправника та забезпечення цілісності даних	RSA (для підписів), ECDSA (еліптичні криві для підписів)
Протоколи аутентифікації	Забезпечують безпечну ідентифікацію суб'єктів	OAuth, Kerberos, OpenID
Квантова криптографія	Використовує властивості квантової механіки для створення безпечних криптографічних систем	Квантова криптографія на основі однофотонних джерел, квантовий розподіл ключів (Quantum Key Distribution)





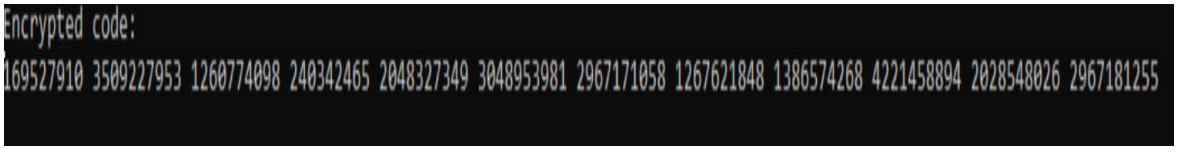


Рис. А.5 Алгоритм побайтових математичних операцій

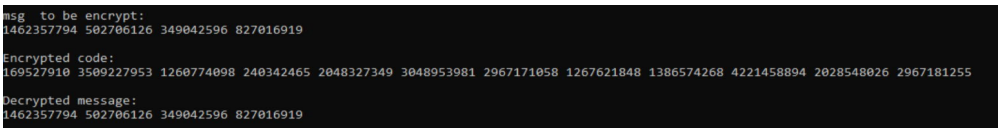


Рис. А.6 Приклад виведення сеансового ключа