виконавчий блок. В ролі засобів взаємодії з середовищем, в якому вона застосовується використовуються давач відбитку пальця та виконавчий блок

Алгоритм роботи наведеної системи можна описати наступним чином: відбиток пальця сканується оптичною системою, аналізується, оцифровується, зберігається в пам'яті терміналу або в пам'яті комп'ютера системи керування і використовується для перевірки кожного, хто видає себе за авторизованого користувача. При цьому в пам'яті пристрою не містяться реальні відбитки пальців, що не дозволяє їх вкрасти зловмиснику. Типовий час занесення в пам'ять одного контрольного відбитку пальця складає до 30 с. Кожен занесений в пам'ять терміналу авторизований користувач проходить стадію перевірки ідентичності, що займає приблизно 0,5 - 2 с. При збігу відбитків, що пред'являються і контрольного, термінал подає сигнал на виконавчий пристрій.

**Висновок**

У даній роботі розроблено систему класифікації зображень відбитків пальців як комплекс програмно-апаратних засобів обробки зображень.

**Список використаних джерел**


1. Завгородний В.И. Комплексная защита информации в компьютерных системах / В.И. Завгородний. – М.: Высшая школа, 2012. – 264 с.
2. Karu K. Fingerprint Classification / K.Karu, Jain A. // Pattern Recognition. – V.29, №3, 2006. – pp. 389-404.



УДК 681.3


# ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОГО КАНАЛУ ОБМІНУ ПОВІДОМЛЕННЯМИ З ВИКОРИСТАННЯМ АПАРАТУ ЕЛІПТИЧНИХ КРИВИХ


**Касянчук М.М.[1)], Михалюк І.В.[2)], Самарик П.С.[3)]**

*Тернопільський національний економічний університет*

*[1)] к.ф.-м.н., доцент; [2)] магістрант; [3)] провідний інженер*


## І. Постановка проблеми

На даний час для захисту передачі інформації одним з ключових елементів є криптографія [1]. Її сутність полягає у використанні перетворення інформації, доступної для однієї сторони та недоступної для іншої. Захист інформації для сьогодення має досить важливе значення, адже у випадку витоку інформації організація або навіть цілі країни можуть понести величезні збитки як фінансового, так і державного значення. Для зменшення негативних наслідків витоку інформації потрібні захищені канали передачі даних для гарантування безпеки.

## ІІ. Мета роботи

Метою даної роботи є програмна реалізація захищеного каналу обміну повідомленнями з використанням апарату еліптичних кривих (ЕК).

## ІІІ. Реалізація захищеного каналу обміну повідомленнями

Для реалізації задачі захищеного каналу обміну повідомленнями її потрібно розбити на дві підзадачі, а саме створення мережевого каналу зв’язку з використанням технології P2P (peer-to-peer) та шифрування повідомлення за допомогою апарату ЕК.

В роботі проаналізовані алгоритми з використанням ЕК та існуючі системи шифрування, в яких використовується апарат ЕК.

Апарат ЕК належить до асиметричного шифрування, яке ґрунтується на складності вирішення деяких математичних задач. Це дає додатковий захист, так як для даного виду шифрування не потрібно забезпечувати абсолютну надійність каналу зв’язку для розсилання секретних ключів. Також в апараті ЕК перевагою є те, що на сьогоднішній день невідомо існування субекспоненціальних алгоритмів для вирішення задачі дискретного логарифмування в групах їх точок. При цьому порядок групи точок ЕК визначає складність задачі.

В порівнянні з симетричними, криптосистема на основі ЕК забезпечує більш високу стійкість при рівній трудомісткості, або ж навпаки: меншу трудомісткість при рівній стійкості. Це пояснюється тим, що для обчислення зворотних функцій на ЕК відомі тільки алгоритми з експоненціальним ростом трудомісткості, тоді як для звичайних, симетричних систем запропоновані

субекспоненціальні методи. В результаті рівень стійкості, який досягається в RSA за допомогою 1024-бітових модулів, реалізується в системах на ЕК 160-бітним модулем.

В ході роботи розроблено систему обміну повідомленнями з використанням шифрування та архітектури системи, в основі якої лежить мережа, заснована на принципі рівноправності учасників, яка характеризується тим, що всі елементи мережі є автономними та можуть зв'язуватись між собою (вузли одночасно функціонують як клієнт та сервер) на відміну від клієнт-серверної архітектури, яка вимагає центрального сервера.

Програма для обміну повідомленнями написана на мові програмування Python [2], що дозволяє їй бути крос-платформенною та виконуватись на різних операційних системах (Windows, Linux, MacOS X). Також використання Python дає можливість редагування програми під конкретні потреби без її подальшої компіляції, так як Python використовує інтерпретацію замість компіляції.

### Висновок

У даній роботі розроблено програмну реалізацію захищеного каналу обміну повідомленнями з використаням апарату ЕК.

### Список використаних джерел


1. Болотов А.А. Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. - М.:КомКнига, 2006. – 280 с.
2. Прохоренок Н.А. Python 3 и PyQt. Разработка приложений / Н.А. Прохоренок. - Спб.:БХВ-Петербург, 2012. - 704 с.



УДК 004.056.5


## МЕТОДИ ЗАХИСТУ КОРИСТУВАЧІВ ВІД ВІДСЛІДКОВУВАННЯ В НАПРАВЛЕНИХ АТАКАХ ІЗ ЗАСТОСУВАННЯМ ДОКУМЕНТІВ MICROSOFT OFFICE


**Крахмалюк І.Г.**

*Національний технічний університет України "Київський політехнічний інститут", студент*


### І. Постановка проблеми

Програмне забезпечення Microsoft Office являється одним із найбільш розповсюджених офісних пакетів. Воно є стандартом де-факто обміну документами в корпоративних та державних інформаційних системах. В контексті інформаційної безпеки наслідком популярності стала активізація досліджень методів вторгнення із застосуванням документів Microsoft Office як засобу доставлення шкідливого програмного забезпечення у випадку цільових атак з боку кримінальних структур та доставлення систем легального перехоплення при проведенні слідчих дій уповноваженими державними органами.

Крім віддаленого виконання коду при відкритті документів в багатьох випадках важливою є ідентифікація факту відкриття документу, встановлення IP адреси користувача та конфігурації програмного забезпечення (версія MS Office та можливо іншого встановленого ПЗ). Наявність IP адреси користувача у випадку легального застосування може допомогти ідентифікувати фізичне місцезнаходження зловмисника, або у випадку цільової атаки перейти до аналізу вразливостей мережевого устаткування. Знання точної версії ПЗ дозволяє підвищити надійність експлоітів для віддаленого виконання коду в обох випадках.

В даній роботі пропонується метод захисту від атак деанонімізації користувачів із застосуванням документів Microsoft Office.

### ІІ. Мета роботи

Метою даної роботи є запропонування методів захисту користувачів від відслідковування через документи Microsoft Office та дослідження їх ефективності на прикладі моделі системи деанонімізації, що використовує відслідковуючі посилання на зображення.

### ІІІ. Використання малодокументованих частин функції Mail Merge для відслідковування розповсюдження документів формату Microsoft Office

Починаючи з ранніх версій офісний пакет Microsoft Office включає в собі функцію Mail Merge, яка дозволяє створювати поштові листи за попередньо визначеними шаблонами. Недокументованою функцією є підтримка контрольних слів (control words), пов'язаних з функцією Mail Merge у звичайних документах. Одним з таких слів є контрольне слово додавання зображення в документ.