Вывод

Несмотря на то, что с развитием информационных технологий так же повышается уровень защиты различных информационных систем, одним из самых уязвимых мест является человеческий фактор. В ходе исследований был разработан программный продукт, с помощью которого можно осуществить фишинговую атаку с целью дальнейшей разработки комплекса защиты от атак данного рода. Так же после реализации продукта были исследованы методы защиты от подобных атак.

Список использованных источников

1. Человеческий фактор [Электронный ресурс] // Википедия. – 2015. – Режим доступа к ресурсу: https://ru.wikipedia.org/wiki/Человеческий_фактор.
2. Социальная инженерия[Электронный ресурс] // Википедия. – 2015. – Режим доступа к ресурсу: https://ru.wikipedia.org/wiki/Социальная_инженерия
3. Фишинг[Электронный ресурс] // microsoft. –2013 – Режим доступа к ресурсу: https://www.microsoft.com/ru-ru/security/online-privacy/phishing-scams.aspx

УДК 004.514

БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ ОСОБИ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

Касянчук М.М.[1)], Кравчук О.М.[2)], Фальфушинська Г.І.[3)], Осадчук О.Й.[4)]

[1)]*Тернопільський національний економічний університет, к.ф.-м.н., доцент*

[2)]*Тернопільський національний економічний університет, магістрант*

[3)]*Тернопільський державний медичний університет ім. І.Горбачевського, д.б.н., завідувач кафедри*

[4)]*Тернопільський обласний онкологічний диспансер, лікар УЗД*

І. Постановка проблеми

Біометрична ідентифікація - автоматизований метод, за допомогою якого шляхом перевірки унікальних фізіологічних особливостей людини здійснюється ідентифікація особи [1]. Фізіологічні особливості, наприклад, такі як папілярний узор пальця, геометрія долоні або малюнок (модель) райдужної оболонки ока, є постійними фізичними характеристиками людини. Даний тип вимірювань практично незмінний, як і самі фізіологічні характеристики. На відміну від пароля або PIN-коду, біометрична характеристика не може бути забута, втрачена або вкрадена. Тому на даний час є актуальною розробка системи ідентифікації зображень за відбитками пальців.

ІІ. Мета роботи

Метою даної роботи **є** розробка системи класифікації зображень за відбитками пальців, використання якої дозволяє пришвидшити визначення типів відбитків пальців.

ІІІ. Система біометричної ідентифікації за відбитками пальців

Використання відбитків пальців в якості біометрики є одним з найстаріших методів ідентифікації особи, але водночас найбільш поширений в наш час. Воно найшвидше знайшло своє застосування в роботі правоохоронних органів. Проте на даний час, крім виготовлення біометричних паспортів, використання відбитків пальців для ідентифікації особи користується значним попитом і в інших галузях. До числа факторів які сприяють цьому слід віднести: незначні розміри та вартість апаратури для обробки зображень відбитків пальців, високопродуктивне апаратне забезпечення для виконання даних задач на комп'ютерів, степінь та швидкість розпізнавання, що відповідають вимогам програмного забезпечення, різкий ріст та розвиток мережних технологій та Інтернету, а також усвідомлення необхідності простих базових методів захисту та безпеки інформації.

Розробка системи біометричної ідентифікації за відбитками пальців є досить складною задачею, тому пропонується виділити основні стадії розробки і впровадження. Основними етапами проектування системи є: проектування системи біометричної ідентифікації в цілому; розробка математичної моделі біометричних методів ідентифікації і методів їх обробки; реалізація алгоритму роботи модуля ідентифікації системи за відбитками пальців на основі створеної математичної моделі і методів обробки; реалізація системи ідентифікації у складі інформаційної системи.

Біометрична система, що реалізовує узагальнений алгоритм ідентифікації відбитків пальців, складається з бази даних і трьох основних блоків: блок реєстрації зображень, блок ідентифікації та

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