3. Гнатчук Є.Г. Інформаційна технологія подання та опрацювання знань на основі нечіткої логіки в експертних системах діагностування комп'ютерних засобів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 «Інформаційні технології» / Є.Г.Гнатчук. – Львів, 2008. – 20 с.
4. Дубчак Л.О. Метод обробки нечітких даних на основі механізму Мамдані /Л.О.Дубчак //Системи обробки інформації.– 2012. - №7(105). – С.131-134.
5. Дубчак Л.О. Спосіб обробки нечіткої інформації / Л.О.Дубчак // Вісник Східноукраїнського національного університету ім. В.Даля. – 2012. - № 8 (179), Ч.1. – С. 306-309.
6. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д.Штовба // Проблемы управления и информатики. – 2007. – №4. – С. 102–114.
7. Дубчак Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації / Л.О.Дубчак, Л.М.Тимошенко, Т.О.Яремчук // Інформаційна безпека – 2011. - №1(5). – С.112-116.

УДК 004.056.5

# СОЗДАНИЕ СИСТЕМЫ РЕАЛИЗАЦИИ ФИШИНГОВЫХ АТАК С ЦЕЛЬЮ АНАЛИЗА МЕТОДОВ ЗАЩИТЫ

**Жиляк А.Г.**
*Национальный технический университет Украины "Киевский политехнический институт", студент*

## I. Постановка проблемы

Новые информационные технологии широко внедрены во все сферы человеческой деятельности. Каждый пользователь желает иметь постоянный доступ к своей персональной и служебной информации, и быть уверенным в невозможности ее неправомерного использования.

При появлении угроз, связанных с возможностью потери, искажения, раскрытия конфиденциальных данных и утечке определенной информации, пользователь может стать жертвой злоумышленников, что приведет к отрицательным последствиям для пользователя (например, хищения крупных финансовых средств, раскрытие конфиденциальных данных и т.д.) . По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается и уровень угроз для используемых информационных технологий.

Одну из самых больших угроз информационной безопасности представляют именно методы социальной инженерии, хотя бы потому, что использование социального хакерства не требует значительных финансовых вложений и доскональных знаний компьютерных технологий, а также потому, что людям присущи некоторые поведенческие наклонности, которые можно использовать для осторожного манипулирования. На сколько бы не была автоматизирована и защищена информационная система, всегда будет присутствовать человеческий фактор (будь то преднамеренные или непреднамеренные действия), который нужно учитывать.

## II. Цель работы

Целью данной работы является разработка программного продукта, с помощью которого можно осуществить фишинговую атаку с целью дальнейшей разработки комплекса защиты от атак данного рода.

## III. Модель атаки

Для модулирования атаки был написан программный продукт, принцип работы которого следующий: на вход программы подается url-ссылка оригинального сайта, который при помощи wget клонируется. Затем в код html-страницы внедряется javascript, собирающий основную информацию с компьютера пользователя (местоположение, IPv4, IPv6, системное время, информация о браузере и операционной системе, HTTP-заголовки, информация о экране, навигатор и плагины — все эти данные отправляются на сервер), а так же обработчик формы ввода персональных данных, который их сохраняет и затем перенаправляет пользователя на оригинальный сайт.

На выходе программы получаем url-ссылку фишингового сайта. Клонированный сайт размещаем в "скрытом сервисе" в сети Tor. Ссылка фишингового сайта присылается обьекту атаки любым способом, используя сервисы по типу tor2web, которые позволяют обращаться к "скрытым сервисам" через обычный HTTP поддомен.

**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