

Причорноморські економічні студії. 2016. №9. С. 2.

3. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

4. Левченко Є. Г. , Рабчун А. О. Оптимізаційні задачі менеджменту інформаційної безпеки. *Сучасний захист інформації*. 2010. №1 (1), С. 16-24.

Ключові слова: математична модель, інформаційна безпека, часові ряди

Ключевые слова: математическая модель, информационная безопасность, временные ряды

Keywords: mathematical model, information security, time series

Янковський Олег Георгійович

Національний університет «Одеська юридична академія»,

доцент кафедри інформаційних технологій,

кандидат технічних наук, доцент

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ АУТЕНТИФІКАЦІЇ FACE ID

Сучасний світ неможливо уявити без використання інформаційних технологій у найрізноманітніших сферах людської діяльності. Обсяг електронної інформації, що використовується, стрімко зростає з кожним днем. Значну частину цієї інформації складає особиста інформація і саме тому питання захисту конфіденційних даних не втрачає своєї актуальності.

Сучасні системи контролю доступу до власних інформаційних ресурсів досить різноманітні та використовують різні підходи. Процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора називається автентифікацією. З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в

інформаційній системі, наступною після ідентифікації і передую авторизації [1].

Одним із перспективних способів аутентифікації є біометрична.

Біометрична автентифікація ґрунтується на унікальності певних антропометричних характеристик людини. У галузі інформаційних технологій термін біометрія застосовується в значенні технології ідентифікації особистості. Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів [1]. Найчастіше використовуються:

- параметри голосу;
- візерунок райдужної оболонки ока і карта сітківки ока — аутентифікація за райдужною оболонкою ока;
- риси обличчя;
- форма долоні;
- відбитки пальців;
- форма і спосіб особистого підпису — електронний цифровий підпис, верифікація підпису.

Система розпізнавання облич — це технологія, здатна ідентифікувати або перевірити особу на цифровому зображенні або відеокадрі. Існує багато методів, які використовуються в системах розпізнавання осіб, але в цілому вони ґрунтуються на порівнянні рис обличчя заданого зображення з обличчями, які зберігаються в базі даних. Він також описується як біометричний додаток на основі штучного інтелекту, який може однозначно ідентифікувати людину шляхом аналізу моделей на основі текстур обличчя та форми людини [2].

На початку свого розвитку системи розпізнавання облич використовувались як окремі додатки. Але останнім часом вони все частіше реалізуються на мобільних платформах та в інших технологіях. Зазвичай цей метод використовується для контролю доступу в системах безпеки нарівні з іншими біометричними системами, такими як розпізнавання райдужної оболонки, або відбитків пальців. Незважаючи на те, що точність роботи системи розпізнавання облич як біометричної технології є нижчою, ніж розпізнавання райдужної оболонки ока та розпізнавання відбитків пальців, вона широко застосовується завдяки безконтактному та неінвазивному процесу. Останнім часом вона також

стала популярною як комерційний інструмент ідентифікації та маркетинговий інструмент [2].

Біометричні системи розпізнавання і програми порівняння обличч поступово стали частиною нашого повсякденного життя, завдяки їх високій точності при виявленні та перевірці особистості людини - у цілях забезпечення безпеки, у комерції та інших сферах.

Одним з прикладів біометричної системи аутентифікації є Face ID - інноваційний спосіб автентифікації шляхом розпізнавання обличчя, в основі якого лежить створення структурної карти обличчя.

У сучасних умовах, пов'язаних з карантинними обмеженнями, особливу актуальність набуває технологія електронного підпису, яка використовується і у банківських операціях, і при отриманні вкрай необхідного COVID19-сертифікату про вакцинацію у системі «Дія».

Саме неупинно зростаюча популярність та все більш широке залучення (не завжди добровільне!) користувачів до використання електронних елементів бізнесу і державного сектору вивели на поверхню проблемні питання практичного використання технології Face ID.

Ще один з творців технології автоматичного розпізнавання обличч Вуді Бледсоу (1966) описував наступні труднощі її використання: «Проблема розпізнавання ускладнюється великою мінливістю повороту і нахилу голови, інтенсивністю і кутом освітлення, виразом обличчя, віком, тощо. Однак метод кореляції (або зіставлення зі зразком) необроблених оптичних даних, які часто використовуються деякими дослідниками, безсумнівно, зазнає невдачі у випадках, коли мінливість велика. Зокрема, кореляція дуже низька між двома зображеннями однієї людини з двома різними поворотами голови» [1].

Було проведено аналітичне дослідження шляхом аналізу власного досвіду та опитування користувачів порталу «Дія», який використовує активний тип розпізнавання реальності особи (Дія.Підпис): просить користувача повернути голову певним чином або виконати якусь дію чи жест, дотримуючись випадкової інструкції — кліпнути 5 разів, закрити ліве око правою рукою, змінити вираз обличчя і т. д. (так звана методика «виклик-відповідь»).

У результаті були визначені основні фактори, які ускладнюють практичне використання технології Face ID:

- недостатня комп'ютерна грамотність конкретного користувача;
- залежність якості авторизації від зовнішніх умов;
- залежність якості авторизації від технічних параметрів пристрою доступу (низька роздільна здатність фіксуючого пристрою);
- залежність якості авторизації від фізичного стану пристрою доступу (забруднення, волога, низька температура тощо);
- недоліки мобільного інтерфейсу (малий шрифт підказок);
- важливість підтримання певної дистанції до камери (важко потрапити у рамку);
- обмеженість часу на виконання певних дій.

Помилки авторизації виникали найбільш частіше у наступних випадках:

- зміна освітлення (недостатнє або зайве освітлення);
- зміна фону;
- наявність окулярів та інших аксесуарів;
- зміна зачіски (форма та колір волосся);
- зміна форми вусів або бороди;
- будь-яка міміка (посмішка, похмурий погляд);
- макіяж;
- одяг (шарф, головний убір);
- невпевнене та неточне відпрацювання команд.

Цілком зрозуміло, що використанні подібної технології викликало найбільше проблем у літніх людей та людей з обмеженими можливостями.

Список використаних джерел:

1. Автентифікація : веб-сайт. URL: <https://uk.wikipedia.org/wiki/> (дата звернення 03.11.2021).
2. Система розпізнавання облич : веб-сайт. URL: <https://uk.wikipedia.org/wiki/> (дата звернення 03.11.2021).

Ключові слова: автентифікація, біометричні методи, Face ID, електронний підпис.

Ключевые слова: аутентификация, биометрические методы, Face ID, электронная подпись.

Keywords: authentication, biometric methods, Face ID, electronic signature.

Баландіна Наталя Миколаївна

*Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки*

ДОСЛІДЖЕННЯ НЕЛІНІЙНОСТІ S-БЛОКА НА ОСНОВІ ТЕОРІЇ ДИНАМІЧНОГО ХАОСУ ПРИ ЙОГО УЯВЛЕННІ ФУНКЦІЯМИ БАГАТОЗНАЧНОЇ ЛОГІКИ

Стійкість сучасних криптографічних алгоритмів у великій мірі залежить від криптографічних властивостей S-блоків, що застосовуються у них. Класичний підхід [1] до оцінки криптографічної якості S-блоків передбачає їх уявлення за допомогою математичного апарату булевих функцій, до яких застосовується стандартний набір критеріїв криптографічної якості: нелінійність, лавинні характеристики, кореляційні характеристики.

Однак дослідники все більш наполягають [2] на необхідності вивчення не тільки криптографічних показників компонентних булевих функцій сучасних шифрів, а також їх компонентних функцій багатозначної логіки (ФБЛ). Сьогодні існує набір критеріїв криптографічної якості ФБЛ, подібний до набору [1], створеного для булевих функцій. Відомі також публікації, присвячені дослідженню криптографічної якості відомих шифрів при їх виявленні за допомогою ФБЛ [3, 4].

Тим не менш, сучасні дослідження показують, що одними з найперспективніших методів синтезу S-блоків, є методи, засновані на теорії динамічного хаосу, яка дозволяє отримати підстановлювальні конструкції, що є