Рис. 2. – Стадіон із сонячними батареями.

Підводячи підсумки, можу зробити висновок що отримання енергії від сонця мабуть одне із найвагоміших відкриттів нашого століття. Навіть не дивлячись на те, що винайшли дану ідею ще сотні років тому, активно втілювати її в життя почали тільки тепер.

Список використаних джерел

1. *Барило А.А., Будько В.І., Васько П.Ф., Величко В.В., Донець А.М., Жовмір М.М. Атлас енергетичного потенціалу поновлюваних джерел енергії України. – Київ: енергетики України, 2020. – 82 с.*
2. *Ю. А. Соколович, Г. С. Богданова.— С59 Фізика: Навчально-практичний довідник: Видавництво «Ранок», 2010.— 384 с.*

УДК 004.415.2

Рудь О. С., здобувачка,
Зелінська О.В. доцент
кафедри інформаційних технологій

АУТЕНТИФІКАЦІЯ ТА ЇЇ МЕТОДИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Більшість з нас є користувачами різних інформаційно-комунікаційних систем, оскільки сьогодні це є невід'ємною частиною нашого життя. Тож, щодня ми зустрічаємося з процесами ідентифікації та аутентифікації аби підтвердити свою особистість. Це відбувається щоразу, коли ми вводимо свій пароль для

доступу, до мережі або ж при запуску тієї чи іншої програми. Якщо даний процес завершується успішно, користувач отримує доступ до певних ресурсів, відповідно, в іншому випадку доступу немає. Аутентифікація- це обов'язковий етап функціонування будь-якої новочасної інформаційно-комунікаційної системи.

Тож, існують різні методи аутентифікації, що відрізняються за різними критеріями. Відмінність може бути у вартості, складності, надійності, стійкості та у багатьох інших показниках. Кожен метод безумовно має свої переваги та недоліки, які ми будемо розглядати нижче [1].

Мета: аналіз запропонованих методів аутентифікації; розгляд їх перспективності, розвитку.

Методи аутентифікації бувають:

1) однобічними

2) двобічними

3) трибічними

Однобічною аутентифікацією є випадок, коли користувач доводить власну аутентичність задля доступу до певної інформації. Двобічна, в свою чергу, включає в себе підтвердження не тільки від користувача, а ще й від системи. Часто такий метод використовується в банках. В трибічній аутентифікації використовується вже нотаріальна служба автентифікації. Це робиться для підтвердження достовірності кожного з партнерів в обміні даними.

Також їх ще можна поділити на однофакторні та двофакторні методи.

Однофакторні, в свою чергу, бувають:

• логічні

-паролі

-ключові фрази, що вводяться з клавіатури пристрою

• ідентифікаційні

-носіями ключової інформації можуть бути: дискета, магнітна карта, штрих-кодова карта, тощо.

Недоліки:

для зчитування інформації з носія необхідний спеціальний рідер;

носій можна згубити чи пошкодити, його можуть викрасти або ж зробити копію-підробку

• біометричні

в їх основі лежить аналіз унікальних людських характеристик. Це можуть бути відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя, сітківка ока і тд.

Недоліки:

Ці методи дорогі і складні в обслуговуванні;

чутливі до зміни параметрів носія інформації та призначені лише для аутентифікації людей [2].

Розглянемо детальніше біометричні методи аутентифікації (рис. 1).

Рисунок 1. - Класифікація методів біометричної автентифікації користувачів

Аутентифікація за відбитками пальців

Аутентифікації за відбитками пальців – найпоширеніша біометрична технологія автентифікації користувачів. Метод використовує унікальність рисунка папілярних візерунків на пальцях людей. Відбиток отримується за допомогою сканера та перетворюється на цифровий код, а потім порівнюється з раніше введеними наборами еталонів. Переваги використання цього методу – легкість у використанні, зручність і надійність. Універсальність цієї технології дозволяє застосовувати її в будь-яких сферах і для вирішення будь-яких і найрізноманітніших завдань, де необхідна достовірна і досить точна ідентифікація користувачів.

Використання геометрії руки

Даний статичний метод побудовано на розпізнаванні геометрії кисті руки за допомогою спеціальних пристроїв, що дозволяють отримувати 3-вимірний образ кисті руки. Отримані дані використовують для отримання унікальної згортки, що однозначно ідентифікує людину. Існує два основних підходи до використання геометричних характеристик кисті руки. Перший з них ґрунтується на геометричних характеристиках руки. Другий вводить ще і образні характеристики руки (образи на стиках між фалангами пальців і візерунки кровоносних судин).

Аутентифікація за райдужною оболонкою ока

Методи ідентифікації особи за райдужною оболонкою ока побудовані за одним принципом – виділення частотної або будь-якої іншої інформації про

текстуру райдужної оболонки із зображенням і збереженням цієї інформації у вигляді спеціальних кодів. Можна порівнювати коди райдужних оболонок і зберігати в базі даних. Побудова коду здійснюється в три етапи:виділення зображення райдужної оболонки із загального зображення; обробка отриманого зображення, наприклад, усунення шуму, поліпшення зображення, у тому числі вирівнювання гістограми, усунення відблиску; деякі методи "розгортають" круглу зіницю в прямокутне зображення – відбувається перехід від полярних координат в декартові; інколи після такої "розгортки" частина зображення відсікається, щоб накопичена на даному етапі помилка не вплинула на складання коду; перетворене зображення фільтрується способом, залежним від конкретного методу; за результатами фільтрації складається представлення у вигляді коду.

Аутентифікація за рисами особи

Розвиток цього напрямку пов'язаний зі стрімким зростанням мультимедійних відеотехнологій. Однак більшість розробників все ще мають труднощі з досягненням високого рівня продуктивності для цих пристроїв. Однак найближчим часом можна очікувати появи в залах аеропорту спеціальних пристроїв розпізнавання облич для захисту від терористів тощо.

Аутентифікація за сітківкою ока

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Ймовірність пропуску незареєстрованого користувача при скануванні сітківки ока складає 0,0001%. При цьому ймовірність помилки другого роду досить висока — порядка 0,1%. Це пояснюється тим, що спочатку дані системи були розроблені на замовлення військових, де до помилок першого роду пред'являють найжорсткіші обмеження. При цьому передбачається, що користувачі можуть повторити процедуру автентифікації кілька разів [3].

Багатофакторні методи аутентифікації отримують в результаті комбінації двох різних однофакторних методів. Як приклад: «пароль + дискета» чи «магнітна карта + PIN».

Кожен клас методів має свої переваги й недоліки. Майже всі вони страждають на один недолік - аутентифікують не конкретного суб’єкта, а лише фіксують той факт, що аутентифікатор суб’єкта відповідає його ідентифікатору.

Список використаних джерел

1. Методи аутентифікації користувачів інформаційно-комунікаційних систем (asv.gov.ua)
2. Методи аутентифікації - Ідентифікація та аутентифікація (google.com)
3. 26.pdf (kpi.ua)