Список використаних джерел

1. Застосування інформаційно-психологічних прийомів [Електронний ресурс] – Режим доступу до ресурсу: http://personal.in.ua/article.php?ida=301

2. Інтернет і його вплив [Електронний ресурс] – Режим доступу до ресурсу: https://applied-research.ru/ru/article/view?id=10618.

3. Інформаційно-психологічний вплив [Електронний ресурс] – Режим доступу до ресурсу: https://pidruchniki.com/1056112736938/politologiya/informatsiyno-psihologichniy_vpliv

---

УДК 004.056.53

КІБЕРБЕЗПЕКОВІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ЗА ДОПОМОГОЮ СКАНУВАННЯ ВІДБИТКІВ ПАЛЬЦІВ

Іллюшко Б. О., ст. гр. КБ-181, **Дьогтяр Р. С.,** ст. гр. ПЕ-181
Наукові керівники: **Петренко Т. А.,** доцент, **Єршов Р. Д.,** старший викладач
Національний університет «Чернігівська політехніка»

У сучасному світі загальної інформатизації особливого значення набувають завдання захисту інформації. Однією з основних задач забезпечення інформаційної безпеки є обмеження кола осіб, що мають доступ до конкретної інформації, і захисту її від несанкціонованого доступу. Біометричні системи автентифікації - системи, що використовують для посвідчення особи людей їх біометричні дані. Наприклад, такими даними можуть бути відбитки пальців людини [3].

Дані тези висвітлюють кібербезпекові аспекти створення системи контролю доступу, яка може бути інтегрована до складу дверей, сейфу, засобів пересування, та інших побутових приладів, конструкція яких дозволяє використовувати сканер відбитку пальців та електромагнітний замок, як однією зі своїх складових частин.

Основними критеріями, відносно яких відбувається вибір сканера відбитку пальців, є: простота використання зі сторони користувача, зручність програмування зі сторони розробника, надійність модуля. Проаналізувавши доступні різновидності сканерів відбитків, їх вартість та популярність, вибір зупинився на сканері ZFM-20 (рис.1). Даний сканер відбитків пальців дозволяє створити систему контролю доступу, засновану на дактилоскопічної ідентифікації.

Рисунок 1 – Сканер відбитку пальців ZFM-20.

Дактилоскопічна ідентифікація - встановлення або підтвердження відбитків шкіри певної людини за особливостями її візерунків шляхом проведення дактилоскопічної експертизи. Дактилоскопічна експертиза - дослідження та вивчення візерунків шкіри людини та її відбитків для доведення їх тотожностей чи встановлення відмінностей. Даний сканер

вирішує такі проблеми кібербезпеки та безпеки людини, які пов’язані з контролем доступу до будь-яких предметів або приміщень за допомогою сучасних технологій[2].

Для створення системи контролю доступу, модуль виконує такі функції:

1) Реєстрація відбитків пальців в базі даних модуля;
2) Видалення відбитків пальців з бази даних модуля;
3) Пошук відбитків пальців в базі даних модуля;
4) Порівняння поточного відбитка пальця з відбитками пальців в базі даних модуля.

Даний сканер відбитку пальців є однією з головних частин пристрою системи контролю яка включає в себе:

1) Модуль Arduino (МК + програматор);
2) Сканер відбитків пальців інтерфейс);
3) LCD-дисплей (інтерфейс);
4) Зумер (Trema);
5) Дискретні кнопки (Trema);
6) Дискретні світлодіоди (Trema);
7) Силовий напівпровідниковий ключ;
8) Електромагнітний замок (соленоїд);
9) Модуль розширення (Trema Shield);
10) Джерело живлення 12В постійного струму;
11) З’єднувач форм-факутора Power Jack.

Алгоритм сканування пальця за допомогою ZFM-20:

Ви побачите наступні рядки: “Scan sensor ... Found sensor! Please put your finger on the scanner …”При цьому сканер модуля буде блимати червоним кольором. Прикладіть палець до сенсора. Якщо Відбиток Вашого пальця є в базі модуля, то на моніторі відобразиться напис: “Found ID = 5, with confidence of 73”, де перше число (у нашому прикладі, це 5) відповідає ID номером під яким записаний співпавший відбиток пальця, а останнє число (у нашому прикладі, це 73) означає рівень відповідності відбитка прикладеного пальця, відбитку збереженому в базі [1].

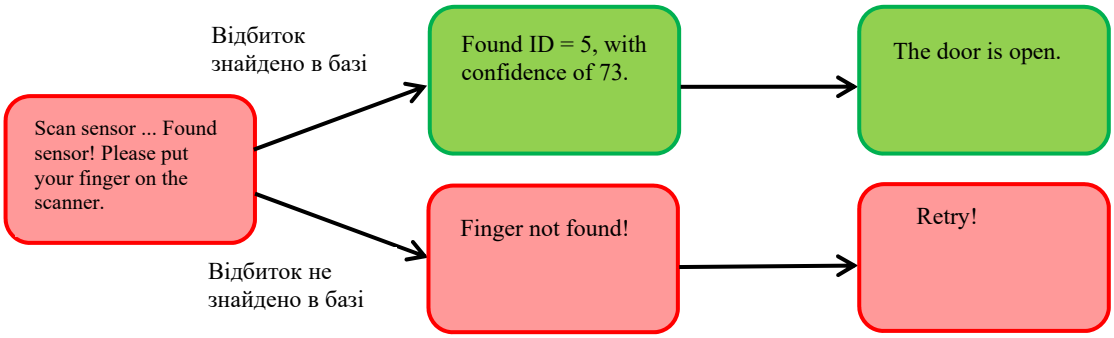

Рисунок 2 – Схема роботи сканування пальця

Алгоритм реєстрації відбитків пальців в базі відбитків модуля:

Ви побачите наступні рядки: "Scan sensor ... Found sensor! Please enter ID number You want save ...". Введіть в монітор послідовного порту число (ID номер під яким потрібно зберегти новий відбиток пальця) і натисніть Enter. На моніторі відобразиться напис: "Please put your finger on the scanner ...". Прикладіть палець до сканера модуля, після того як сканер вважає зображення Вашого відбитка пальця, на моніторі з'являться ще два рядки: "Image converting: Ok! Please remove your finger from the scanner ..." Відпустіть палець від сканера, на моніторі з'явиться напис: "Place same finger again ...". Прикладіть той же палець до сканера модуля ще раз, на моніторі з'являться такі рядки: "Image converting: Ok! Creating model: Ok! Saving model in ID = 0: Ok!" Тепер відбиток Вашого пальця збережений в базі відбитків модуля і братиме участь в порівнянні[1].

Дивлячись на вищенаведені алгоритми роботи сканера, можемо побачити що зі сторони його програмування були збережені певні норми кібербезпеки. При скануванні пальця, якщо його схожість менша за 60 одиниць, при максимальному рівні в 100 одиниць, користувачу буде відказано в доступі. Кожному відбитку присвоюється унікальний ID. При занесенні нового відбитку в базу сканера, притуляти палець потрібно 2 рази, щоб сканер мав змогу чітко провести дактилоскопічна ідентифікацію. Тільки програміст має змогу редагувати або видаляти безпосередньо відсканованні відбитки.

Таким чином, за допомогою аналізу ринку відповідних пристроїв, пошук необхідних компонентів відповідно поставлених цілей було створено робочу модель контролю доступу за допомогою сканера відбитку пальців з цифровим дисплеєм та багатофункціональним меню. Шляхом вдосконалення проекту є забезпечення автономного живлення пристрою за допомогою акумуляторів та написання програми для керування приладом з ПК.

Список використаних джерел

1. IARDUINO [Электронный ресурс] // Урок 28. Контроль доступу по відбитку пальця. URL: https://lesson.iarduino.ru/page/urok-28-kontrol-dostupa-po-otpechatku-palca/

2. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах - НД ТЗІ 2.5-008-2002

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов - Д.А., Хорошко В.А., Под ред. В.А. Хорошко. - К. : Арий, 2008

УДК 004.056.53

ОСНОВНІ ЗАХОДИ ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ THE INTERNET OF THINGS

Мальцева М. В., студ. гр. КБ-161
Науковий керівник**: Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

На даний момент ми є свідками посилення тенденції автоматизації різноманітних сфер життєдіяльності. Інформаційні та телекомунікаційні технології стали не тільки невід'ємною частиною повсякденного життя сучасної людини, але і необхідною технологічною платформою для організації сучасних бізнес-процесів. Активний розвиток смартфонів, створення мобільних додатків для гаджетів дозволяють оперативно відслідковувати, фіксувати, зберігати різну інформацію, пов'язану з життєдіяльністю людини: від списку контактів, здійснення банківських транзакцій, покупок в Інтернеті до відстеження фізичного та емоційного самочуття людини [1] Однією з технологій, яка стає все більш популярною за останні роки стала концепція Інтернет речей (The Internet of Things, IoT). Інтернет Речей або Internet of Things (IoT) - це мережа речей, які підключені до мережі Інтернет. Ці речі включають IoT-пристрої і фізичні об'єкти, оснащені IoT [2].

Інтернет Речей (IoT) це новий крок в еволюції сучасного Інтернету, де будь-який фізичний об'єкт (в термінах Інтернету Речей Thing), оснащений обчислювальними і комунікаційними можливостями, може бути ефективно інтегрований на різних рівнях в Інтернет. Метою роботи є визначення сфер застосування, основних принципів та методів захисту концепції Інтернет речей.

Інтернет речей дає можливість нових способів управління і моніторингу віддалено виконуваних операцій в будь-яких сферах. Він дозволяє повністю контролювати віддалено розташовані об'єкти і постійно передавати інформацію в сховище даних. Інтернет речей - це не тільки виконавчий холодильник, який сам замовляє улюблену їжу господаря, або послужливий чайник, який кип'ятить воду на першу вимогу зі смартфону. Це розумні датчики