

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

НА ТЕМУ

ВДОСКОНАЛЕННЯ МЕТОДУ ТРИФАКТОРНОЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ
ПОЄДНАННЯ БІОМЕТРИЧНОГО СКАНУВАННЯ ВІДБИТКІВ ПАЛЬЦІВ,
QR-ІДЕНТИФІКАТОРА ТА ПАРОЛЬНОЇ ІДЕНТИФІКАЦІЇ

ВИКОНАВ: СТУДЕНТ ГРУПИ УБ-19_м БЛОНСЬКИЙ ВЛАДИСЛАВ

НАУКОВИЙ КЕРІВНИК: К. Т. Н., ПРОФЕСОР КАФ. МБІС: АЗАРОВА АНЖЕЛІКА ОЛЕКСІЇВНА

МЕТА РОБОТИ: Вдосконалення методу трифакторної аутентифікації на основі поєднання біометричного сканування відбитків пальців, QR-ідентифікатора та парольної ідентифікації.

АКТУАЛЬНІСТЬ ТЕМИ:

- Дотримання правил розмежування доступу до інформації в організації;
- Усунення можливості несанкціонованого доступу до інформації;
- Необхідність забезпечення конфіденційності та цілісності інформації;
- Передчасне виявлення витоку інформації.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРИСТРОЇВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Для досягнення найвищого рівня безпеки використовується двофакторна/трифакторна ідентифікація/автентифікація користувачів, які хочуть отримати доступ до конфіденційної інформації у системах безпеки.

Також використовуються:

- Паролі, що мають довжину не менш як вісім символів, великі та малі букви та інші символи;
- Картки контролю доступу **RFID**;
- Авторизацію через смартфон;
- Ідентифікатор у вигляді штрихкоду або **QR**-коду;
- Біометричні ознаки людини, які невід'ємні від неї.

Саме останнє є найбільш безпечним та порівняно простим способом захисту та контролю доступу до середовища із конфіденційною інформацією, адже невід'ємні ознаки від людини відділити неможливо, так як і відтворити їх.

ІСНУЮЧІ АНАЛОГИ ПРИСТРОЮ

На сьогодні існують різні варіації біометричних замків із додатковими можливостями окрім біометричної автентифікації користувача:

- Електричний замок із картою доступу **RFID**;
- Електричний замок із скануванням відбитку пальця;
- Електричний механічний замок із можливістю відкривання по фізичному ключу;
- Електричний замок із використанням паролю.
- Електричний замок із використанням смартфона.

TTLOCK-BOSS



TTLOCK-HANDLE



TTLOCK-SLIM



НЕДОЛІКИ ІСНУЮЧИХ ПРИСТРОЇВ

- Однокорпусне виконання пристрою, що дозволяє отримати зловмиснику доступ до керуючих компонентів;
- Малий строк служби при автономному живленні від батареї типу АА;
- Відсутність можливості керування роботоздатністю пристрою;
- Наявність в деяких моделях механічного замка, що надає можливість отримання доступу зловмисником;
- Відсутність сповіщення системи безпеки про несанкціонований доступ;
- Низька якість використовуваних матеріалів.

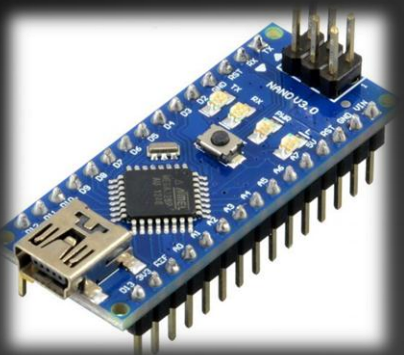
ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ARDUINO

Arduino — торгова марка апаратно-програмних засобів для побудови простих системних рішень автоматизи.

- Програмна частина платформи складається із оболонки (**IDE**) для написання, компіляції програм.
- Апаратна частина представляє собою набір змонтованих плат із мікроконтроллером.

Існують наступні варіанти рішень **Arduino**:

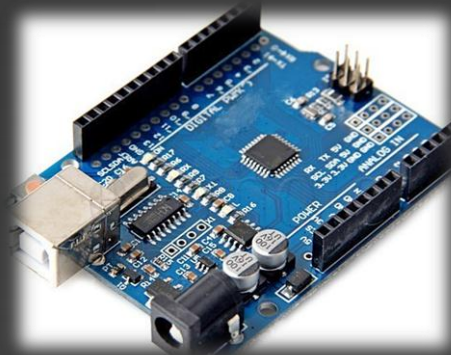
Nano



Pro micro



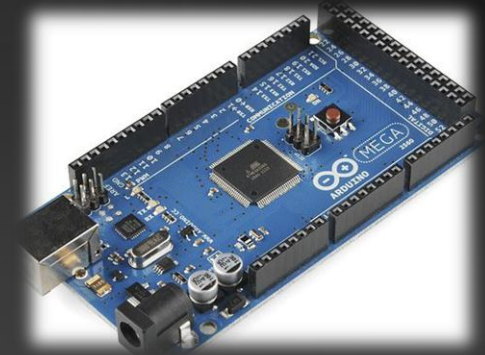
Uno R3



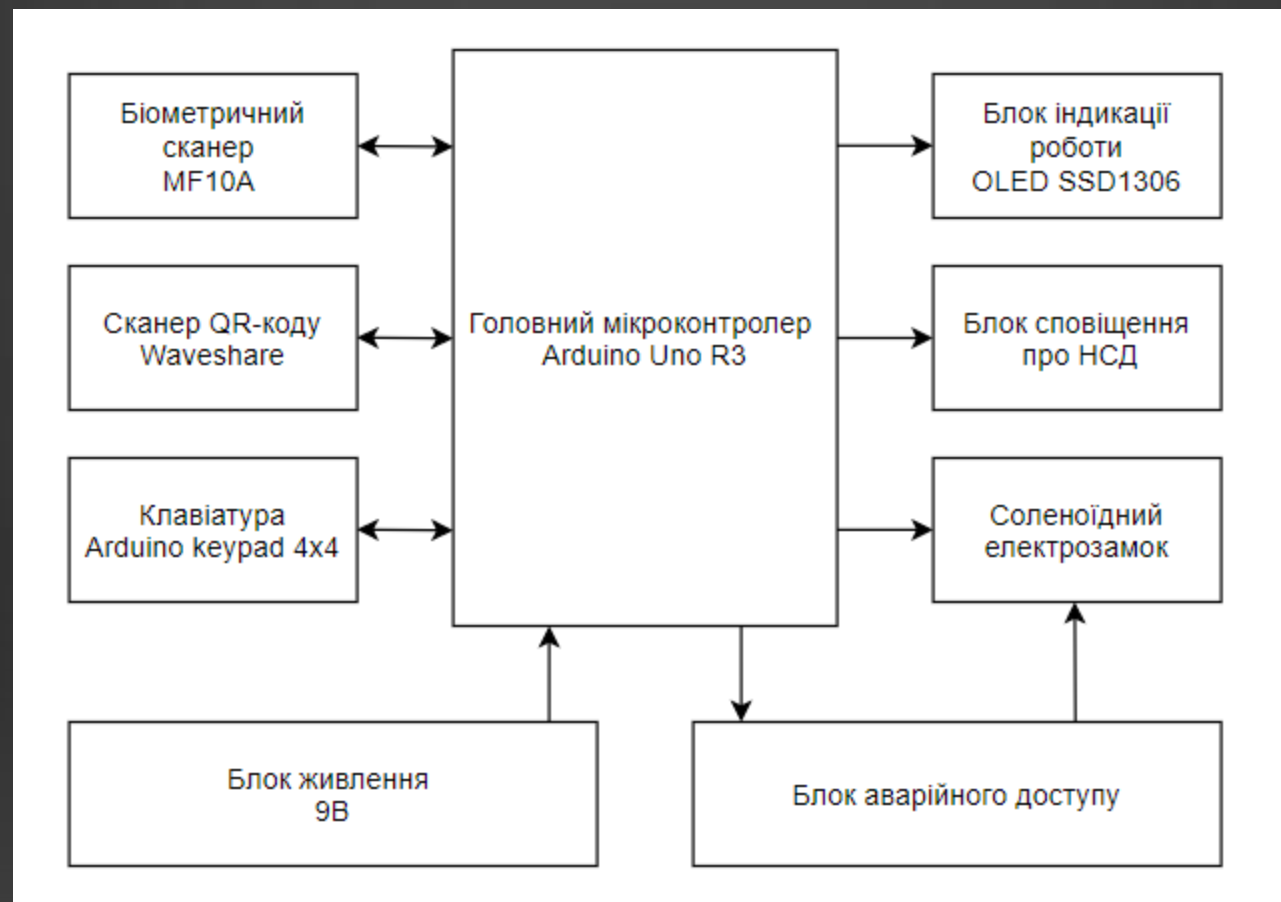
DUE



MEGA



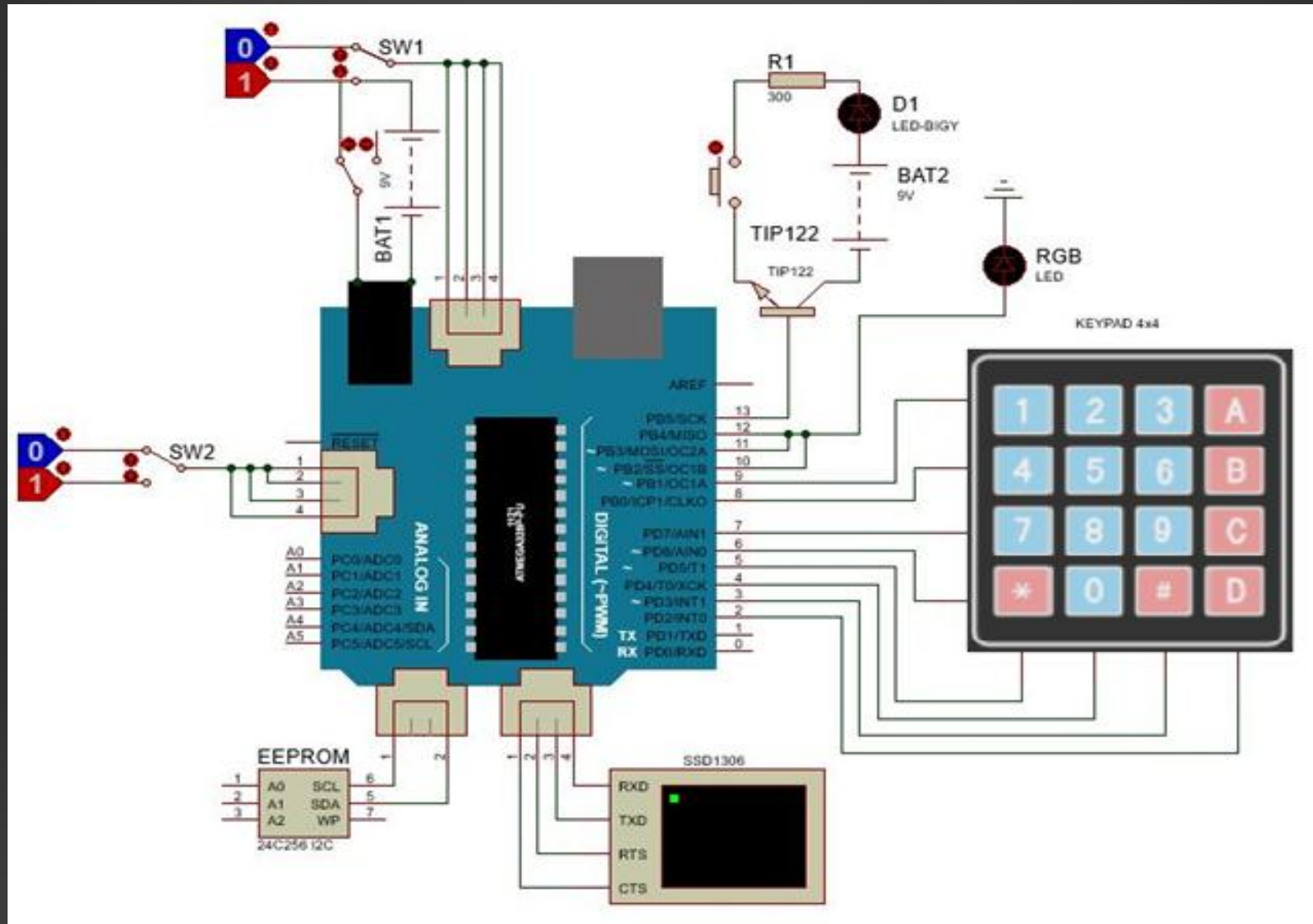
СТРУКТУРНА СХЕМА ПРИСТРОЮ



БЛОК-СХЕМА АЛГОРИТМУ ПРИСТРОЮ



СХЕМАТИЧНА МОДЕЛЬ ПРИСТРОЮ



МЕТОДИКА РОБОТИ З ПРИСТРОЄМ

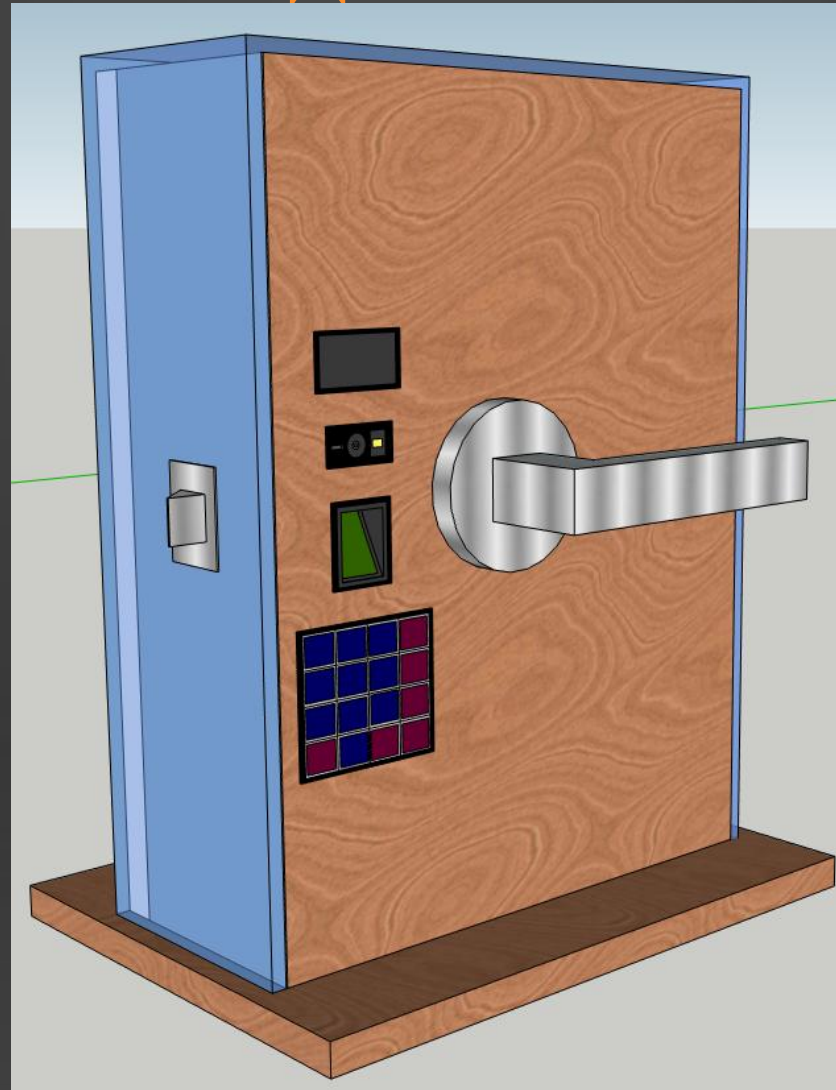
Перш за все необхідно встановити пристрій наступним чином:

- Встановити **OLED** дисплей, сканер **QR**-коду, сканер відбитків пальців, а також клавіатуру **4x4** на поверхні дверей, у зручному для користувачів місці та висоті;
- Керуючі компоненти встановити у недоступному для звичайного користувача місці;
- Електрозамок під'єднати до контролера;
- Сигнал сповіщення про НСД під'єднати до системи безпеки.

Виконати налаштування пристрою:

- Під'єднати контролер до ПК і виконати реєстрацію користувачів у базі даних;
- Перевірити правильність роботи пристрою.

ВИГЛЯД ПРИБОРУ



ДЯКУЮ ЗА УВАГУ!