Вінницький національний технічний університет

Спеціальність 125 «Кібербезпека»

Магістерська кваліфікаційна робота на тему:

«Розробка методу захисту зовнішніх носіїв інформації від використання несанкціонованими користувачами»

Виконав: студент групи УБ-16м
Погорєлов Олександр
Керівник: д.т.н. проф. Яремчук Ю.Є.

Актуальність

На сьогоднішній день існують такі методи захисту зовнішніх носіїв інформації:

- стандартні засоби Windows;
- спеціальні програми для встановлення пароля;
- носії інформації з криптографічним шифруванням;
- активація ПІН кодом;
- захист від перебору пароля;
- захист від вірусів.

Дані засоби враховують тривалий захист інформації, але не гарантують повну безпеку даних через період часу. Але дані з часом можливо розшифрувати та підібрати паролі.

Врахувавши недоліки існуючих систем захисту, пропонується розробити комплексний метод захисту зовнішніх носіїв інформації.

Постановка задач

- ✓ Об’єктом дослідження є процес створення захищеного носія інформації.
- ✓ Предмет дослідження – розроблення методу захисту носіїв інформації.
- ✓ Теоретичне значення результатів роботи: результати даної роботи

можуть бути застосовані для захисту зовнішніх носіїв інформації на об’єктах це циркулює інформації з обмеженим доступом.

- ✓ Наукова новизна: створення методу захисту зовнішніх носіїв інформації

Аналіз можливих атак на носії інформації

- неправомірне оволодіння носієм інформації;
- порушення авторських прав на інформацію;
- модифікація інформації на зовнішньому носію;
- знищення інформації;

Імовірність реалізації внутрішніх каналів витоку інформації через зовнішні носії інформації

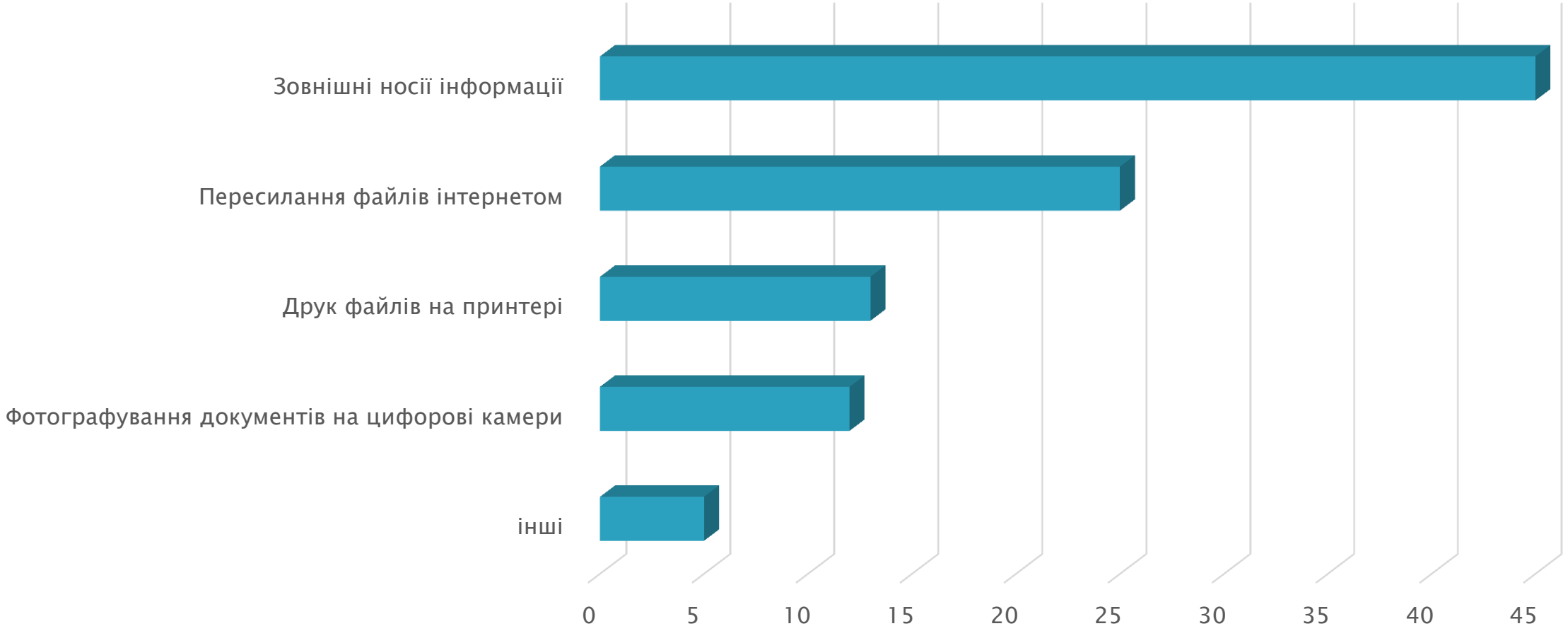
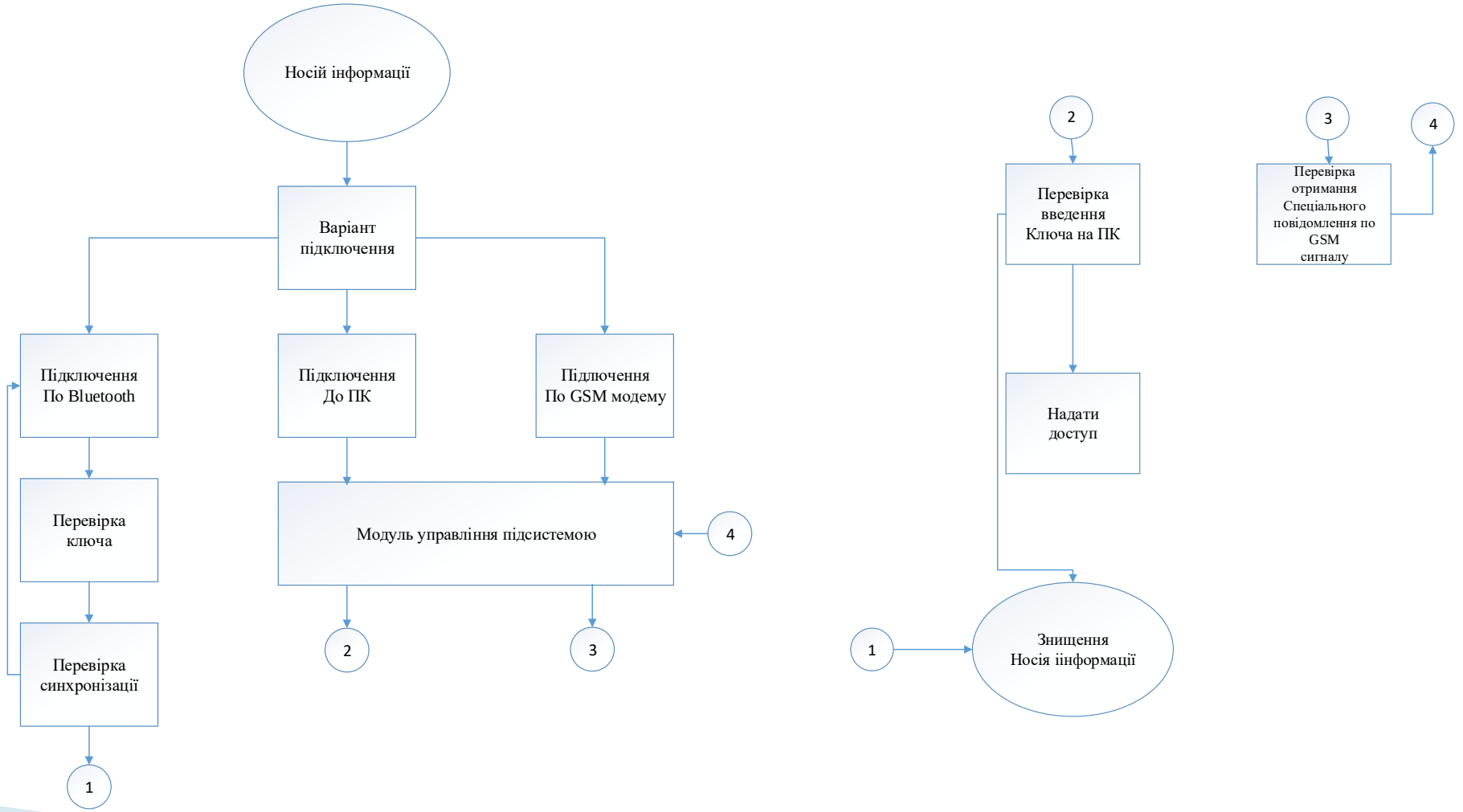
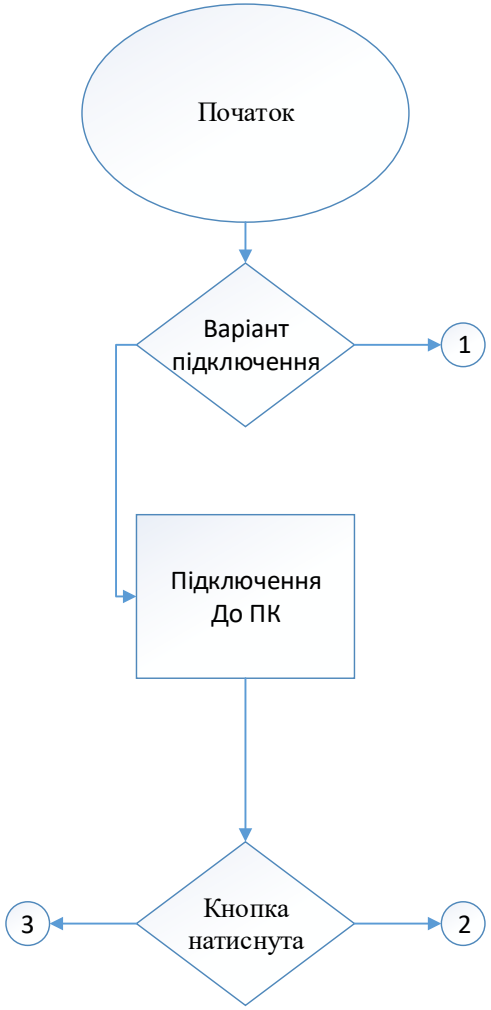
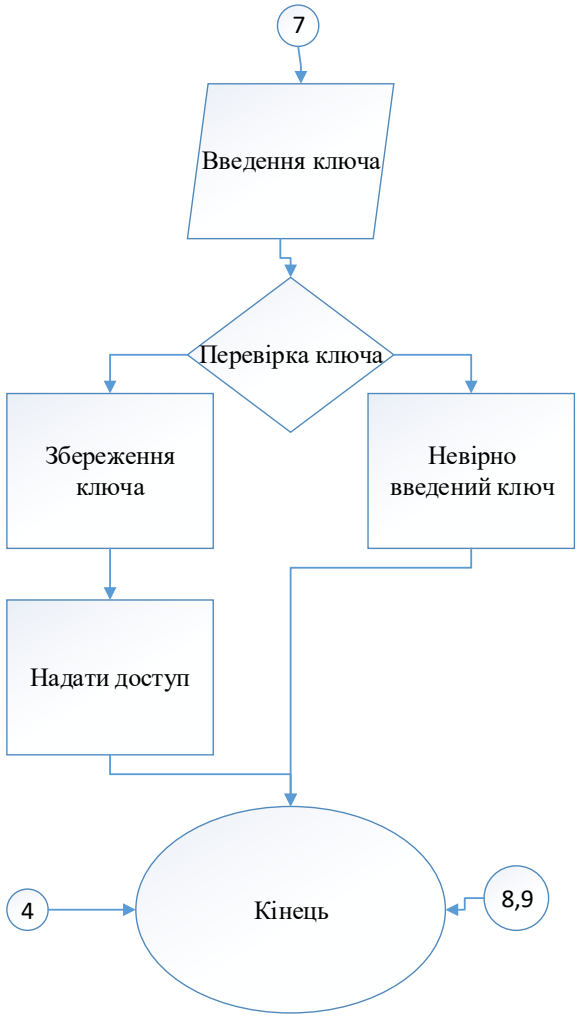


СХЕМА МЕТОДУ ЗАХИСТУ ЗОВНІШНІХ НОСІЇВ ІНФОРМАЦІЇ

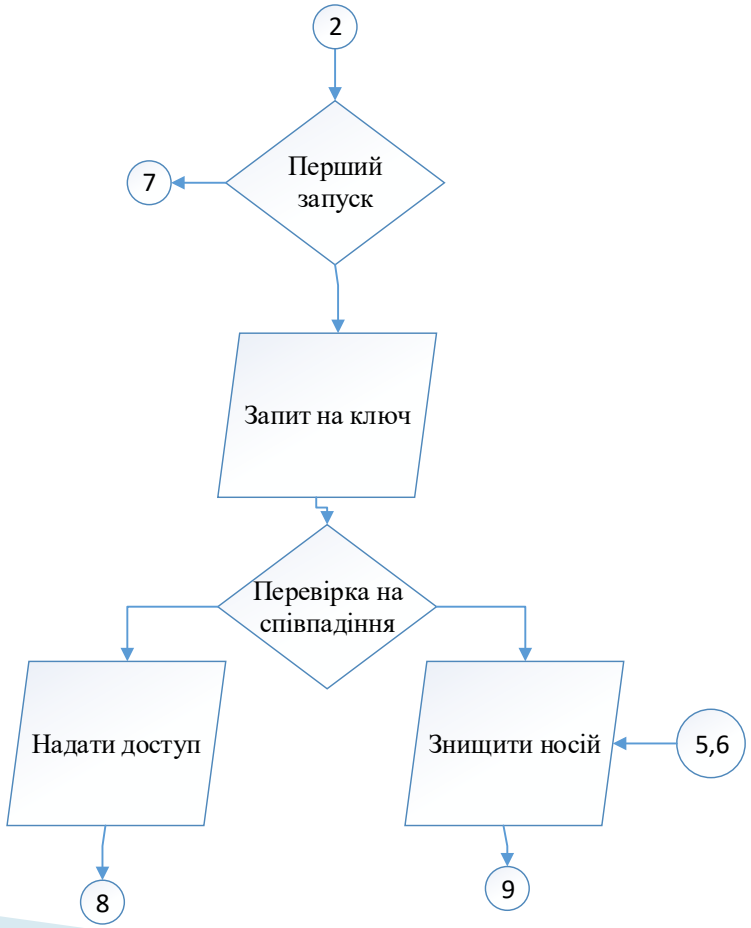


Розробка блок схеми алгоритму роботи мікроконтролера

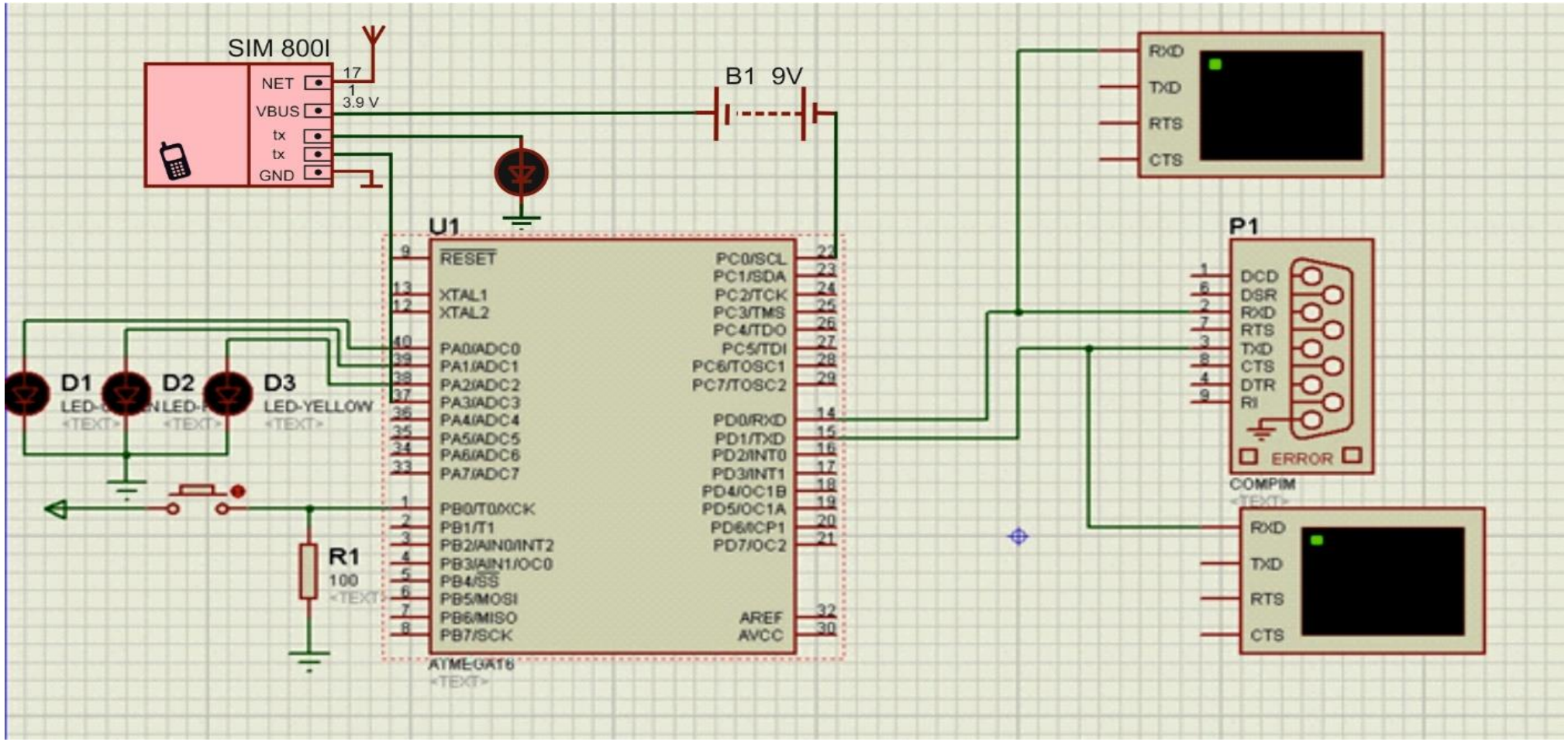




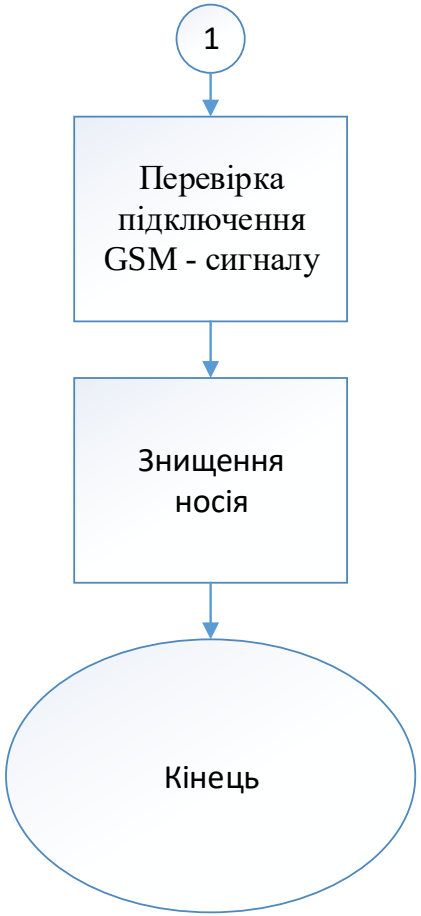
Розробка блок схеми алгоритму роботи мікроконтролера

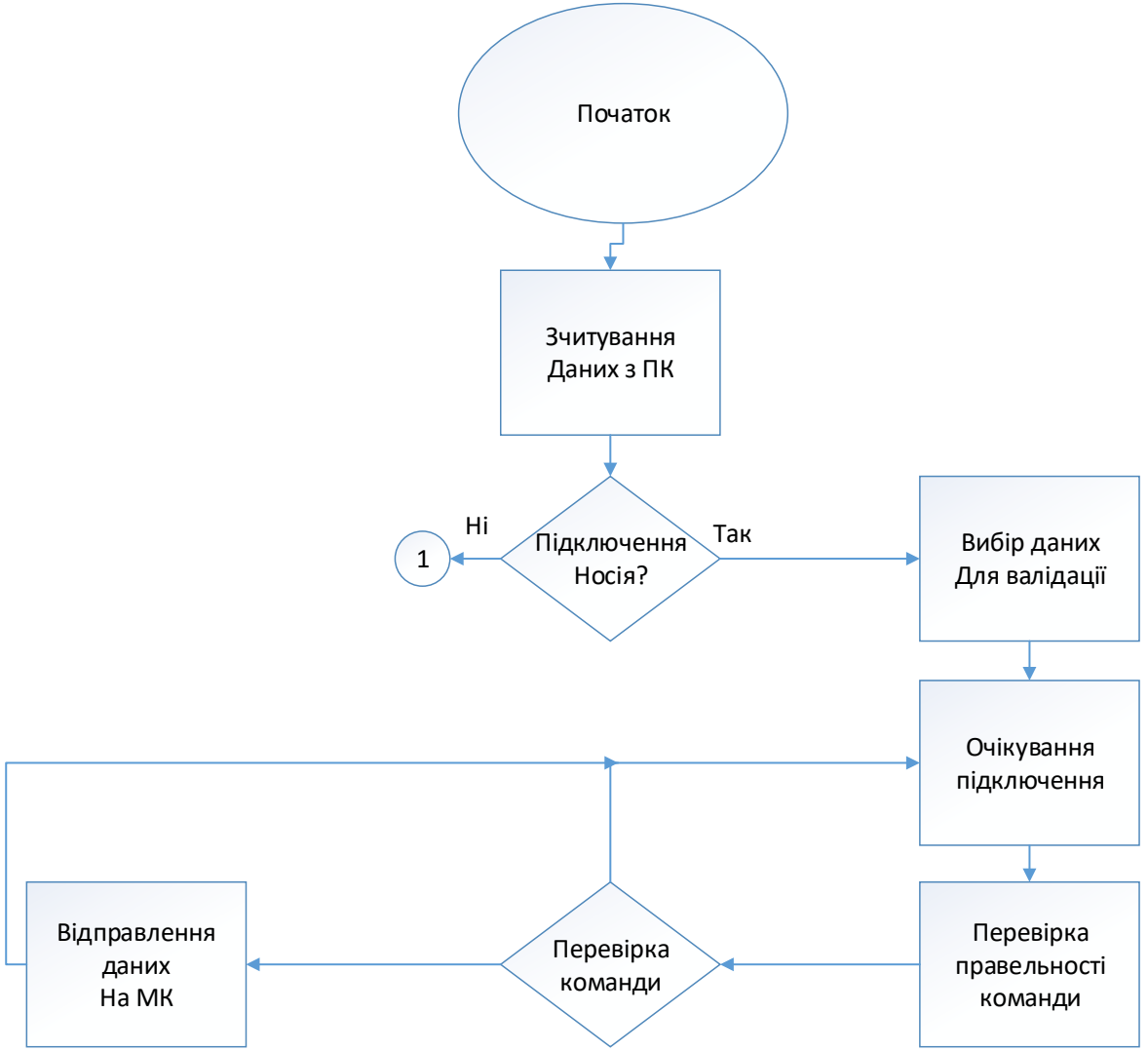


Проектування схеми мікроконтролера



Розробка блок схеми підсистеми управління для ПК



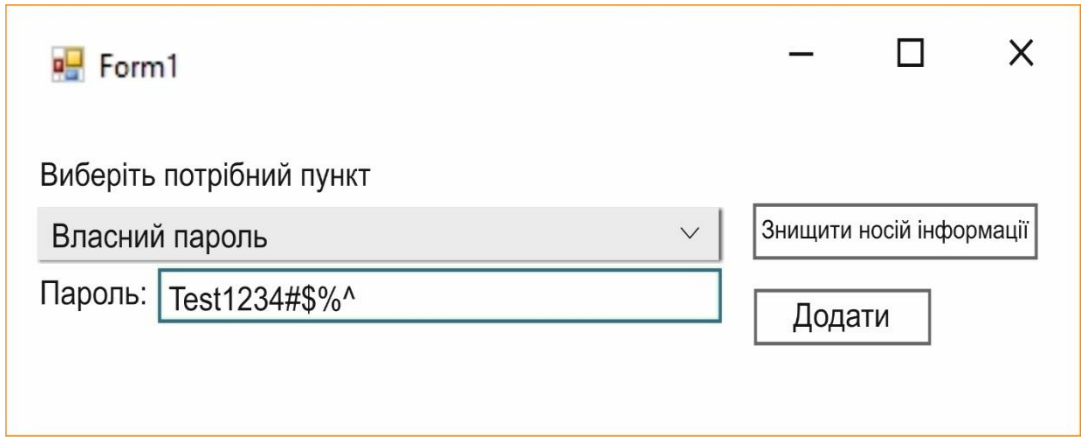


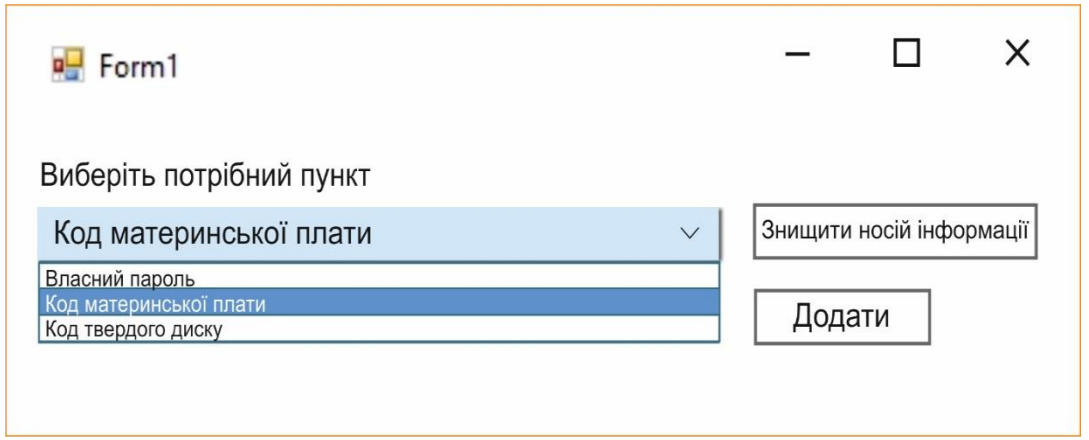
Інструкція користувача

Крок 1. Запустити модуль захисту.

Крок 2. Вибір реєстрації з випадаючого списку (пароль повинен містити великі та малі букви, цифри, символи).

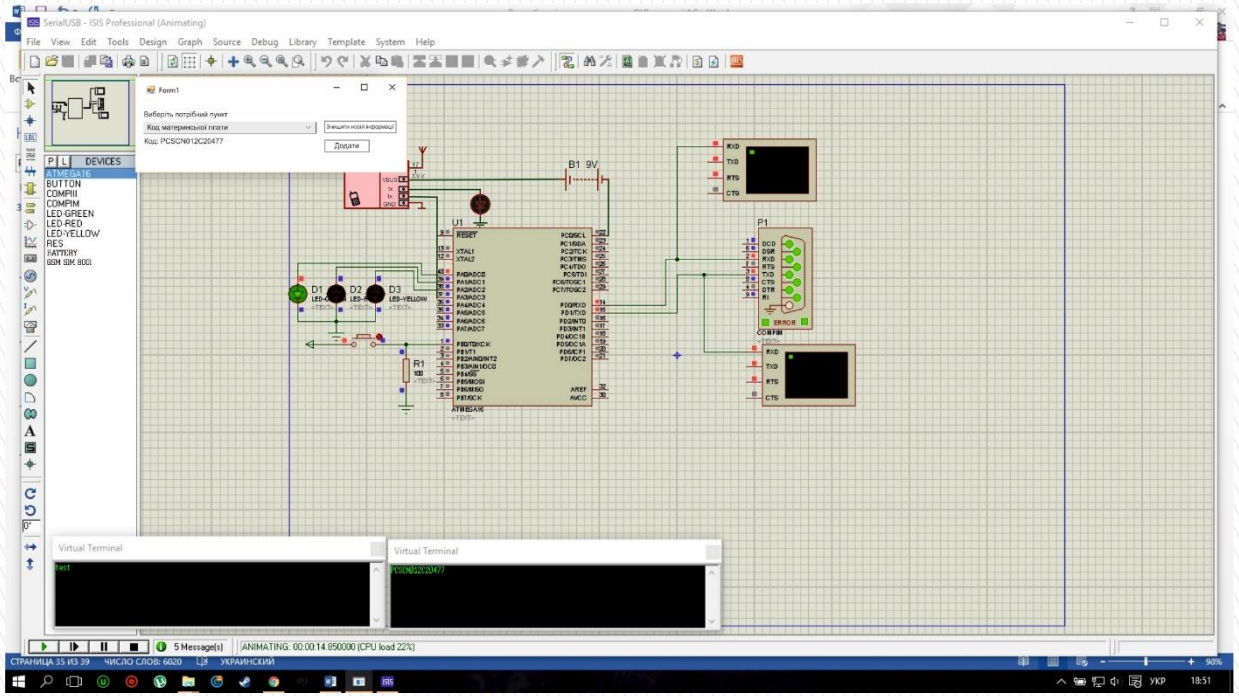
Крок 3. Підключити носій інформації.



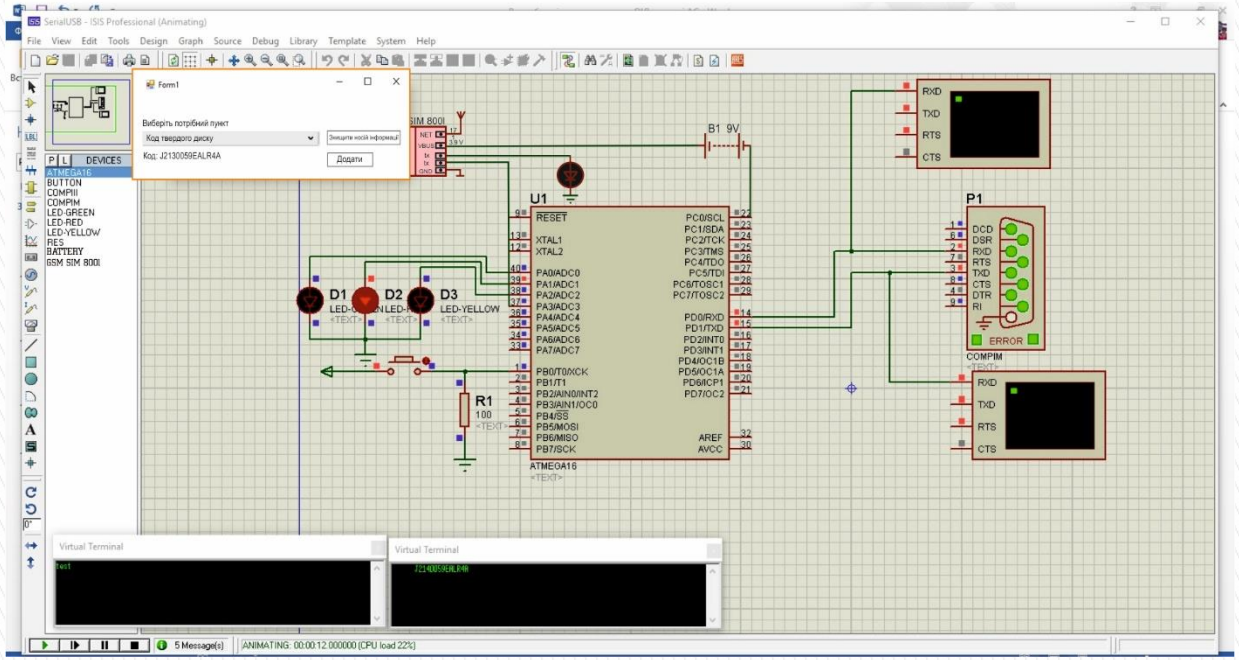


Випробуваня методу взаємодії з недовіреним ПК

Прив’язування по серійному номеру материнській платі

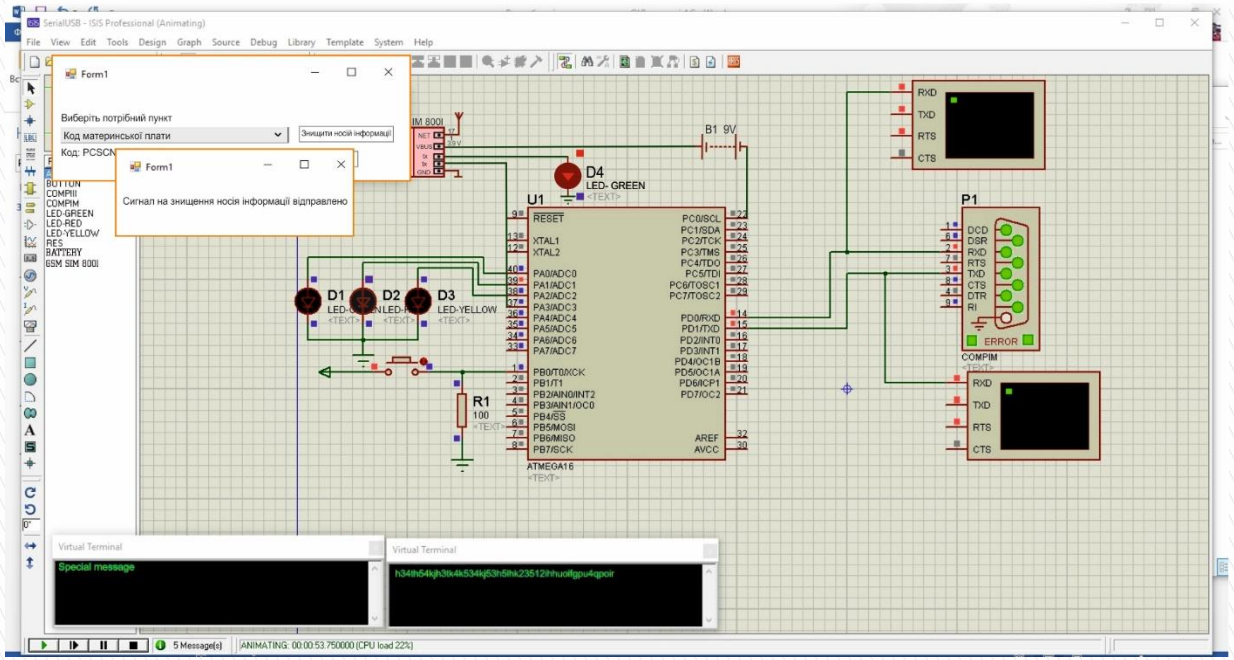


Перевірка по серійному номеру жорсткого диску



Випробуваня методу відправлення спеціального повідомлення на GSM модуль

- Загорівся червоний сигнал, який показує що на носій інформації було відправлено спеціальне повідомлення
- (h34th54kjh3tk4k534kj53h5lhk23512ihhuoifgpu4qpoir).
- Після отримання спеціально повідомлення, мікроконтролер
- перевіряє ключ на співпадіння.
- Якщо повідомлення співпадає з записаним у МК то носій інформації знищує себе.



ВИСНОВКИ

- В даній дипломній роботі було розроблено метод захисту зовнішніх носіїв інформації від використання несанкціонованими користувачами.
- Було створено два програмних продукти, що дають змогу зберегти носії інформації, які містять інформацію з обмеженим доступом, від крадіжки зловмисниками або від випадкової передачі таємної інформації. У ситуації коли користувач помилково, залишив носій інформації, а потенційний зловмисник намагається викрасти важливі дані, даний носій інформації можливо буде знищити віддалено по GSM сигналу або носій інформації сам себе знище при взаємодії з недовіреним ПК.
- Таким чином, якщо носій інформації буде викрадено, незалежно чи це довірений працівник чи зловмисник, то можна бути впевненими, що інформація розкрита не буде.
- Отже, використання даного методу захисту доцільне для захисту інформації від витоку через знімні накопичувачі даних.

ДЯКУЮ ЗА УВАГУ