Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
кафедра автоматизації технологічних процесів і виробництв
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: «Розробка мобільної системи автоматизованого контролю несанкціонованого доступу до приміщень»

Виконав(ла): студент(ка) IV курсу, групи КАс-41
спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»
(шифр і назва спеціальності)

(підпис) Гулій Р.П. (прізвище та ініціали)

Керівник (підпис) Трембач Р.Б. (прізвище та ініціали)

Нормоконтроль (підпис) Козбур В.Р. (прізвище та ініціали)

Завідувач кафедри (підпис) Савків В.Б. (прізвище та ініціали)

Рецензент (підпис) Королюк Р.І. (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра автоматизації технологічних процесів і виробництв
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Савків В.Б.
(підпис) (прізвище та ініціали)
« ___» _____2023р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології»
(шифр і назва спеціальності)

студенту Гулій Роману Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка мобільної системи автоматизованого контролю несанкціонованого доступу до приміщень»

Керівник роботи к.т.н., доцент Трембач Р.Б.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «02» лютого 2023 року № 4/9-117
2. Термін подання студентом завершеної роботи 10 червня 2023 року
3. Вихідні дані до роботи Технічні характеристики складських приміщень

4. Зміст роботи (перелік питань, які потрібно розробити)
1) аналітична частина; 2) проектна частина;
3) спеціальна частина; 4) Безпека життєдіяльності, основи охорони праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Презентація кваліфікаційної роботи 12 аркушів формату А4

АНОТАЦІЯ

В результаті виконання кваліфікаційної роботи було розроблено мобільну системи контролю несанкціонованого доступу до промислових приміщень. Система являє собою електронну пломбу. Захисна система є надійною. Щоб отримати доступ до роботи з пломбою потрібно знати первинні чи зашифровані паролі, які розшифрувати зможе не кожен зловмисник. Пломба є достатньо досконалою, адже вона видає інформацію про точний час її встановлення і відкривання. "Плюсом" даного пристрою є те, що це мобільна система, яку можна встановлювати у будь-якому приміщенні. Після використання на одному об’єкті її легко можна встановити на іншому. Ще один "плюс" є те, що пломба працює на батарейці.

Розроблено структурну схему, алгоритм функціонування мікроконтролерного пристрою і системи загалом, програмно реалізовано програма мовою С++.

ЗМІСТ

ВСТУП

В багатьох мовах поняття «друк» і «пломба» позначені одним і тим же словом. Наприклад, в англійському - словом «seal», а в українській мові поняття «опечатати» і «опломбувати» практично синоніми.

Пломбу можна охарактеризувати як пристрій, який об'єктивно (механічно, без участі людини) здатний надійно засвідчити свою власну цілісність або її відсутність. Якщо укріпити пломбу на опечатуваному об'єкті таким чином, що розтин об'єкту пломбування неминуче спричинить порушення цілісності пломби, пломба починає виконувати функцію сигнального пристрою - індикатора недоторканності або несанкціонованого доступу.

Конструкція пломбувальних пристроїв може бути різною - існують механічні пломбувальні пристрої (ПП): пластикові, стрічкові, дротяні, замкові, болтові і тросові. Є прості і складні оптоволоконні і електронні спеціальні ПП. Пасивні і активні ПП.

На сучасному ринку вже є декілька видів електронних пломб, які є набагато надійнішими ніж механічні захисні пристрої. Проте їх ціна є досить великою. Таким чином, актуальною постає проблема розробки вітчизняної системи контролю несанкціонованого доступу до промислових приміщень.

В кваліфікаційній роботі створена мобільна захисна система.

1 АНАЛІТИЧНА ЧАСТИНА

1.1 Механічні захисні пристрої

Чим так звана «сучасна пломба» відрізняється від стародавніх - типу свинцевою, восковою, глиняною або пластиліновою? Сучасні пломби зобов'язані своєю появою інтенсивним пошукам способів позбавити недобросовісних працівників можливості повторно нанести пломбу з тим же відтисненням на вже розкритий об'єкт. Вдале рішення було знайдене на шляху перетворення пломби в предмет, що існує в єдиному екземплярі, дублікат якого зловмисникові виготовити практично неможливо. Під цим розуміють застосування при виготовленні сучасної пломби складних, недоступних приватній особі промислових технологій і режимів безпеки, що виключають реплікацію пломби, а також привласнення кожному екземпляру виробу індивідуального комплексу ознак, що не повторюється у інших екземплярів. До таких ознак можуть відноситися буквенно-цифровий або цифровий код, штрих-код, електронна плата із занесеною туди інформацією, варіанти виконання, включаючи колір і логотип.

Пломбу можна охарактеризувати як пристрій, який об'єктивно (механічно, без участі людини) здатний надійно засвідчити свою власну цілісність або її відсутність. Якщо укріпити пломбу на опечатуваному об'єкті таким чином, що розтин об'єкту пломбування неминуче спричинить порушення цілісності пломби, пломба починає виконувати функцію сигнального пристрою - індикатора недоторканності або несанкціонованого доступу.

Конструкція пломбувальних пристроїв може бути різною - існують механічні пломбувальні пристрої (ПП): пластикові, стрічкові, дротяні, замкові, болтові і тросові. Є прості і складні оптоволоконні і електронні спеціальні ПП. Пасивні і активні ПП. Всі ці засоби об'єднані загальним

призначенням - служити сигнальним пристроєм, справність якого свідчить про благополуччя захищеного ним об'єкту.

Отже, сенс застосування пломбувальних пристроїв полягає в наступному. По-перше, ПП надають можливість об'єктивно упевнитися в цілісності і недоторканності самого ПП. Якщо розтин опечатаного об'єкту «з чорного ходу», наприклад розтин опечатаного електрощита шляхом зняття його задньої стінки виключено, то цілісність ПП одночасно означає і недоторканність вмісту цього щита. По-друге, виявлення розкритого або пошкодженого ПП говорить про вірогідність прориву системи безпеки. Стан опечатаного об'єкту (щита) і об'єкту захисту (лічильника) потребує перевірки.

Що таке «хороша» пломба і що таке «погана»? Краще питати - надійна вона чи ні як сигнальний пристрій і в якому ступені дана модель підходить для цілей користувача?

Перерахуємо принципові критерії оцінки надійності пломбувального пристрою (ПП):

- чи володіє дане ПП комплексом ознак, що додає кожному екземпляру властивість унікальності?

- чи ефективно ПП як індикатор - конструкція і вживані матеріали повинні виключати можливість розтину із застосуванням механічних, температурних, хімічних і інших методів без залишення характерних слідів (криміналістська стійкість / цінність)?

- наскільки вірогідна можливість реплікації (заводської підробки)?

- чи є в широкому доступі технічні засоби (матеріали і технології) для ефективного маскування ?

Інші критерії оцінки виробу:

- чи достатньо конструкція ПП відповідає об'єкту пломбуванню і вимогам системи безпеки?

- чи відсутній виробничий брак?

- чи прийнятна для споживача ціна?

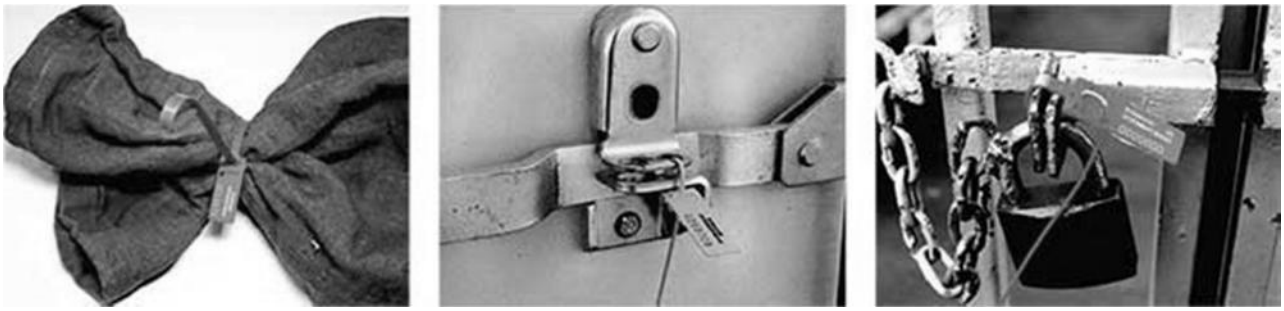


Рисунок 1.1 – Механічні пломбувальні пристрої

Степінь стійкості пломб проти розтину або «Нерозкривання» пломби - зарубіжні експерти одностайні в оцінці стійкості пломбувальних пристроїв проти розтину, що проводиться із застосуванням найпримітивніших технічних засобів: пломб, здатних чинити серйозний опір розтину, не існує. З цими висновками узгоджується і наявний вітчизняний досвід.

Група оцінки уразливості Лос-Анжельської національної лабораторії США (лабораторія займається засобами забезпечення безпеки ядерних об'єктів) провела дослідження по розтину 120 різних видів широко вживаних пломб. Дослідження показали, що всі 120 пломб можуть бути зламані за допомогою низькотехнологічних інструментів і простих методів, доступних широкій публіці. Середній час розтину однієї пломби досвідченим фахівцем склав 5 хвилин, мінімальне - 3 секунди, максимальне - 2 години.

Ця ж група розробила класифікацію способів розтину пломб, підрозділивши їх на 11 класів:

1. Розтин активної системи пломбування у момент її відмови. Характерне втручання в програмне забезпечення активного пломбувального пристрою під приводом виявлення помилок його роботи.

2. Розтин пломби за допомогою відмички. Відмичка використовується так, щоб пломба розкривалася без помітних при візуальному контролі слідів розтину.

3. Розтин способом розпечатування: роздрукувати (відкрити) пломбу, після чого полагодити (приховати) видимі пошкодження.

4. Розтин, що супроводжується втручанням в дані про пломбу: втручання в дані, що містяться на самій пломбі (такі, як серійний номер), і / або в дані журналу обліку, звітів і пояснень за наслідками огляду.

5. Розтин, що супроводжується втручанням в пристрій зчитування нанесеної на пломбу інформації, дія якого заснована на електронному або оптичному зчитуванні, і використовуване для індикації втручання.

6. Розтин на основі саботажу процедури пломбування. Для зриву процедури пломбування можуть використовуватися як персонал, що бере участь в її проведенні, так і сторонні особи.

7. Розтин «з чорного ходу». Внесення до пломби до її установки дефекту, який може бути використаний надалі. Цей дефект може бути введений на етапі конструювання, в процесі виробництва, перевезення і зберігання, а також безпосередньо перед застосуванням.

8. Розтин з реплікацією (виготовленням копії). Використання заводу-виробника для виготовлення дубліката пломби. Забезпечується будь-якими доступними засобами, включаючи злом і несанкціоноване проникнення, методи проведення таємних операцій, підкуп, шантаж, насильство та інші подібного роду методи.

9. Розтин з використанням підробки. Дублікат пломби виготовляється поза заводом-виробником, можливо, з використанням нових пломб або деталей використаних пломб.

10. Розтин з дією на електроніку: втручання в компоненти активних електронних пломб, такі як датчики, мікропроцесор, сигнальні ланцюги, джерела живлення, пристрої подачі сигналу тривоги або настройку параметрів розпізнавання режиму тривоги.

11. Альтернативні способи розтину - всі інші методи, вага кожного з яких в загальній статистичній картині невеликий.

При цьому у багатьох випадках зазвичай вживані візуальні процедури перевірки цілісності свідомо порушених пломб (на погляд, без обмацування руками) були неефективні - не дозволяли встановити факт розтину.

З сказаного відносно стійкості (точніше, відсутність стійкості) пломб витікає, що покладатися на пломбу як на технічний засіб, що серйозно перешкоджає проникненню до об'єкту, що охороняється, щонайменше, необачно.

Рисунок 1.2 – Застосуваннння механічних пломб

Випробування пломб:

Для того, щоб зробити обгрунтований вибір на користь того або іншого виробу, користувач може провести попередні випробування різних моделей. Не можна обійти увагою, що повсюдно і широко поширено нерозуміння істоти випробувань пломб. Оцінка уразливості (стійкості проти спроб розтину) помітно відрізняється від інших типів випробувань, таких як випробування придатності до даного виду застосування, випробування простоти застосування, випробування придатності в польових умовах, міцності і стійкості до дії навколишнього середовища. Багато користувачів пломб змішують всі типи випробувань в одну загальну групу і знаходять необгрунтовану упевненість у використовуваній ними пломбі, якщо вона пройде один або інший тип випробувань.

Надійність виробника:

Оцінюючи, наскільки надійна конкретна пломба, необхідно приймати до уваги відсутність у зловмисника реальної можливості реплікації з використанням виробника для виготовлення дубліката пломби. У цьому і полягає принципова різниця між виробами провідних світових виробників, репутація яких підтримується вже багато десяток років, на підприємствах яких підтримується ефективний режим обліку продукції і безпеки, що виключає можливість отримання дубліката, з одного боку, і за зовнішнім виглядом малого чим виробами численних виробників «другої і третьої черги», що відрізняються, а також виробами численних «копіювальників-реплікаторів», на підприємствах яких з упевненістю виключити можливість подібного інциденту часто не можна. Протокол застосування пломби повинен містити процедуру моніторингу стану пломб і опломбованих об'єктів. Процедура може передбачати, що моніторинг пломб виконується кожні три години двома співробітниками охорони. Перевірка припускає візуальний огляд справності об'єкту пломбування і ретельний візуальний і дотиковий контроль стану ПП на предмет виявлення ознак спроби відкриття . Процедура повинна передбачати перелік типових ознак розтину ПП, а також тих дій (прийомів), за допомогою яких ці ознаки або їх відсутність встановлюються в процесі моніторингу.

Рисунок 1.3–Приклад найпростіших пломбувальних пристроїв

Далі будуть наведені вже відомі на сучасному ринку механічні пломби, їх характеристика, опис, особливості та ціна:

БЕГСИЛ індикаторна пластикова пломба - 5,50 грн./1шт.

Опис:

Пломба зручна пломба з надійним металевим замком. Виключена підробка і повторне використання пломби. Кожна пломба має свій індивідуальний номер.

Застосування:

Різні мішки, контейнери, автотранспорт, складські приміщення і ін.

Технічні характеристики:

- розміри:

  загальна довжина - 368мм і 457мм;

  ширина стрічок - 5,6мм.

  - матеріал - нейлон/поліпропілен, замокнув – сталь;
  - маркування - семизначний цифровий номер (можливе нанесення логотипу);
  - кольори: білий, жовтий, синій, червоний, зелений;
  - встановлюється вручну - шляхом затягування;
  - зняття - за допомогою ножиць.

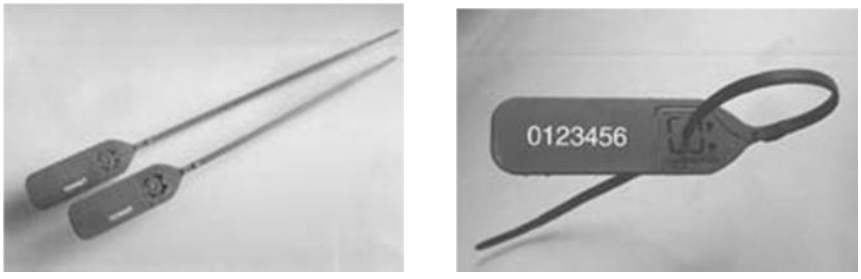


Рисунок 1.4 – БЕГСИЛ- індикаторна пластикова пломба

КРАБСИЛ - індикаторна металева пломба 1,50 грн./1шт.

Опис:

Пломба - зручна пломба для оперативного опломбування. Конструкція є кліпсою, яка защипується на дріт. Використовується із

застосуванням дроту, кінці якого затискаються в корпусі. Не схильна до корозії. Виключена підробка і повторне використання пломби. Кожна пломба має свій індивідуальний номер.

Застосування:

- різні лічильники;
- різні місткості;
- бензоколонки;
- вимірювальні прилади;
- грошові сховища в банках;
- різні контейнери, сейфи , складські приміщення і ін.

Технічні характеристики:

- розміри: 20мм х 14мм х 5,5мм;
- довжина дроту - будь-яка;
- матеріал-алюміній;
- маркування - шестизначний цифровий номер;
- встановлюється - вручну шляхом замикання;
- зняття - за допомогою кусачків, ножиць.

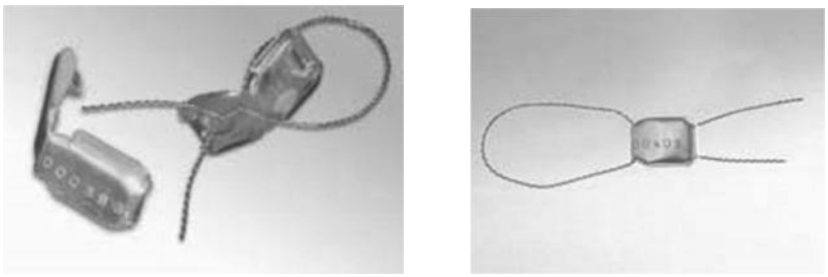


Рисунок 1.5 – КРАБСИЛ- індикаторна металева пломба

1.2 Електронні захисні пристрої

На сучасному ринку вже є декілька видів електронних пломб, які є набагато надійнішими ніж механічні захисні пристрої. Нижче наведено декілька захисних електричних пломб, їх технічні характеристики, опис, особливості та ціна.

CRYPTA 2K - електронна пломба багаторазового використання (економічне, зручне і дуже надійний засіб опломбування) 9300,00 грн./1шт.

Опис:

Електронна пломба CRYPTA 2K є спеціальним пристроєм опломбування, що складається з ударостійкого, литого і вологостійкого корпуси пломби Crypta 2K і спеціального троса, захищеного прозорою пластиковою оболонкою. Корпус пломби має електронне захищене табло, яке інформує про стан пломби.

Процес опломбування полягає в тому, що два кінці троса встановлюються в спеціальних отворах корпусу пломби, фіксуються пластиною і при установці перемикача-фіксатора в закрите положення, на дисплеї пломби висвічується номер, який запам'ятовується до моменту перемикання перемикача-фіксатора у відкрите положення (поворот управо або вліво). Як тільки перемикач-фіксатор встановлюється у відкрите положення, на дисплеї пломби поперемінно з'являються номер і напис OPEN. Коли перемикач -фіксатор установлюється в закрите положення, на дисплеї пломби з'являється абсолютно інший номер. Кожного разу при опломбуванні на дисплеї пломби з'являється непорядковий, хаотичний номер, який неможливо передбачити наперед.

Особливості:

- низька вартість;
- довговічність (термін служби - до 5 років) ;
- неможливість прогнозу номера при опломбуванні;
- надійна захищена конструкція;
- функціонує в будь-яких умовах (дощ, сніг, суха пара, вологих пар, солона вода, пил, грязь і ін.) ;
- проста установка.

Застосування: - електронна пломба Crypta 2K - високонадійний засіб для опломбування автомашин, контейнерів, фургонів, складів і ін.

Процес опломбування:

- поверніть перемикач-фіксатор пломби у відкрите положення;
- закріпите один кінець троса в одному з двох отворів для троса на корпусі пломби за допомогою пластини і стопорного гвинта;
- другий кінець троса проденьте через конструкцію і вставте в другий отвір для троса на корпусі пломби;
- поверніть перемикач-фіксатор в закрите положення - пломба знаходиться в опломбованому стані;
- натиснувши кнопку перегляду, на дисплеї висвітиться номер;
- запишіть номер пломби в документи;
- встановите навісний замок в спеціальні отвори в пломбі.

Для того, щоб перевірити номер, натисніть на кнопку проглядання (на корпусі пломби).

Технічні характеристики:

- стійкість корпусу пломби до сильної вібрації;
- корпус пломби вологонепроникний;
- висока ударостійкість корпусу пломби;
- температура застосування пломби: від -40 градусів до +70 градусів;
- габаритні розміри пломби: 101мм х 156мм х 41мм.

У комплект входять: електронна пломба Crypta 2K, трос, захищений прозорою пластиковою оболонкою (довжина троса виконується за бажанням замовника), спеціальна настановна гумова пластина, верхній кожух, кріплення.

Рисунок 1.6 - CRYPTA 2K

ЕЛЕКТРОННА ПЛОМБА CRYPTA DATA багаторазового використання (економічне, зручне і дуже надійний засіб опломбування) 13200,00 грн./1шт.

Опис:

Електронна пломба CRYPTA DATA є спеціальним пристроєм опломбування, що складається з ударостійкого, литого і вологостійкого корпусу пломби CRYPTA DATA і спеціального троса, захищеного прозорою пластиковою оболонкою. Корпус пломби має електронне захищене табло, яке інформує про стан пломби. Процес опломбування пломбою CRYPTA DATA полягає в тому, що один кінець троса протягується і кріпиться в спеціальному правому або лівому отворі; інший кінець троса фіксується в спеціальному отворі під перемикачем-фіксатором в корпусі пломби. При установці перемикача-фіксатора в закрите положення, на дисплеї пломби висвічується номер, який запам'ятовується до моменту перемикання перемикача-фіксатора у відкрите положення. Разом з номером запам'ятовується дата і час закриття пломби. Як тільки перемикач-фіксатор встановлюється у відкрите положення, на дисплеї поперемінно з'являються напис OPEN, номер, дата, час закриття і відкриття пломби. Коли перемикач -фіксатор

встановлюється в закрите положення, на дисплеї пломби з'являється абсолютно інший номер. Кожного разу при опломбуванні на дисплеї пломби з'являється непорядковий, хаотичний номер, який неможливо передбачити наперед. Оскільки ця пломби має пам'ять, є можливість у будь-який час проглянути номери, дату і час закриття і відкриття останніх 50 процесів опломбування.

Особливості:

- Низька вартість (використання даної пломби значно знижує витрати на опломбування);
- довговічність - пломба багаторазового використання (термін служби - до 6 років);
- неможливість прогнозу номера при опломбуванні;
- фіксує і запам'ятовує дату і час закриття і відкриття пломби;
- запам'ятовує номер, дату, час закриття і відкриття пломби (у пам'яті пломби постійно знаходяться дані про 50 останніх процесів закриття-відкриття пломби);
- функціонує в будь-яких умовах (дощ, сніг, суха пара, волога пара, солона вода, пилюка);
- надійна захищена конструкція пломби. Застосування - електронна пломба Crypta Data - високонадійний засіб для опломбування автомашин, контейнерів, фургонів, складів і ін.

Перегляд даних з пам'яті:

- натисніть кнопку перегляду, на дисплеї висвітиться або OPEN (якщо пломба відкрита) або поточний номер (якщо пломба закрита), потім відразу натисніть кнопку вибору, на дисплеї висвітиться рахунок процесів опломбування;
- поперемінним натисненням виберете потрібний процес опломбування (01,02.) (для проглядання часу і дати закриття і відкриття пломби потрібного вам процесу або номера, натискайте кнопку перегляду).

Технічні характеристики:

- стійкість до сильної вібрації;
- корпус вологонепроникний;
- висока ударостійкість;
- температура застосування: від -40 градусів до +70 градусів.

Рисунок 1.7 - CRYPTA DATA

1.3 Постановка задач проектування

Огляд існуючих способів захисту промислових обєктів та складських приміщень показує, що на сучасному ринку товарів є вже досить багато аналогів. Проте, ми можемо бачити , що механічні пломби не є достатньо надійними. Їх можна використовувати лише у тих випадках, коли на промисловому об’єкті є інші захисні пристрої. Щодо електронних пломб, то проблемою є їх ціна. Вище зазначено, що найнижча ціна такого пристрою складає близько 9 тисяч гривень.

Задача роботи полягає в наступному:

- розробити алгоритм та програму функціонування мобільної системи контролю доступу;
- розробити діаграми станів роботи пристрою захисту та алгоритму його роботи;
- спроектувати мікроконтролерний пристрій захисту (Принципову схему, друковану плату) ;
- спроектувати програмну частину МК-пристрою мовою С;

- розробити управляючу програми для встановлення системи захисту;

- розробити алгоритм роботи пломби (блок- схема) ;

- реалізувати програму мовою С++;

- створити приклад пломбувального пристрою, який буде мати нижчу і доступнішу ціну, буде більш безпечним, а робота якого буде довготривалою та надійною.

2. ПРОЕКТНА ЧАСТИНА

2.1 Огляд можливих способів несанкціонованого доступу та розробка алгоритму їх запобігання

Всі пристрої захисту об'єднані загальним призначенням - служити сигнальним пристроєм, справність якого свідчить про благополуччя захищеного ним об'єкту.

Які є можливі способи розкриття або пошкодження пломби?

Відносно обставин пошкодження:

- навмисна атака;
- випадкове пошкодження;
- інцидент відбувся за участю власного персоналу;
- власний персонал до інциденту не причетний.

Відносно об'єкту атаки:

- спроба атаки на пломбу - може бути успішною або не успішною;
- спроба атаки опломбованого об'єкту - може бути успішною або не успішною;
- спроба атаки об'єкту охорони - може бути успішною або не успішною.

Відносно мети атаки:

- з хуліганських міркувань;
- без наміру атакувати, випадково;
- з метою діставання доступу до об'єкту охорони;
- з метою відвернення уваги;
- з іншими різноманітними цілями.

Цілісна пломба завжди означає одне: нічого з цього переліку не мало місця, іншими словами - пломба, об'єкт пломбування, об'єкт

охорони атаці не піддавалися. Тобто справна пломба - це завжди індикатор недоторканності.

Алгоритм запобігання несанкціонованого доступу полягає в наявності на підприємстві цілого комплексу заходів і засобів захисту.

Так нормальна господарська (і інша) діяльність постійно піддається різноманітним ризикам. Наприклад, існує ризик, що відключиться електропостачання, ризик пограбування, ризик арифметичної помилки, ризики втрати або розкомплектація документів в процесі їх обороту.

Під системою заходів безпеки ми розуміємо комплекс сил, засобів і процедур, направлений на протидію ризикам, загрозливим нормальному перебігу бажаного процесу. Наприклад, для організації ефективної охорони контейнерного майданчика може бути розроблена система, об'єднуюча охорону і порядок її дій, технічні засоби, такі як охоронна сигналізація зовнішнього периметра майданчика, засоби освітлення і відеоспостереження, а також засоби пломбування прийнятих на зберігання контейнерів і порядок їх застосування і контролю.

Зарубіжні дослідження свідчать, що вірогідність ризику розтину пломби і маскування слідів тим менше, чим більше зусиль користувач вклав в розробку протоколу застосування пломб і процедур, що гарантують його дотримання.

Протокол є комплекс окремих процедур, інакше кажучи - інструкцій, в якому саме порядку виконується те або інше передбачене протоколом завдання. Так, протокол повинен містити ретельно розроблені процедури і / або графіки:

- прийому, обліку, зберігання і видачі пломб персоналу;
- контролю якості і проведення випробувань пломби до її установки;
- попередньої перевірки технічної справності об'єкту установки пломби;
- виконання установки пломби;

- обліку встановлених пломб і пломбованих об'єктів;

- перевірки (інспекції) встановлених пломб і опломбованих об'єктів;

- ведення записів про всі перевірки технічної справності пломб і пломбованих об'єктів;

- навчання і контролю дій персоналу;

- санкціонованого розтину пломб;

- знищення розкритих пломб;

- резервних варіантів дій на випадок неможливості виконання штатних процедур;

- порядку дій у разі виявлення несанкціонованого розтину пломби.

Наприклад, протокол застосування пломби повинен містити процедуру моніторингу стану пломб і опломбованих об'єктів. Процедура може передбачати, що моніторинг пломб виконується кожні три години двома співробітниками охорони. Перевірка припускає візуальний огляд справності об'єкту пломбування і ретельний візуальний і дотиковий контроль стану ПП на предмет виявлення ознак спроби відкриття . Процедура повинна передбачати перелік типових ознак розтину ПП, а також тих дій (прийомів), за допомогою яких ці ознаки або їх відсутність встановлюються в процесі моніторингу. Процедура повинна передбачати порядок відмітки результатів моніторингу, а також порядок дій на випадок виявлення ознак атаки.

Підготовка установників і виконуючих моніторинг інспекторів:

Особливу увагу доцільно приділити ефективній підготовці установників пломб і інспекторів, які виконують процедури перевірки (інспекції) встановлених пломб і опломбованих об'єктів. Ефективність протидії спробам злому припускає розуміння інспекторами конкретних слабких місць виробів і ознайомлення з найбільш вірогідними сценаріями злому.

Проте зазвичай інструкція, яку отримує інспектор, звучать так: «Подивіться, чи немає слідів втручання»! Інформація про те, за чим взагалі потрібно стежити, нерідко відсутня. Інспекторам слід показувати приклади атакованих пломб. Ще краще, якщо їм показуватимуть, як можна атакувати конкретно вживані ними пломби , оскільки цей метод навчання дає пряму і найбільш корисну інформацію.

Отже, система заходів безпеки - це комплекс сил, засобів і процедур, направлений на протидію ризикам, загрозливим нормальному перебігу бажаного процесу. Кожна складова частинка несе в собі відповідальність за безпеку всього промислового об’єкту. Важливу роль тут відіграють і засоби пломбування, і засоби освітлення і відеоспостереження, і кваліфікація та старанність виконання своїх обов’язків відповідального за безпеку персоналу.

2.2 Розробка діаграм станів роботи пристрою захисту та алгоритму його роботи

Робота мікроконтролерного пристрою електронної пломби показує, що пристрій захисту може перебувати у трьох станах:

- BLANK – “чистий”
- STARTED – “запуск”
- OPENED-“відкритий”.

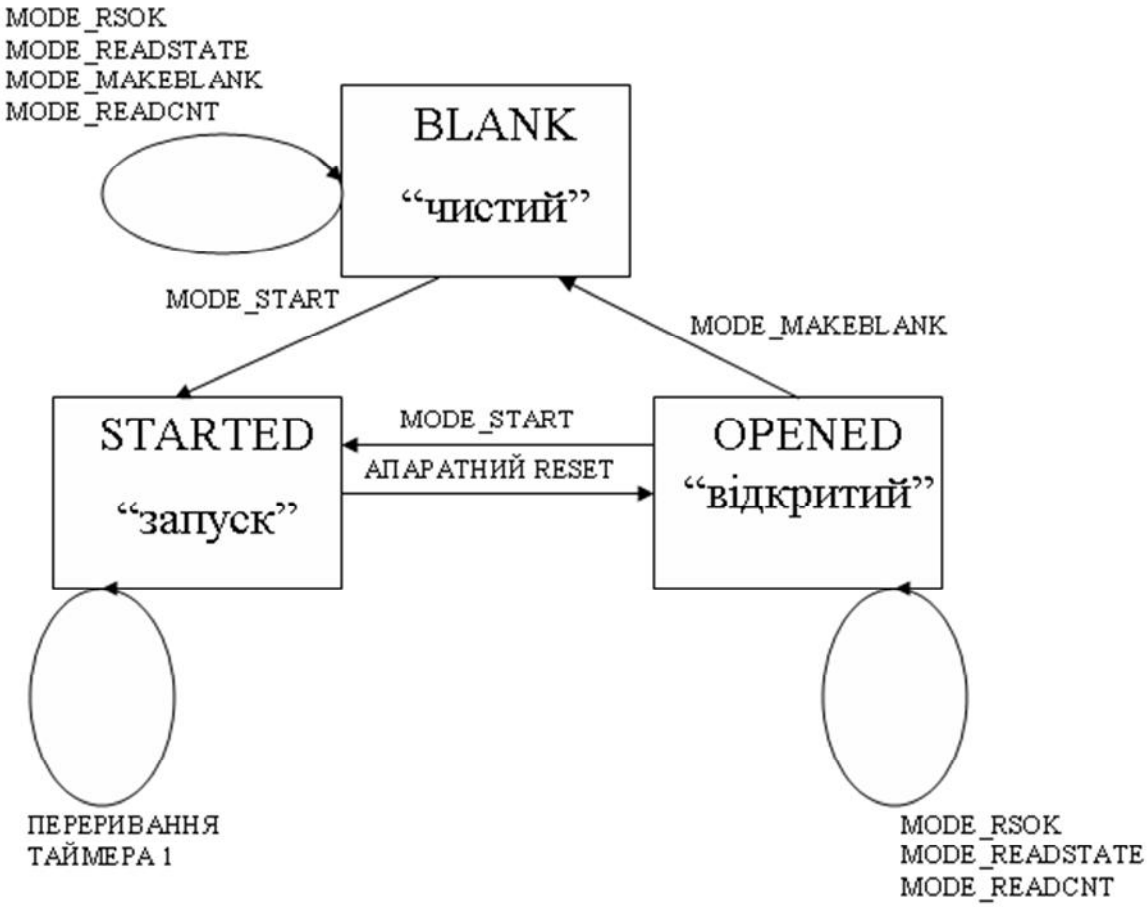


Рисунок 2.1 - Діаграма станів роботи пристрою захисту

Мікроконтролерний пристрій може перебувати у першому стані - BLANK – “чистий” у випадку, коли виконуються функції MODE_RSOK або MODE_READSTATE або MODE_READCNT або MODE_MAKEBLANK. У цьому стані пристрій не запущений і не відкривався, тут є лише інформація про пломбу: серійний номер, заводські характеристики, частота кварцового генератора, тощо.

Зі стану №1 в стан №2 можна перейти лише через команду MODE_START .

Другий стан - STARTED – “запуск”- пломба запущена. Якщо вона встановлена , записується стартовий час в хвилинах, серійний № пломби, видається підтвердження до ЕОМ про її встановлення. Цей стан зациклюється при перериванні таймера 1.

З стану № 2 в стан № 3 можна перейти через виконання апаратного RESETу.

Стан № 3 OPENED-“відкритий” –це стан зчитування інформації про час відкриття пломби. Тут надається № пломби, час її встановлення , і якщо вона була “відкрита”, то час відкриття. Стан OPENED має зв’язки з усіма іншими станами. Залишатися в цьому стані пристрій буде, коли виконуються команди MODE_RSOK або MODE_READSTATE або MODE_READCNT. Перейти в стан STARTED можна через виконання команди MODE_START , а в стан BLANK - через команду MODE_MAKEBLANK.

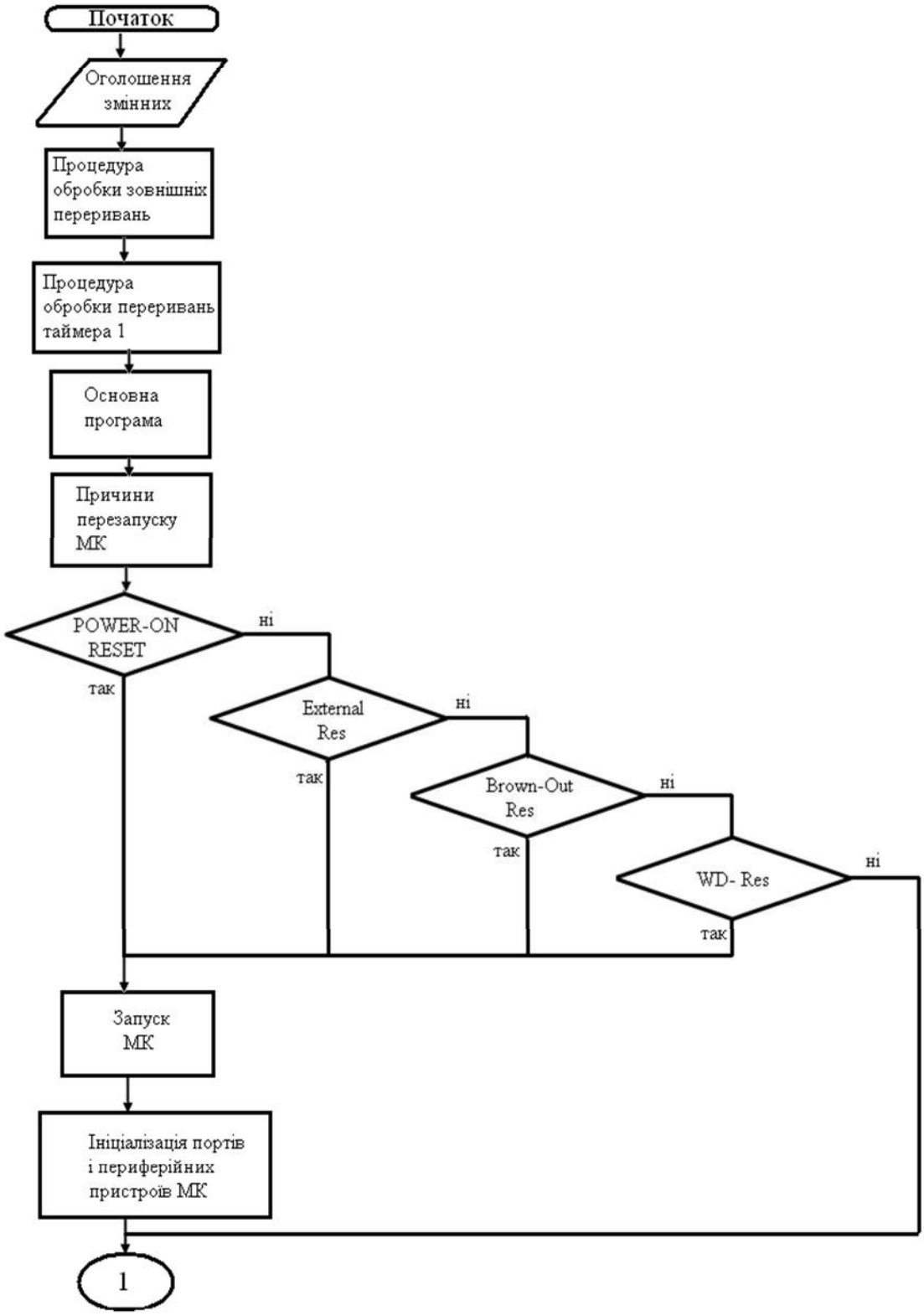
2.3 Проектування програмної частини МК-пристрою мовою С++

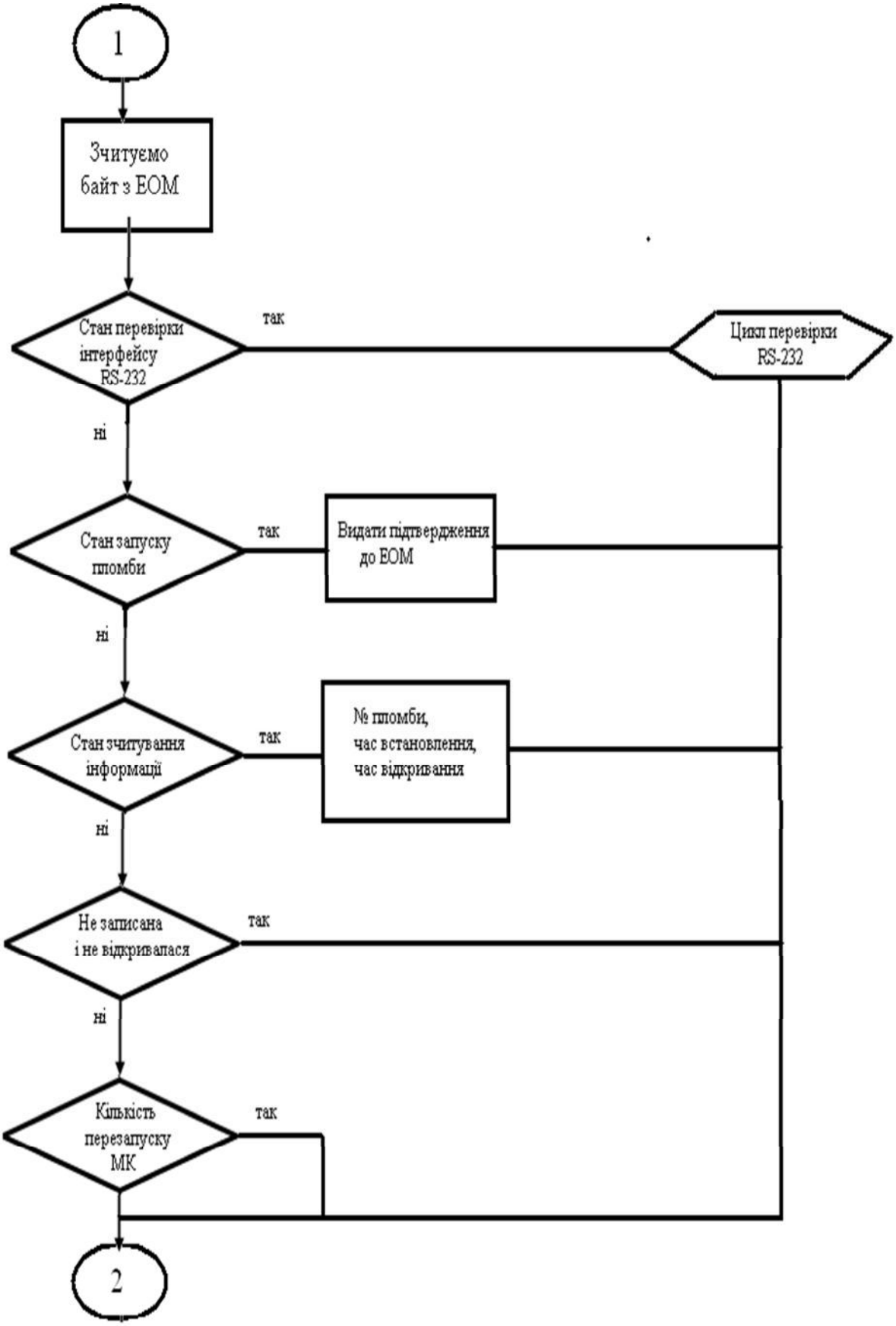
Далі буде показано алгоритм (блок- схема) функціонування МК-пристрою електронної пломби представлена на рис.2.2.

Програмна частина МК-пристрою реалізована мовою С++.

Процес роботи з програмою спочатку вимагає задання початкової інформації про мікроконтролер: встановлення його типу, загальні характеристики та робочу частоту кварцового генератора.

```
This program was produced by the
CodeWizardAVR V1.25.5 Professional
Automatic Program Generator
© Copyright 1998-2007 Pavel Haiduc, HP InfoTech s.r.l.
http://www.hpinfotech.com
Project :
Version :
Date    : 05.03.2023
Author  : F4CG
Company : F4CG
Comments:
  Chip type           : ATtiny2313
Clock frequency     : 0,375 MHz
Memory model        : Tiny
External SRAM size  : 0
Data Stack size     : 64
```


Початок
Оголошення змінних
Процедура обробки зовнішніх переривань
Процедура обробки переривань таймера 1
Основна програма
Причини перезапуску МК
POWER-ON RESET
ні
так
External Res
ні
так
Brown-Out Res
ні
так
WD- Res
ні
так
Запуск МК
Ініціалізація портів і периферійних пристроїв МК
1


1
Зчитуємо байт з ЕОМ
Стан перевірки інтерфейсу RS-232
так
Цикл перевірки RS-232
ні
Стан запуску пломби
так
Видати підтвердження до ЕОМ
ні
Стан зчитування інформації
так
№ пломби, час встановлення, час відкривання
ні
Не записана і не відкривалася
так
ні
Кількість перезапуску МК
так
2

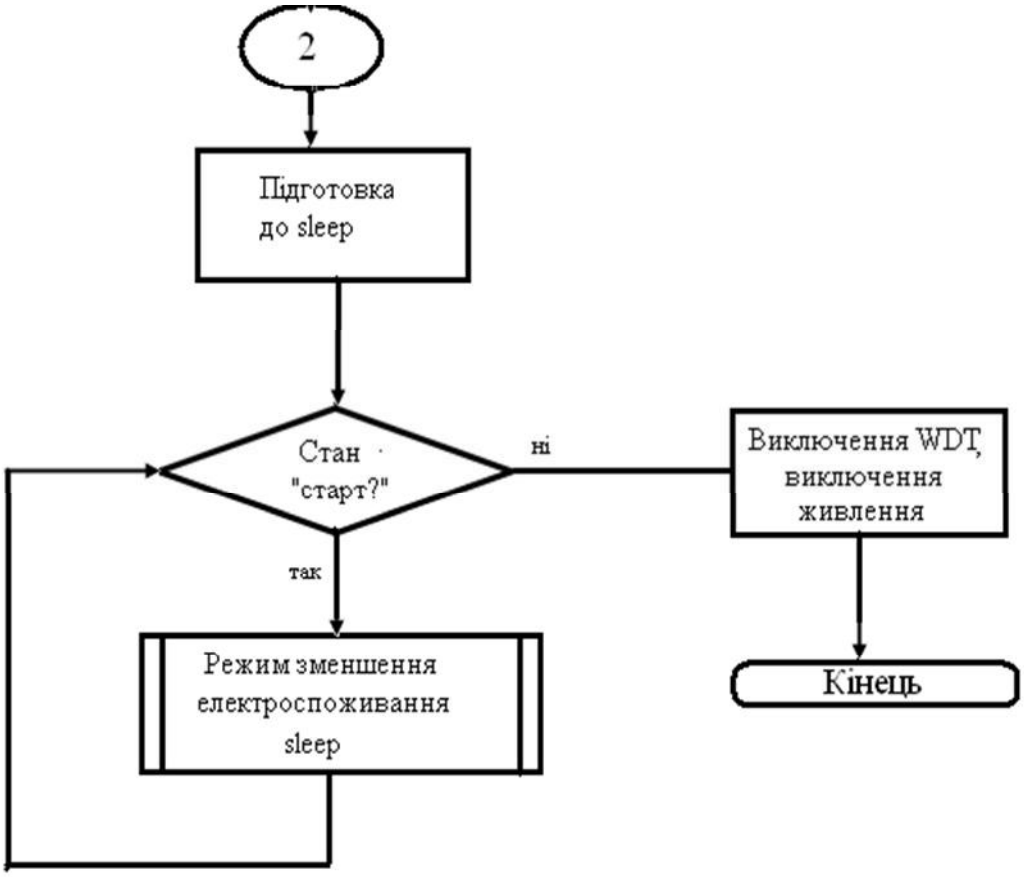


Рисунок 2.2 - Алгоритм функціонування МК- пристрою

Оголошення основних змінних, змінних, які зберігаються в EEPROM, а також зберігаються при втраті живлення.

```
#include <tiny2313.h>
#include <sleep.h>
// Standard Input/Output functions
#include <stdio.h>
 #define STATE_BLANK 0x31
#define STATE_STARTED 0x37
#define STATE_OPENED 0x39
#define MODE_RSOK       0x5a  //01011010
#define MODE_START      0x69  //01101001    // sends state
#define MODE_READSTATE   0x26   //00100110      // state, number, start time, open time
#define MODE_MAKEBLANK  0x4d  //01001101    // sends state
#define MODE_READCNT   0xd6  //11010110
unsigned int i;
unsigned long int min;
char tick=0,mode,waiting_command;
```

```
eeprom unsigned long FSmin=0; // Time of start device
eeprom unsigned long FXmin=0; // Time when device open
eeprom unsigned long FTmin=0; // Temporary time in EEPROM
eeprom unsigned int  number=0;
eeprom unsigned char state=STATE_BLANK;
eeprom unsigned int  WDT_reset_cnt=0;
eeprom unsigned int  PWR_reset_cnt=0;
```

Запис константи в пам'яті програми:

```
flash char RS_OK[9]="RS232 OK";
```

Програма виключення WD- таймера

```
void WDT_off(void)
{
   #asm("cli")
   #asm("wdr")
/* Clear WDRF in MCUSR */
MCUSR &= 0b11110111;    //~(1<<WDRF);
/* Write logical one to WDCE and WDE */
/* Keep old prescaler setting to prevent unintentional time-out*/
WDTCR |= 0b00011000;   //(1<<WDCE) | (1<<WDE);
/* Turn off WDT */
WDTCR = 0x00;
   #asm("sei")
}
```

Процедура обробки зовнішніх переривань реалізовується наступним чином:

```
// External Interrupt 0 service routine
interrupt [EXT_INT0] void ext_int0_isr(void)
{
   #asm("wdr")
   #asm("cli")
   FXmin=min;
   state=STATE_OPENED;

   WDT_off();
   powerdown();
}
```

Процедура обробки переривань таймера 1:

```
// Timer 1 overflow interrupt service routine
interrupt [TIM1_OVF] void timer1_ovf_isr(void)
{
// Reinitialize Timer 1 value
```

```
   TCNT1H=0x8D;
   TCNT1L=0x91;
   #asm("wdr")
   #asm("cli")
   if(++tick>=12){tick=0; min++;}
   if((*((char*)&min) & 0b0011111)==0 && (tick==1))
   {
      FTmin=min;
   }
   #asm("sei")
}
```

Основний цикл програми, тут встановлюється робоча частота

Crystal Oscillator division factor: 16

та визначається причина перезапуску МК

```
void main(void)
{#pragma optsize-
CLKPR=0x80;
CLKPR=0x04;
#ifdef _OPTIMIZE_SIZE_
#pragma optsize+
#endif
// Reset Source checking
if (MCUSR & 1)
   {
   // Power-on Reset
    MCUSR=0;
    i=PWR_reset_cnt; i++; PWR_reset_cnt=i;
   }
else if (MCUSR & 2)
   {
   // External Reset
    MCUSR=0;
    waiting_command=1;
}
else if (MCUSR & 4)

{
   // Brown-Out Reset (disabled)
    MCUSR=0;
   }
else
   {
   // Watchdog Reset
```

```
   MCUSR=0;
```
Тут визначається кількість збоїв МК
```
   i=WDT_reset_cnt; i++; WDT_reset_cnt=i;
  }
```
Далі йде ініціалізація портів
```
if(state==STATE_STARTED) min=FTmin;      // restore after reset

// Input/Output Ports initialization
// Port A initialization
// Func2=In Func1=In Func0=In
// State2=T State1=T State0=T
PORTA=0x00;
DDRA=0x00;

// Port B initialization
// Func7=Out Func6=In Func5=In Func4=In Func3=In Func2=In Func1=In Func0=In
// State7=0 State6=T State5=T State4=T State3=T State2=T State1=T State0=T
PORTB=0x00;
DDRB=0x80;

// Port D initialization
// Func6=In Func5=In Func4=In Func3=In Func2=In Func1=In Func0=In
// State6=T State5=T State4=T State3=T State2=T State1=T State0=T
PORTD=0x00;
DDRD=0x00;
```
Та ініціалізація периферійних пристроїв МК:
```
Даний блок не використовується

// Timer/Counter 0 initialization
// Clock source: System Clock
// Clock value: Timer 0 Stopped
// Mode: Normal top=FFh
// OC0A output: Disconnected
// OC0B output: Disconnected
TCCR0A=0x00;
TCCR0B=0x00;
TCNT0=0x00;
OCR0A=0x00;
OCR0B=0x00;
```
Переривання при переповненні

```
// Timer/Counter 1 initialization
// Clock source: System Clock
// Clock value: 5,859 kHz
// Mode: Normal top=FFFFh
// OC1A output: Discon.
// OC1B output: Discon.
// Noise Canceler: Off
// Input Capture on Falling Edge
// Timer 1 Overflow Interrupt: On
// Input Capture Interrupt: Off
// Compare A Match Interrupt: Off
// Compare B Match Interrupt: Off
TCCR1A=0x00;
TCCR1B=0x03;
TCNT1H=0x8D;
TCNT1L=0x91;
ICR1H=0x00;
ICR1L=0x00;
OCR1AH=0x00;
OCR1AL=0x00;
OCR1BH=0x00;
OCR1BL=0x00;
```

Ініціалізація послідовного порта:

```
// USART initialization
// Communication Parameters: 8 Data, 1 Stop, No Parity
// USART Receiver: On
// USART Transmitter: On
// USART Mode: Asynchronous
// USART Baud Rate: 1200 (Double Speed Mode)
UCSRA=0x02;
UCSRB=0x18;
UCSRC=0x06;
UBRRH=0x00;
UBRRL=0x26;
```

Далі зчитується 1 байт інформації з ЕОМ

```
if(waiting_command)     // after external reset
{
   mode=getchar();
   #asm("wdr")
   switch(mode)
```

Перевірка стану інтерфейсу RS- 232

```
{
```

```
   case MODE_RSOK:
   {   for(i=0;i<9;i++) putchar(RS_OK[i]);
      break;
   }
```

Далі МК переходить до стану запуску пломби

```
case  MODE_START:
```

Записується стартовий час в хвилинах, якщо пломба встановлена

```
{
      *((char eeprom*)&FSmin)=getchar(); // write start date in min
      *((char eeprom*)&FSmin+1)=getchar();
      *((char eeprom*)&FSmin+2)=getchar();
      *((char eeprom*)&FSmin+3)  =getchar();
```

Серійний № пломби

```
*((char eeprom*)&number)=getchar(); // write serial number of label
      *((char eeprom*)&number+1)=getchar();
      #asm("wdr")
```

Видається підтвердження до ЕОМ про встановлення пломби

```
 state=STATE_STARTED;
       putchar(STATE_STARTED);
```

Тут МК переходить в стан зчитування інформації про час відкривання пломби:

```
case MODE_READSTATE:
   {
      putchar(state);
```

Серійний № пломби

```
if(state!=STATE_BLANK)
      {
         putchar(*((char eeprom*)&number));
         putchar(*((char eeprom*)&number+1));
```

Час встановлення пломби:

```
putchar(*((char eeprom*)&FSmin));
         putchar(*((char eeprom*)&FSmin+1));
         putchar(*((char eeprom*)&FSmin+2));
         putchar(*((char eeprom*)&FSmin+3));
```

Тут записується час відкривання, якщо пломба була відкрита:

```
#asm("wdr")
         if(state==STATE_OPENED)
```

```
            putchar(*((char eeprom*)&FXmin));
            putchar(*((char eeprom*)&FXmin+1));
            putchar(*((char eeprom*)&FXmin+2));
            putchar(*((char eeprom*)&FXmin+3));
        }    break;// read day hour min to computer
    }
```

МК в стані коли пломба не запущена і не відкривалася

```
case MODE_MAKEBLANK:
    {
        state=STATE_BLANK;
        putchar(STATE_BLANK);
    }
```

Стан зчитування кількості перезапуску МК по WD- таймера і по втраті живлення

```
case MODE_READCNT:
    {
        putchar(*((char eeprom*)&WDT_reset_cnt));
        putchar(*((char eeprom*)&WDT_reset_cnt+1));

        putchar(*((char eeprom*)&PWR_reset_cnt));
        putchar(*((char eeprom*)&PWR_reset_cnt+1));
        #asm("wdr")
        putchar(*((char *)&min));
        putchar(*((char *)&min+1));
        putchar(*((char *)&min+2));
        putchar(*((char *)&min+3));
        putchar(tick);
        break;
    }
    }// switch
}
```

Стан «sleep» - режим зменшення електроспоживання

```
//if
sleep_enable();
if(state!=STATE_STARTED)
{
```

МК виключається повністю до наступного RESETу

```
  WDT_off();
```

Вихід з power down по таймеру 1

```
    powerdown();
```

```
}
while (1)
```

Зменшення енергоспоживання і пробуджуваність кожні 5 секунд для відліку часу.

```
{
    idle();
  }}
```

2.4 Проектування мікроконтролерного пристрою захисту

Принципові електричні схеми призначені для відображення принципу дії системи і відображають взаємні зв’язки окремих приладів, засобів автоматизації і допоміжної апартури, які входять в склад функціональних вузлів систем автоматизації з врахуванням послідовності їх роботи і принципу дії. Вони є основою для розробки інших документів пректу: зовнішнього вигляду приладу, таблиць з’єднань приладу і ЕОМ, схем зовнішніх з’єднань, схем підключень і інших, а також служать для вивчення принципу дії систем автоматизації і необхідні при проведенні налагодження робіт і в експлуатації.

Принципові схеми складаються на основі схем автоматизації, виходячи із заданих алгоритмів функціонування окремих вузлів контролю, сигналізації, управління і загальних технологічних вимог, які висуваються до проектованого приладу.

Ці схеми повинні забезпечувати:

– високу надійність;

– простоту і економічність;

– зручність експлуатації і роботи;

– чіткість дій;

Найпоширенішими є принципові електричні схеми сигналізації і управління з елементами захисту і блокування.

В даному проекті розроблено 2 схеми електричні принципові: схема електронної пломби та узгоджуючого пристрою «пломба/ЕОМ» (програматор).

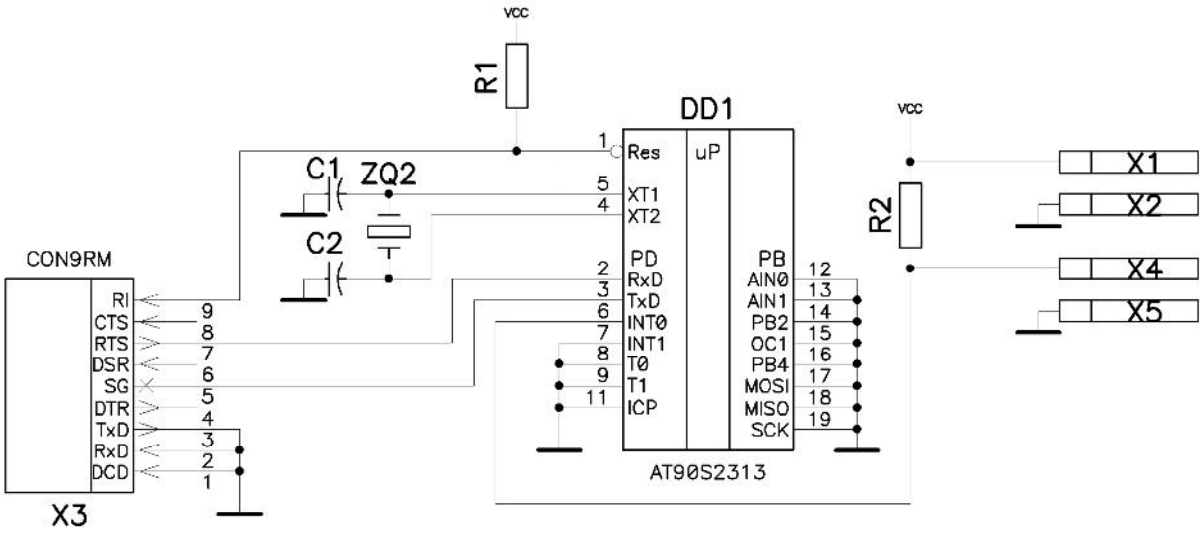


Рисунок 2.2 - Електронна пломба. Схема електрична принципова

Плата друкована наведена на кресленні ДП. АУ-05.00.00.001. Друкована плата розведена у системі (САПР) P-CAD. Проект у системі автоматичного проектування (САПР) P-CAD представляється у двох видах: у виді електричної принципової схеми й у виді друкованої плати. Для цього у САПР P-CAD є два графічних редактори:

1) схемний редактор (Schematic), який забезпечує створення принципової схеми;

2) технологічний редактор (PCB), призначений для редагування топології друкованої плати.

Основою проекту є бібліотека радіоелементів, яка створюється за допомогою наступних утиліт:

1) символьного редактора (Symbol Editor), призначеного для створення символьного (умовного позначення) елемента для електричної принципової схеми;

2) технологічного редактора (Pattern Editor), який застосовується при створенні технологічного елемента (“посадочного місця” або корпуса радіоелемента) для його встановлення на друковану плату;

3) диспетчера бібліотек (Library Executive), призначеного для створення взаємозв’язку між символьним елементом принципової схеми та технологічним елементом.

До основних етапів проектування друкованої плати можна віднести:

1. Створення бібліотечних елементів, необхідних для проектування принципової електричної схеми й друкованої плати.

2. Створення принципової схеми. Даний етап необхідний для створення документа “схема електрична принципова”, а також для опису радіоелементів, що входять у проект, і задання електричних зв’язків між ними.

3. Перехід до технологічного образу проекту. При цьому схемні бібліотечні елементи автоматично замінюються на технологічні.

4. Розміщення радіоелементів на друкованій платі. Даний етап виконується в автоматичному або в напівавтоматичному режимах. На заготовці друкованої плати, яка містить її контури й області заборони для розміщення, встановлюються радіоелементи, а якість розміщення оцінюється за інтегральним критерієм, який враховує загальну довжину електричних зв’язків та щільність електричних зв’язків на друкованій платі.

5. Створення топології друкованих провідників плати. Виконується шляхом автоматичного трасування з’єднань або інтерактивної (напівавтоматичної) прокладки трас.

Схеми з'єднань – це комбінована схема, на якій зображуються зовнішні підключення апаратів та електричні зв’язки між приладами і засобами автоматизації. Схеми узгоджуються з кресленнями загального вигляду приладів, а також з планами розміщення ЗА. В загальному випадку схеми зовнішніх проводок повинні вміщувати: місцеві пункти контролю і управління, електричні проводки, основний надпис, таблиця умовних графічних позначень і перелік кабелів, проводок та монтажної арматури.

Основними документами при проектуванні і функціонуванні є: схеми автоматизації технологічними процесами; специфікація на обладнання та технічні засоби автоматизації; принципові електричні та пневматичні схеми.

Схеми підключень виконуються без дотримання масштабу. На практиці використовують два варіанта проектування схем: графічний і табличний. В даному проекті ми використовуємо графічний метод, який є більш розповсюдженим.

Узгоджуючий пристрій «пломба/ЕОМ» (програматор) призначений для узгодження інтерфейсу RS-232 та комунікаційного порта пломби.

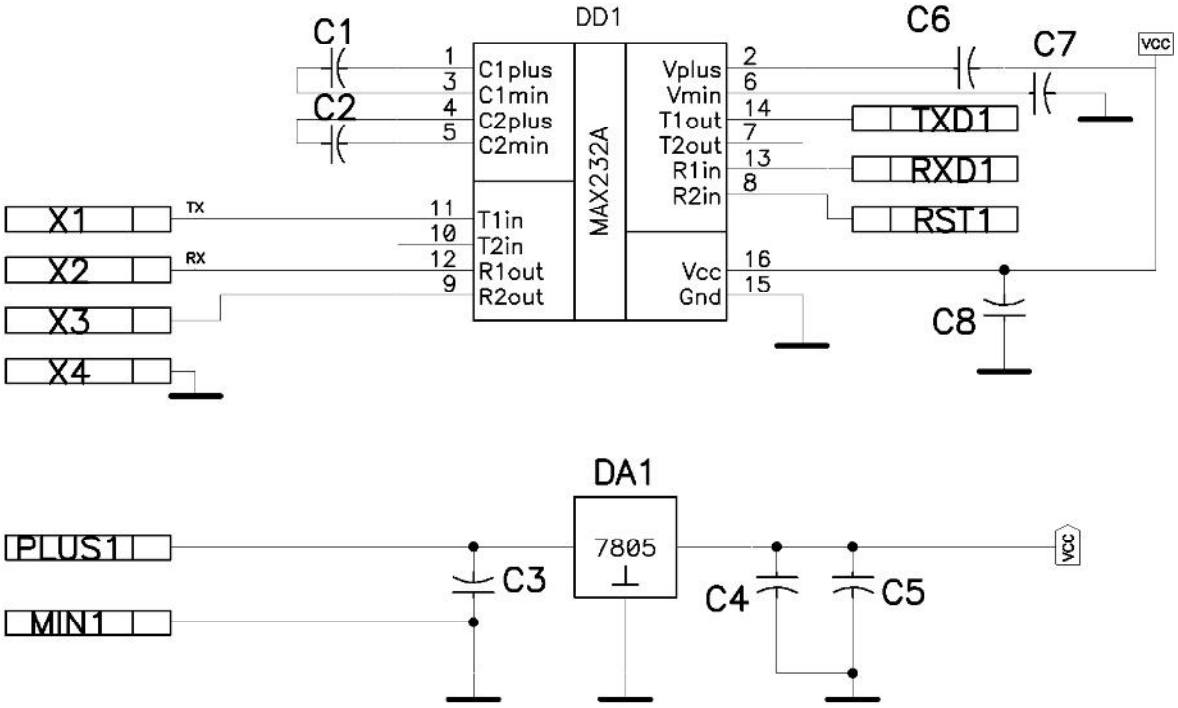


Рисунок 2.3 - Узгоджуючий пристрій «пломба/ЕОМ» (програматор). Схема електрична принципова

3. СПЕЦІАЛЬНА ЧАСТИНА

3.1 Розробка управляючої програми

Управляюча програма для встановлення розробленої системи захисту реалізована мовою програмування С++. З алгоритму роботи системи видно, що вона є досить надійною. При запуску та ініціалізації програми відкривається створений раніше файл з зашифрованими паролями:

fn[]="mem.cit"

Цей файл має наступну структуру:

2000 Байт випадко-вих даних	N1	S1	2000 Байт випадко-вих даних	N2	S2	2000 Байт випадко-вих даних

Рисунок 3.1 – Структура файлу fn[]="mem.cit"

Тут - N1 і N2 – кількість символів у першому та другому зашифрованих паролях.

- S1 і S2 – зашифровані символи паролів
- 6000 байт випадкових символів та чисел роблять файл досить великим і не зрозумілим.

Якщо не знати структури файлу, то процес знаходження зашифрованих паролів є достатньо складним.

Знайдені зашифровані паролі потрібно розшифрувати. Це можна зробити за допомогою відповідно ключа 1 і ключа 2. Далі їх потрібно інвертувати і аж після цього ми отримаємо істинні паролі.

Якщо файл fn[]="mem.cit" не створений , то в програмі є наведені початкові паролі : user і master. Якщо користувач ввійшов у програму під паролем user , для нього відкривається лише перший рівень доступу. Тут

створена мінімальна форма, в якій можна змінити цей пароль та висвітлюється повідомлення "Ви можете тільки визначати час відкривання пломб".

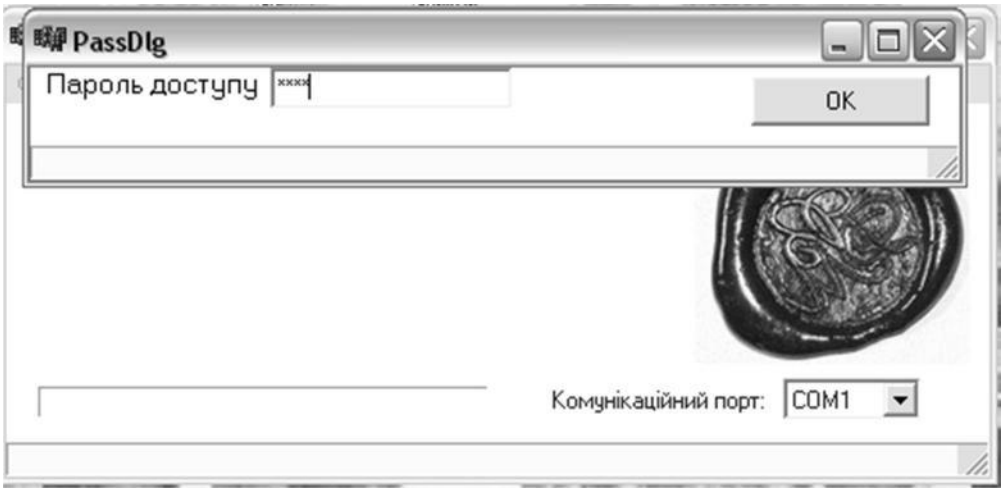


Рисунок 3.2 – Мінімальний рівень доступу до пристрою

Якщо користувач ввійшов до програми під паролем master , для нього відкривається рівень повного доступу. Тут створена форма в якій можна змінювати паролі 1 і 2 рівня, а також можна робити будь-які операції з пломбою. Висвітлюється повідомлення: "Ви можете встановлювати пломби та визначати час їх відкривання."

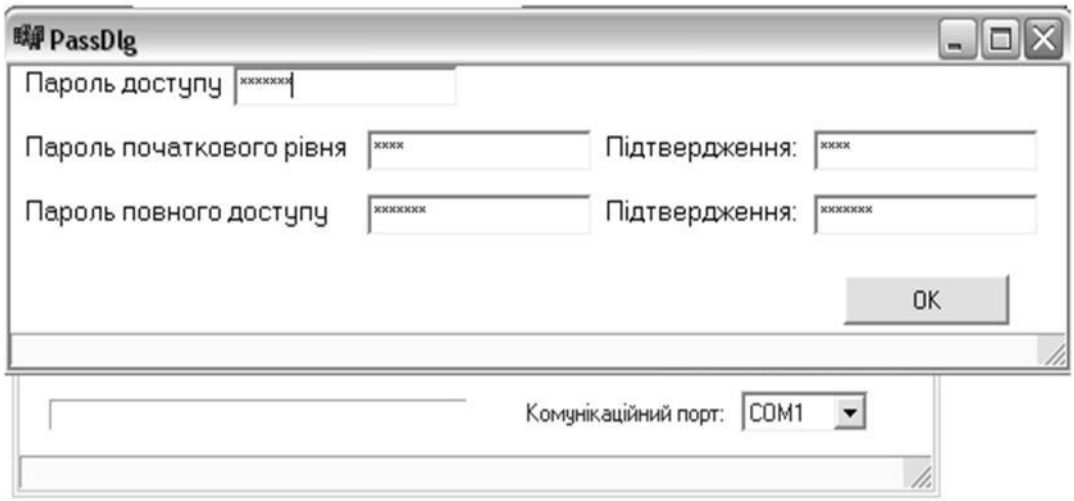


Рисунок 3.3 – Повний рівень доступу до пристрою

Тут можна зчитати час встановлення і відкривання пломби, встановити пломбу, очистити її чи перезапустити. Також тут можна змінювати тип комунікаційного порта.

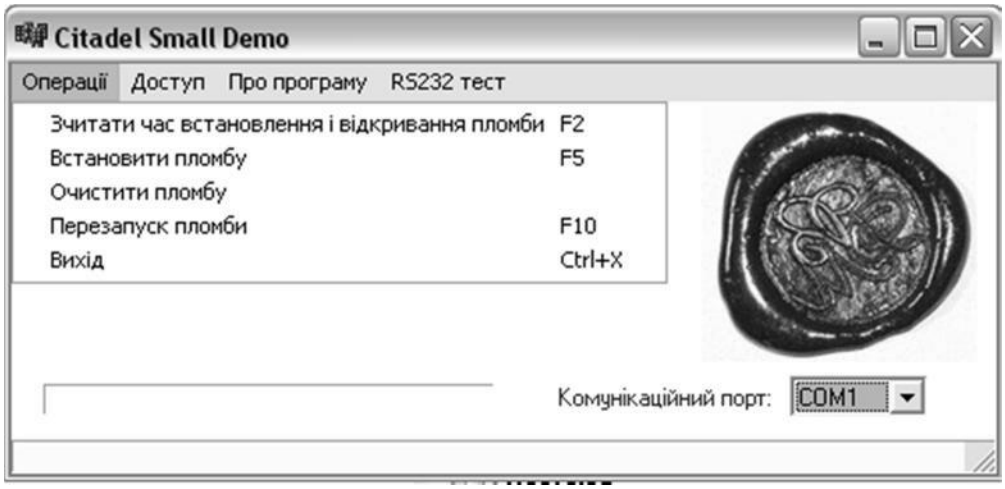


Рисунок 3.4 – Головне меню пристрою захисту.

Якщо був введений не правильний пароль , програма видає про це повідомлення "Невірний пароль!" і "Ви не маєте права працювати з програмою".

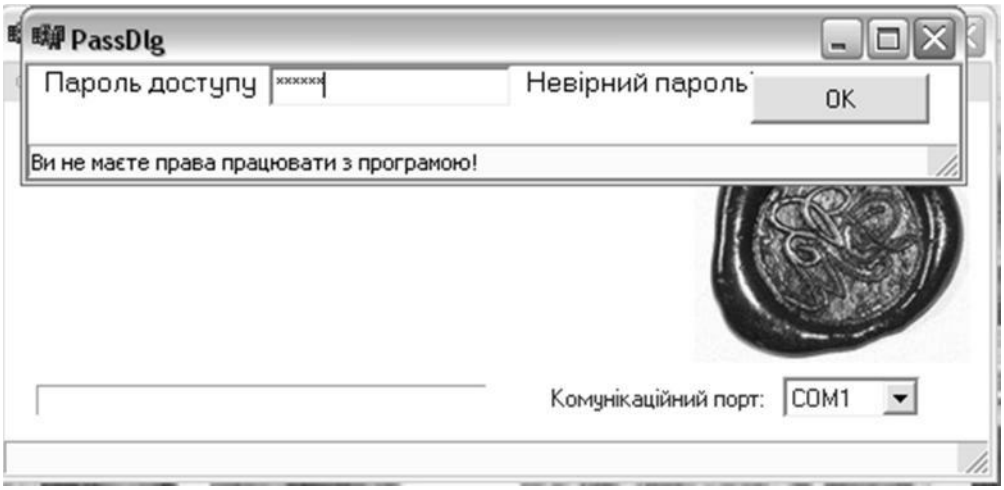


Рисунок 3.5 – Введено неправильний пароль.

Далі програма проводить перевірку справності мікроконтролера та каналу зв’язку . Якщо мікроконтролер чи порт не працює появляється повідомлення про помилку.

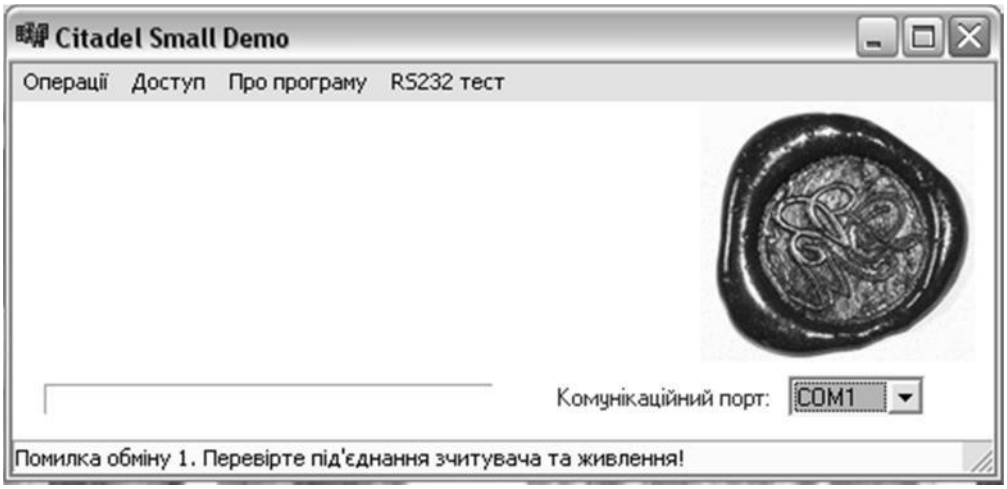


Рисунок 3.6 – Помилка зєднання

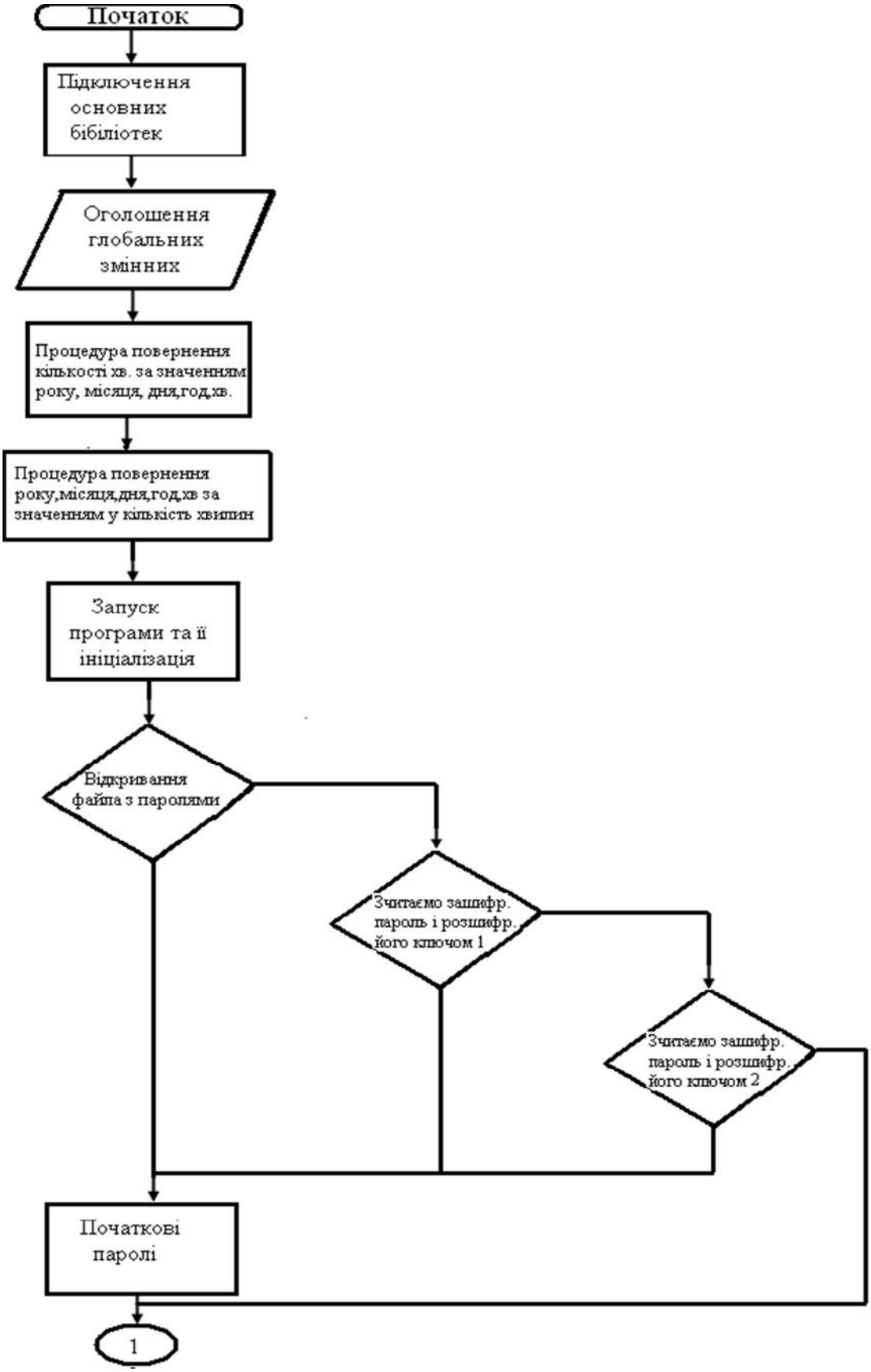
Якщо виникла помилка потрібно перевірити тип комунікаційного каналу, і якщо він не вірний, змінити його.

Якщо усе гаразд , тоді викликається ТЕСТ RS-232 і лише після натиснення клавіши ENTER відбувається обмін даних.

Далі програма запускає пломбу та зчитує усі дані з мікроконтролерного пристрою. Коли вся інформація прочитана програма приводить пломбу у початковий стан.

Великий "плюс" програми – те, що інформація про встановлення та відкривання пломби записана у хвилинах починаючи з 2000 року. Це зроблено для того, щоб ця інформація займала не багато памяті у мікроконтролерному пристрої. Спочатку роки, місяці, дні, години і хвилини записуються у хвилинах і передаються у пам'ять пломби. Пізніше програма зчитує всі дані з мікроконтролера, а потім вже у комп’ютері автоматично повертає кількість хвилин у відповідно рік, місяць, день, годину і хвилини обраховані з 2000 року. Також тут врахований і високосний рік.

Як видно із вище сказаного дана захисна система є надійною. Щоб отримати доступ до роботи з пломбою потрібно знати первинні чи зашифровані паролі, які розшифрувати зможе не кожен зловмисник. Пломба є достатньо досконалою, адже вона видає інформацію про точний час її встановлення і відкривання. Великим "плюсом" даного пристрою є те, що це мобільна система, яку можна встановлювати у будь-якому приміщенні.


Початок
Підключення основних бібліотек
Оголошення глобальних змінних
Процедура повернення кількості хв. за значенням року, місяця, дня,год,хв.
Процедура повернення року,місяця,дня,год,хв за значенням у кількість хвилин
Запуск програми та її ініціалізація
Відкривання файла з паролями
Зчитаємо зашифр. пароль і розшифр. його ключом 1
Зчитаємо зашифр. пароль і розшифр. його ключом 2
Початкові паролі
1

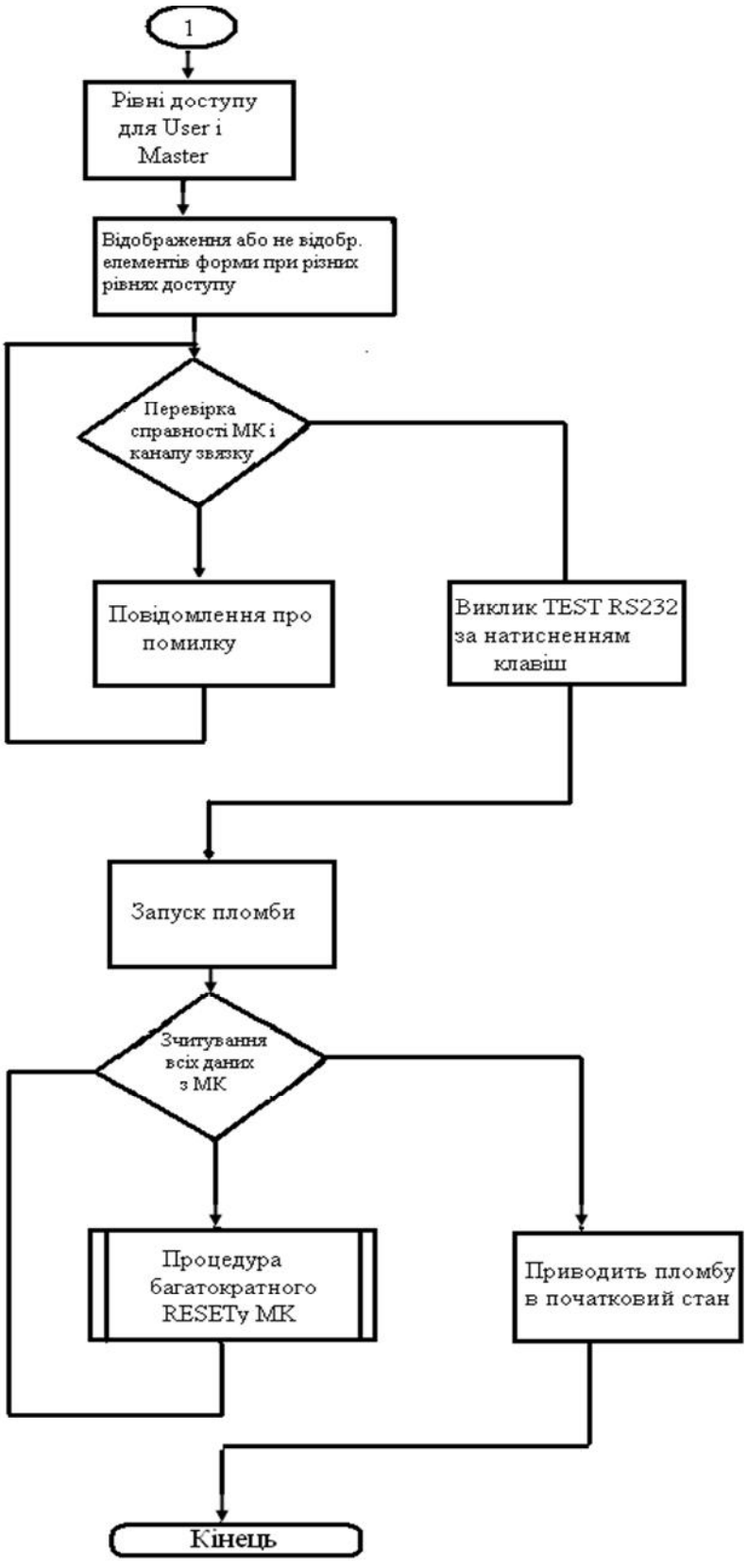


Рисунок 3.2 – Алгоритм функціонування електронної пломби

Після використання на одному об’єкті її легко можна встановити на іншому. Ще один "плюс" є те, що пломба працює на батарейці. По-перше, це економічно вигідно,а по-друге, з точки зору ОП –безпечно .

Описаний алгоритм роботи даної системи захисту представлений на рисунку 3.2.

3.2 Програмна реалізація програми мовою С++

Робота розробленої електронної пломби реалізована мовою С++. Далі буде описана робоча програма.

Головне вікно програми:

Спочатку підключаємо необхідні бібліотеки та оголошуємо змінні, які використовуються мікроконтролерним пристроєм:

```
#include <vcl.h>
#include <DateUtils.hpp>
#pragma hdrstop
 #define CLEAR_BUF for(int i=0; i<25;i++) buf[i]=0;
 #define MK_RST ComPort1->SetRTS(false); Sleep(50); ComPort1->SetRTS(true); Sleep(50); ComPort1->SetRTS(false); Sleep(100);
#include "Unit1.h"
#include "Unit2.h"
#include "About.h"
#include "time.h"
#include "stdio.h"
//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma link "CPort"
#pragma link "CPortCtl"
#pragma link "CCALENDR"
#pragma resource "*.dfm"

TForm1 *Form1;
char buf[25];
Word Nm;

#define STATE_BLANK 0x31
#define STATE_STARTED 0x37
#define STATE_OPENED 0x39

#define MODE_RSOK       0x5a  //01011010
#define MODE_START      0x69  //01101001    // sends state
#define MODE_READSTATE  0x26  //00100110    // state, number, start time, open time
#define MODE_MAKEBLANK  0x4d  //01001101    // sends state
#define MODE_READCNT    0xd6  //11010110
```

Далі оголошуємо глобальні змінні

```
unsigned char ch, state;

AnsiString str;

unsigned short AYear,AMonth,ADay,AHour,AMinute,ASecond,AMilliSecond;
const System::TDateTime AValue;
//---------------------------------------------------------------------
const unsigned int MIN_IN_DAY=24*60;
const unsigned int MIN_IN_YEAR=MIN_IN_DAY*365;
const unsigned int dm[13]={0,31,28,31,30,31,30,31,31,30,31,30,31};
unsigned int min,min2;
#define MINMIS(m) (dm[m]*MIN_IN_DAY)
```

Процедура, що повертає кількість хвилин за значенням року, місяця, дня, години, хвилини починаючи з 2000 року. Тут також враховано високосний рік.

```
unsigned int minut(unsigned int r, unsigned char m, unsigned char d, unsigned char h, unsigned char mn)
{

   unsigned int res=(r-2000)*MIN_IN_YEAR;
     unsigned int n_vis=(r-2001)/4; res+=n_vis*MIN_IN_DAY;
   for(int i=1; i<m; i++) res+=MINMIS(i);
   res+=(d-1)*MIN_IN_DAY+h*60+mn;
     return res;
}
```

Обернена до попередньої процедура, що повертає рік, місяць, день, годину і хвилини, починаючи з 2000 року у кількість хвилин.

```
void dat(unsigned int min,
      unsigned int &r, unsigned char &m, unsigned char &d, unsigned char &h, unsigned char &mn)
{

      unsigned int tmp=min;
      r=min/MIN_IN_YEAR;

      int n_vis=(r-1)/4;
      if(n_vis>0)
      {
            tmp-=n_vis*MIN_IN_DAY;
            r=tmp/MIN_IN_YEAR;
      }

      tmp-=r*MIN_IN_YEAR;
      for(m=1;m<12;m++)
      {
            if(tmp<MINMIS(m)) break;
            else tmp-=MINMIS(m);
      }
```

```
    d=tmp/MIN_IN_DAY+1; tmp-=(d-1)*MIN_IN_DAY;
    h=tmp/60; tmp-=h*60;


    mn=tmp; r+=2000;
    //res[0]=r; res[1]=m; res[2]=d; res[3]=h; res[4]=mn;
}
```

Далі йде запуск програми та її ініціалізація:

```
void __fastcall TForm1::FormActivate(TObject *Sender)
{

  FILE *stream;
  int i,n,x;
  AnsiString s;
```

Файл з зашифрованим паролем

```
  char fn[]="mem.cit";

  char sg[60000],gx[60000];


   PassDlg->key1="Simple key for coding. Life is good. Back for Good. Forever.345tyu..";
   PassDlg->key2="2347298374,cmvn,dmfngoi459-0rgdklfgjldkjgqq]This not simple...";
```

Відкриваємо файл з паролями

```
  if((  stream  = fopen( fn, "rb" ))!=NULL)

  {
    for(i=0;i<2000;i++) fscanf(stream,"%s\n",sg);
   //passs1
   fscanf(stream,"%s\n",sg);
   s=sg;
```

Перетворюємо символ в число

```
   n=StrToInt(s);
```

Зчитуємо зашифрований пароль і розшифровуємо його з допомогою ключа 1

```
   for(i=1;i<=n;i++)

   {fscanf(stream,"%s\n",sg);
    x=StrToInt(sg);
    gx[i-1]=(char)(x^PassDlg->key1.operator [](i));
   };
```

Запамятаємо розшифрований пароль

```
  PassDlg->c_pass1=gx;
```

Далі йде аналогічна процедура для 2 паролю

```
fscanf(stream,"%s\n",sg);
 s=sg;
 n=StrToInt(s);
 for(i=1;i<=n;i++)
 {fscanf(stream,"%s\n",sg);
  x=StrToInt(sg);
  gx[i-1]=(char)(x^PassDlg->key2.operator [](i));
 };
```

Зчитуємо 2000 байт випадкових даних

```
PassDlg->c_pass2=gx;
  for(i=0;i<2000;i++) fscanf(stream,"%s\n",sg);
  fclose(stream);
}
```

Якщо файл з зашифрованими паролями не створений то можна використовувати початкові паролі:

```
else {
    PassDlg->c_pass1="user";
    PassDlg->c_pass2="master";
}
```

Відповідно до того під яким паролем ввійшов користувач визначається рівень доступу:

```
if(PassDlg->passlevel==1) Form1->ReadAll->Enabled=true;
if(PassDlg->passlevel==2)          {Form1->ReadAll->Enabled=true;Form1->Startt->Enabled=true;}
}
```

При різних рівнях доступу відображаються або не відображаються елементи форми.

```
void __fastcall TForm1::FormPaint(TObject *Sender)
{
if(PassDlg->passlevel==2)
 {
 Form1->ReadAll->Enabled=true;
 Form1->Startt->Enabled=true;
 }
 else
 {
 Form1->ReadAll->Enabled=false;
 Form1->Startt->Enabled=false;
 }
if(PassDlg->passlevel==1) {Form1->ReadAll->Enabled=true;}
```

Процедура перевірки справності мікроконтролера та каналу зв’язку:

```
int TForm1::TestRS(void)
{
```

```
  if(ComPort1->Connected!=true) ComPort1->Connected=true;

  MK_RST;
  ComPort1->ClearBuffer(true,true);
  ch=MODE_RSOK;   ComPort1->Write(&ch,1);
  CLEAR_BUF;
  ComPort1->Read(buf,9);
  str=buf;
  if (str!="RS232 OK")
  {   for(int i=0;i<=5;i++)
      {
        Label8->Visible=(Label8->Visible^1);
        Application->ProcessMessages();
        Sleep(500);
      }
      StatusBar1->SimpleText=
        "Помилка обміну 1. Перевірте під'єднання зчитувача та живлення!";
      ComPort1->Connected=false;
      return 0;
  }
  ComPort1->ClearBuffer(true,true);
  return 1;
}
```

Виклик тесту RS232 за натисканням клавіш:

```
void __fastcall TForm1::RScheck1Click(TObject *Sender)
{
 StatusBar1->SimpleText="Тест...";

 if(!TestRS())return;
 Label3->Caption=str;
 StatusBar1->SimpleText=str;

 ComPort1->Connected=false;
}
```

Запуск пломби:

```
void __fastcall TForm1::StarttClick(TObject *Sender)
{
 StatusBar1->SimpleText="Запис...";
 ProgressBar1->Position=0;
 Application->ProcessMessages();

   if(!TestRS()) return;

   ProgressBar1->Position=0;
   ch=MODE_START; ComPort1->Write(&ch,1);
   ProgressBar1->Position=30;

   AValue=Now();
   DecodeDateTime( AValue, AYear, AMonth, ADay, AHour, AMinute, ASecond,
            AMilliSecond);
```

```
        min=minut(AYear,AMonth,ADay,AHour,AMinute);

        ComPort1->Write(&min,4);       // write current date
        ProgressBar1->Position=65;

        Nm=555; ComPort1->Write(&Nm,2);  // write serial number

        ComPort1->Read(&state,1);       // read resulting state

        if(state==STATE_STARTED)  StatusBar1->SimpleText="Пломба успішно встановлена.";
          else  StatusBar1->SimpleText="Помилка! Пломба не встановлена. state="+IntToStr(state);

        ProgressBar1->Position=100;
        ComPort1->Connected=false;
        Sleep(500);
        ProgressBar1->Position=0;
      }
```

Зчитування всіх даних з МК:

```
      void __fastcall TForm1::ReadAllClick(TObject *Sender)
      {
        unsigned int rik;
        unsigned char mis,den,god,hvyl,open;

        Label5->Caption="Номер пломби:"; Label3->Caption="";
        Label2->Caption="Встановлена:";  Label9->Caption="";
        Label4->Caption="Відкрита:";     Label11->Caption="";
        Label5->Visible=true; Label2->Visible=false; Label4->Visible=false;

        ProgressBar1->Position=0;
        StatusBar1->SimpleText="Зчитування...";

        if(! TestRS()) return;

        ch=MODE_READSTATE;  ComPort1->Write(&ch,1);
        ComPort1->Read(&state,1);

        if(state==STATE_BLANK)
        {
          Label3->Caption="не встановлена";
        }
        else    // read number & start time
        {
          ComPort1->Read(&Nm,2); // read number
          Label3->Caption=IntToStr(Nm);
          ProgressBar1->Position=30;
          ComPort1->Read(&min,4);
          dat(min,rik,mis,den,god,hvyl);
          ProgressBar1->Position=60;
```

```
        Label2->Visible=true; Label4->Visible=true;
        Label9->Caption=IntToStr(rik)+"р. "+ IntToStr(mis)+"міс.";
        Label9->Caption=Label9->Caption+": "+ IntToStr(den)+"день.";
        Label9->Caption=Label9->Caption+"  = "+ IntToStr(god)+"год.";
        Label9->Caption=Label9->Caption+" : "+ IntToStr(hvyl)+"хв.";
      }
      if(state==STATE_OPENED)     // read opening time
      {
        ComPort1->Read(&min2,4);
        min2+=min;
        dat(min2,rik,mis,den,god,hvyl);
        ProgressBar1->Position=80;

        Label11->Caption=IntToStr(rik)+"р. "+ IntToStr(mis)+"міс.";
        Label11->Caption=Label11->Caption+": "+ IntToStr(den)+"день.";
        Label11->Caption=Label11->Caption+"  = "+ IntToStr(god)+"год.";
        Label11->Caption=Label11->Caption+" : "+ IntToStr(hvyl)+"хв.";
      }
      else Label11->Caption="Не відкривалася";

      ComPort1->Connected=false;
      ProgressBar1->Position=100;
      Sleep(500);
      ProgressBar1->Position=0;
      StatusBar1->SimpleText="Інформація зчитана";
    }
```

Процедура, що приводить пломбу у початковий стан:

```
    void __fastcall TForm1::MakeBlankClick(TObject *Sender)
    {
      StatusBar1->SimpleText="Очистка...";
      ProgressBar1->Position=0;
      if(!TestRS()) return;
      ch=MODE_MAKEBLANK;  ComPort1->Write(&ch,1);
      ComPort1->Read(&state,1);
      if(state==STATE_BLANK) StatusBar1->SimpleText="Очистка виконана.";
        else StatusBar1->SimpleText="Помилка! Очистка не виконана.
state="+IntToStr(state);
      ComPort1->Connected=false;
    }
```

Процедура багатократного RESETу МК:

```
    void __fastcall TForm1::ResettClick(TObject *Sender)
    {
     StatusBar1->SimpleText="RST...";
     ProgressBar1->Position=0;
     if(ComPort1->Connected!=true) ComPort1->Connected=true;
     for(int i=0;i<1;i++)
     {
      MK_RST;
      Sleep(100);
```

```
 }
 StatusBar1->SimpleText="  ";
 ComPort1->Connected=false;
}
```

Вікно вводу паролів:

```
#include <vcl.h>
#pragma hdrstop

#include "Unit2.h"
#include "stdio.h"

//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma resource "*.dfm"
TPassDlg *PassDlg;
```

Обробник події «відпускання клавіша» :

```
void __fastcall TPassDlg::MaskEdit1KeyUp(TObject *Sender, WORD &Key,
    TShiftState Shift)
```

Далі програма запрограмована на різні рівні доступу користувача, яка починає спрацьовувати при вводі паролю та натисненні клавіши Enter.

```
{
 if (Key==13) // enter UP
{ pass=MaskEdit1->Text;
  passlevel=0;
  if (pass==c_pass1)
  { passlevel=1;
  };
  if (pass==c_pass2)
  { passlevel=2;
  };
```

Якщо пароль введена неправильно, програма видає повідомлення про це та повідомляє користувача, що він не має права працювати з програмою:

```
if(passlevel==0)
  {Label2->Caption="Невірний пароль!";
  StatusBar1->SimpleText="Ви не маєте права працювати з програмою!";
  }
```

Якщо введено пароль 1 рівня доступу програма видає повідомлення про те, що користувач може тільки визначити час відкривання пломби:

```
if(passlevel==1)
  {//Label2->Caption="OK!";
  StatusBar1->SimpleText="Ви можете тільки визначати час відкривання пломб.";
```

```
    Label3->Visible=false; Label4->Visible=false;
    Label5->Visible=false; Label6->Visible=false;
    MaskEdit3->Visible=false; MaskEdit4->Visible=false;
    MaskEdit5->Visible=false; MaskEdit2->Visible=false;

    SpeedButton1->Left=360; SpeedButton1->Top=4;    // Move & resizing
    PassDlg->Width=470;  PassDlg->Height=76;
    Label8->Visible=false;
    ComboBox1->Visible=false;
   };
```

Якщо введено пароль 2 рівня доступу програма видає повідомлення про те, що користувач може встановлювати пломби та визначати час їх відкриття:

```
if(passlevel==2)
  {//Label2->Caption="OK!";
   StatusBar1->SimpleText="Ви можете встановлювати пломби та визначати час їх відкривання.";
    Label3->Visible=true; Label4->Visible=true;
    Label5->Visible=true; Label6->Visible=true;
    MaskEdit3->Visible=true; MaskEdit4->Visible=true;
    MaskEdit5->Visible=true; MaskEdit2->Visible=true;

    SpeedButton1->Left=448; SpeedButton1->Top=104;    // Move & resizing
    PassDlg->Width=572;  PassDlg->Height=178;
  //  Label8->Visible=true;
  //  ComboBox1->Visible=true;

   };
 }
}
```

Створення форми, обробка днів, годин та хвилин у кількість хвилин:

```
void __fastcall TPassDlg::FormCreate(TObject *Sender)
{
pass11=pass10=c_pass1;
pass22=pass20=c_pass2;

ComboBox1->Text=ComboBox1->Items->operator [](0);
if (ComboBox1->Text=="5хв.")delay=5;
if (ComboBox1->Text=="10хв.")delay=10;
if (ComboBox1->Text=="30хв.")delay=30;
if (ComboBox1->Text=="1год.")delay=60;
if (ComboBox1->Text=="2год.")delay=120;
if (ComboBox1->Text=="5год.")delay=300;
if (ComboBox1->Text=="12год.")delay=720;
if (ComboBox1->Text=="24год.")delay=1440;


if (passlevel!=2){
    SpeedButton1->Left=360; SpeedButton1->Top=4;    // Move & resizing
    PassDlg->Width=470;  PassDlg->Height=78;
```

```
}
else
{
   SpeedButton1->Left=448; SpeedButton1->Top=104;    // Move & resizing
   PassDlg->Width=572;  PassDlg->Height=178;
}
}
```

Встановлення паролей різних рівнів доступу та видача повідомлень про можливості кожного з користувачів:

```
void __fastcall TPassDlg::FormCloseQuery(TObject *Sender, bool &CanClose)
{ FILE *stream;       // Store Data
   int i,n;
   char fn[255];

CanClose=true;
StatusBar1->SimpleText=" ";

if (pass11!=pass10) // ps1
{StatusBar1->SimpleText="Невірно встановлений пароль початкового рівня!";
CanClose=false;
}
if (pass20!=pass22) //ps2
{StatusBar1->SimpleText="Невірно встановлений пароль повного доступу!";
CanClose=false;
}
if (CanClose==true && pass20 ==pass10 && passlevel==2)
{StatusBar1->SimpleText="Паролі рівневого доступу не можуть бути однаковими!";
CanClose=false;
}

if ((CanClose==true) && (passlevel==2) )
{
    strcpy(fn,"mem.cit");
   if((  stream  = fopen( fn, "wb" ))!=NULL)
   {
    randomize();
      for(i=0;i<2000;i++) fprintf(stream,"%s\n",IntToStr(rand()%245+10));
   // PASS2
   fprintf(stream,"%d\n",pass10.Length());
   for(i=1;i<= pass10.Length();i++)
   {
    n=pass10.operator [](i)^(int)key1.operator [](i);
    fprintf(stream,"%d\n",n);
   }
   // PASS2

fprintf(stream,"%d\n",pass20.Length());
   for(i=1;i<= pass20.Length();i++)
   {
    n=pass20.operator [](i)^(int)key2.operator [](i);
    fprintf(stream,"%d\n",n);
```

```
    }

     for(i=0;i<2000;i++) fprintf(stream,"%s\n",IntToStr(rand()%245+10));
       fclose(stream);
     }
```

Створення форм:

```
void __fastcall TPassDlg::SpeedButton1Click(TObject *Sender)
{ TShiftState Shift;
  Word key;
bool CanClose=false;
if (passlevel==2)
{ MaskEdit1->OnKeyUp(Sender,key,Shift);
}
if (passlevel==2)
{key=13;
 MaskEdit2->OnKeyUp(Sender,key,Shift);
 MaskEdit3->OnKeyUp(Sender,key,Shift);
 MaskEdit4->OnKeyUp(Sender,key,Shift);
 MaskEdit5->OnKeyUp(Sender,key,Shift);
}
PassDlg->OnCloseQuery(Sender,CanClose);
if (CanClose==true) PassDlg->Close();
}
void __fastcall TPassDlg::FormActivate(TObject *Sender)
{
MaskEdit2->Text=c_pass1;  MaskEdit3->Text=c_pass1;
MaskEdit4->Text=c_pass2;  MaskEdit5->Text=c_pass2;
}
```

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ІПРАЦІ

4.1 Значення охорони праці для забезпечення безпечних та здорових умов праці

Гарантія безпечних умов праці та збереження здоров'я людей під час їх діяльності належить до пріоритетних напрямків державної політики України. Тому одна з найважливіших державних задач - охорона життя та здоров'я громадян в процесі їх трудової діяльності створення безпечних та нешкідливих умов праці.

Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних, лікувально-профілактичних заходів, спрямованих на збереження життя, здоров'я і працездатності людини в процесі праці.

Поняття „охорона праці" фактично розкриває напрями, які створюють систему забезпечення безпеки життя і здоров'я працівників у процесі їх трудової діяльності, тобто ця система містить заходи, які окремо або в сукупності спрямовані на створення умов праці, що відповідають вимогам збереження життя та здоров'я працівників у процесі трудової діяльності.

В умовах економічної кризи, високого безробіття працівники часто згідні працювати в будь-яких умовах, аби отримати зарплату, а роботодавець не завжди в змозі повністю створити необхідні умови та забезпечити безпеку праці. Статистичні дані свідчать, що нещасні випадки, професійні захворювання та аварії трапляються переважно у незадовільному економічному стані. На більшості виробничих підприємствах суми витрат за регресивними позовами на сьогодні дорівнюють фонду оплати праці, а це є не тільки гальмом економічного зростання, а й тим пресом, що душить підприємство.

За таких витрат на відшкодування шкоди в умовах непомірного податкового надзвичайного податкового тиску підприємствам малого бізнесу надзвичайно складно піднятися на ноги.

Економічне становище більшості підприємств не дає змоги забезпечити належний рівень охорони праці. Мале підприємство на стадії становлення має витратити певні кошти не тільки на організацію виробництва, придбання обладнання, законодавчо-нормативної літератури та посібників, індивідуальних і колективних засобів контролю і захисту.

На сьогодні понад 800 тис. одиниць обладнання, машин, механізмів не відповідають нормативно-правовим актам про охорону праці, використовується застаріле обладнання. Тому ЕТЦ виконують надзвичайно важливу функцію, визначаючи придатність обладнання для подальшої експлуатації. Але парадоксом є те, що технічний проект, зроблений в проектному інституті, власник має подавати на додаткову експертизу в ЕТЦ і платити за це відповідні кошти. Оскільки проектна організація реалізує закінчену роботу, яка повинна відповідати всім вимогам нормативних актів про охорону праці, то саме вона, на мою думку, й повинна мати справу з експертно-технічним центром на предмет проведення експертизи.

Враховуючи те, що існуючий стан охорони праці важким тягарем полягає на економіку країни, мають бути якнайшвидше впровадженні в життя економічні важелі, тобто введені страхові внески підприємств на охорону праці залежно від категорії підприємства і стану охорони праці. При цьому необхідно врахувати, що економічні санкції можуть прискорити банкрутство підприємств , які зазнають фінансових труднощів. Підприємства ставлять „на коліна" якраз ті які вони отримують, адже стиль і методи роботи інспектуючих органів залишився нам у спадщину від планової економіки.

Визначальним фактором процвітання і економічного благополуччя будь-якого підприємства малого бізнесу не тільки рівень

доходу, але й загальний стан охорони здоров'я. Нехтування таким фактором, як охорона праці, призводить до швидкого погіршення стану виробництва.

4.2 Аналіз потенційних небезпек та шкідливих факторів виробничого середовища

Дослідження показали, що сучасна професія користувача ЕОМ являє собою модель розумової праці, яка виконується в одноманітній позі в умовах обмеження загальної м'язової активності і при рухливості кистей рук, при високому напруженні зорових функцій та нервово-емоційному напруженні в умовах дії різноманітних фізичних факторів. В період роботи з моніторами на основі електронно-променевих трубок (ЕПТ) на організм користувача впливає цілий ряд факторів фізичної природи, але всі вони знаходяться в межах і значно нижче за нормовані величини відповідно до діючих зараз нормативних документів (таблиця 4.1).

При дослідженні зорових функцій у лабораторних та виробничих умовах були виявлені розлади акомодації, конвергенції, гостроти зору та контрастної чутливості ока. Причому виявлені зміни мали більш глибокий характер, коли праця супроводжувалась високим нервово-емоційним компонентом. Зоровий дискомфорт та втома виявляються у користувачів у вигляді різі, печії, болю в очах, ломоти у надбрівній області (так званої м'язової або окулярної астенопії), а також у вигляді розпливчатості меж або нечіткості зображення об'єкта, викликаних тимчасовим порушенням світлочутливого апарата ока (так званої візуальної астенопії, пов'язаної з порушенням світлочутливого апарата ока).

Ці явища часто супроводжуються головним болем, важкістю в голові, загальною втомою, сонливістю, млявістю.

Таблиця 4.1 - Аналіз потенційно-небезпечних виробничих факторів при роботі з ЕОМ.

Небезпечний фактор	Фактичне значення	Нормативне значення	Характер дії на людину
Рентгенівське випромінювання	45 мкР/год	75 мкР/год	Загальна втома, головний біль, різь в очах, роздратування
Ультрафіолетове випромінювання	0,001 мкР/год	0,01 Вт/м^2	
Видимий діапазон	4 Вт/м^2	10 Вт/м^2	
Яскравість	90 кД/м^2	>35 кД/м^2	
ІЧ-випромінювання	90 Вт/м^2	100 Вт/м^2	
Електростатичне поле	35 кВт/м	20-60 кВт/м	
Шум	ЗОдБ	50 дБ	Втрата слуху, головний біль, втомлюваність
Електричний струм	U=220 В, 1=3 А F=50Гц	U=220В,1>100тА f=50 Гц	Ураження електричним струмом

Світлотехнічна специфіка робочих місць з ЕОМ викликана такими унікальними особливостями:

- світлотехнічна різнорідність об'єктів зорової роботи користувачів ЕОМ пов'язана з наявністю трьох об'єктів (екран, клавіатура,

документація), розташованих у різних зонах спостереження, що вимагає багаторазового переведення лінії зору від одного до іншого. Таким чином, умови роботи ускладнюються необхідністю постійної перебудови апаратів акомодації та конвергенції, не кажучи вже про постійну необхідність переадаптації від яскравих об'єктів з позитивним контрастом на темні - з негативним. Разом узяті всі ці особливості створюють багато незручностей, а також напруження м'язового та світловідчуваючого апарата очей, що й є однією з головних причин виникнення астенопічних явищ;

- робота з пульсуючим самосвітним об'єктом, який постійно знаходиться у центрі поля зору, що не відповідає нормативним вимогам щодо обмеження пульсації та засліпленості;

- на робочому місці несприятливо розподілена яскравість у полі зору, оскільки освітлені поверхні периферії поля зору (стеля, стіни, меблі і т. п.) можуть виявитися світлішими, ніж центр поля зору - темний, обмежено освітлений та іноді слабо заповнений знаками екран. Такий розподіл яскравості у полі зору сприяє порушенню основних зорових функцій;

- засліплююча дія світильників, які освітлюють приміщення на робочому місці з монітором більша, ніж на інших, бо лінія зору користувача при роботі з екраном майже горизонтальна, що призводить до зменшення кута дії різних засліплюючих джерел (світильники, вікна і т. п.) і, відповідно, до зростання засліпленості;

- наявність дзеркально відбиваючої і неплоскої зовнішньої поверхні екрана не дає можливості повністю усунути з поля зору користувача всі відбиті відблиски.

4.3 Забезпечення нормальних умов праці

Забезпечення здорових і безпечних умов праці у виробничій сфері досягається при проектуванні, за рахунок дотримання діючих

нормативних документів, а для існуючих об'єктів - шляхом порівняння фактичних значень з нормативними і при їх відхилені розробкою та впровадженням заходів по приведенню їх до умов праці згідно вимог нормативних документів.

При роботі з ЕОМ температура повітря у приміщенні повинна становити 19-21 °С, відносна вологість повітря 55 - 65%, швидкість руху повітря не більше 0,2 м/с, відповідно до вимог «Санітарних норм мікроклімату виробничих приміщень» № 4088-86. Нормативні характеристики метеорологічних умов у приміщенні наводяться в таблиці 4.2. Характеристики системи вентиляції подано в таблиці 4.3.

Таблиця 4.2 - Нормативні характеристики метеорологічних умов

Виробниче приміщення	Категорія важк.фіз. робіт	Період року	Температура °С	Відносна вологість,%	Шв. руху повітря
Офіс	Іа (сер.)	Теплий Холодний	+21-23 +18-20	40-60 40-60	0,3 0,2
Промислове приміщення	Іа (сер.)	Теплий Холодний	+23-25 +16-18	40-60 40-60	0,2 0,2

Рівні звуку та еквівалентні рівні звуку у приміщеннях -де працюють оператори ЕОМ, не повинні перевищувати 50 дБ А, а на робочих місцях у приміщеннях, де розташовані шумні агрегати обчислювальних машин, рекомендується забезпечити рівень шуму не більше 75 дБ.

Необхідне проведення комплексу заходів щодо боротьби зі статичною електрикою. Рівні іонізації повітря при роботі з ЕОМ наведені в таблиці 4.4. Найбільш допустимим і простим способом є підтримання відносної вологості повітря на рівні 55 - 65%. Підлоги в дисплейних класах мають бути застелені антистатичним лінолеумом. Програмістам та операторам можна рекомендувати носити одяг, особливо першого шару, з натуральних

матеріалів. Всі полімерні покриття (чохли) ЕОМ слід складати у найбільш віддаленому від операторів місці приміщення.

Таблиця 4.3 - Характеристика системи вентиляції

Виробниче приміщення	Вид вентиляції	Вентиляційне обдаднання	Кратність пов. обміну (1/год)
Офіс	Механічна місцева	Кондиціонер повного кондиціювання повітря TOCHIBA – 2SMG	3
Промислове приміщення	Механічна місцева	Кондиціонер повного кондиціювання повітря ВЦ 4-70	3

Таблиця 4.4 - Рівні іонізації повітря в операторній

Рівні	Кількість іонів в 1 $см^3$ повітря	
	Позитивні	негативні
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально допустимі	50000	50000

Враховуючи специфіку зорової роботи з ЕОМ, першочерговим завданням є забезпечення необхідних умов візуальної роботи користувачів ЕОМ за рахунок найкращого розподілу яскравостей у полі зору працюючого та максимально можливого зменшення засліпленості від прямого і відбитого блищання та відмежування від постійної пульсації

зображення на екрані та інших перешкод, які посилюють загальну та зорову втому. Необхідно забезпечити як кількісні, так і якісні параметри освітлення. Для цього слід перш за все правильно вибрати приміщення: необхідно враховувати, що вікна можуть давати відблиски на екранах дисплеїв і викликати значну засліпленість у сидячих перед ними, особливо літом та в сонячні дні; для розміщення ЕОМ найбільш придатні приміщення з однобічним розміщенням світлових отворів, які обов'язково мають бути обладнані сонцезахисними пристроями: шторами, жалюзі та ін., площа засклення не повинна перевищувати 25% від площі стіни з вікнами. Для мінімізації засвічування від сонячних променів екранів вікна мають бути орієнтовані на північ (північний захід, північний схід).

Таблиця 4.5 – Характеристика штучної освітленості робочих місць

Виробниче Приміщення	Розряд та підозряд зорової роботи	Освітленість, Лк			Типи Світильників
		Загальна	Комбінована	Аварійна	
Офіс	III, г	400	450	10	ЛПО-12 «Косо-світло»
Промислове приміщення	V,б	200	250	8	ВЗГ-100

Необхідно забезпечити відповідне оформлення інтер'єра, бо давати відблиски на екранах і сліпити працюючих можуть не тільки вікна, але й інші поверхні великої яскравості, у тому числі стеля, стіни, поверхні столів, шаф і навіть одяг персоналу. Тому все повинне мати невисокі коефіцієнти віддзеркалення.

Робочі місця з ЕОМ доцільно розміщувати в глибині приміщення. При використанні в загальному освітленні світильників прямого світла комп'ютери мають бути обов'язково організовані в ряди, паралельні до стіни з вікнами.

Система освітлення має бути загальною і загальною локалізованою. Найбільш оптимальними є світильники навкісного світла. Це - дзеркальні світильники з параболо - циліндричними відбивачами.

Світильники мають бути розташовані над проходами між рядами ЕОМ суцільною лінією або з проміжками залежно від кількості світильників у лінії, необхідної для забезпечення нормованої освітленості.

4.4 Розрахунок вентиляції промислових приміщень

Системи опалення і системи кондиціонування розташовуються так/щоб ані тепле, ані холодне повітря не спрямовувалось на людей. На виробництві рекомендовано створювати динамічний клімат з визначеними перепадами показників. Температура повітря на поверхні підлоги і на рівні середнього людського зросту не повинна відрізнятися більш, ніж на 5°С. У виробничих приміщеннях, крім природної вентиляції, передбачають витяжну вентиляцію. Основним параметром, що визначає характеристики вентиляційної системи, є кратність обміну, тобто скільки разів у годину переміниться повітря в приміщенні.

Далі наведено розрахунок потрібної вентиляції для операторної ЕОМ згідно довідкової інформації. Вихідними даними є:

Vвент - об'єм повітря, необхідний для обміну;

Vприм - об'єм робочого приміщення.

Для розрахунку прийнято наступні розміри робочого приміщення:

Довжина В = 7,35 м;

Ширина Л - 4,9 м;

висота Н - 4,2 м. Відповідно, об'єм приміщення дорівнює:

$$V_{прим} = A*B*H$$

$$V_{прим} = 7,5*4,2*3,5=110,25$$

Необхідний для обміну обсяг повітря К, визначимо, виходячи з рівняння теплового балансу:

Vвент *C*(tвент- t прим)*Y=3600*Qнадлишкове

де: Qнадлишок - надлишкова теплота (Вт);

C=1000 - питома теплопровідність повітря (Дж/кг * К);

Y =1,2 — густина повітря (мг/см^3).

Температура повітря, що витікає з приміщення, визначається за формулою:

$$t_{вент} = tp.м + (H - 2)*t$$

де t = l-5 °С-перевищення і на їм висоти приміщення;

tp.м. = 25 °С - необхідна температура на робочому місці; H=4,2 м — висота приміщення;

Qнадлишок= Qнадлишок1+ Qнадлишок2+ Qнадлишок3

$$t_{вент} = 25 + (3.5- 2)*2 = 28 °C.$$

де Qнадлишок1- надлишок тепла від електроустаткування і освітлення:

Qнадлишок1= E*P

де E - коефіцієнт втрат електроенергії на тепло відвід (E=0,55 для освітлення);p –потужність, p= 40*15 = 600 (Вт).

Qнадлишок1= 0,55*600 = 330 (Вт).

Qнадлишок2- теплопоступлення від сонячної радіації:

Qнадлишок2= m *S*k*Qc

де m - число вікон, приймається m=4; S- площа вікна,

S = 1.8*2.9 = 5.22 (м^2);

k - коефіцієнт, що враховує заскленість. Для подвійної засклености (береться подвійна, оскільки в комп'ютерному класі використовуються пластикові вікна, що по рівню теплоізоляції можна прирівняти до подвійно засклених вікон): k=0.6;

Qc = 127 Вт/м2 - теплопоступлення від вікон.

Qнадлишок2= 5.22 *4*0.6* 127= 1591.056(Вт)

Qнадлишок3- тепловиділення людей

$$Q_{надлишок3} = n*q$$

де q- 80 Вт/люд.;

n - число людей, наприклад, n=6.

$$Q_{надлишок3} = 3*80 = 240(Вт)$$

$$Q_{надлишок} = 330 + 1591.056 + 240 = 2161.056\ (Вт).$$

З рівняння теплового балансу випливає:

$$V = \frac{3600 \cdot 2161.056}{1000(28-18)} = 777.98$$

Оптимальним варіантом є кондиціонування повітря, тобто автоматична підтримка його стану в приміщенні відповідно до визначених вимог (задана температура, вологість, рух повітря) незалежно від зміни стану зовнішнього повітря й умов у самому приміщенні.

Вентиляційна система, побудована за такими принципами складатиметься з наступних основних елементів (промисловий варіант такої системи зображений на рисунку 5.1):

-пригінної камери, до складу якої входять вентилятор з електродвигуном, калорифер для підігріву повітря в холодний час

-року і грати, типу жалюзі, для регулювання обсягу повітря, що надходить;

-круглого сталевого повітропроводу довжиною 0,5 м;

-повітророзподільника для подачі повітря в приміщення.

Втрати тиску у вентиляційній системі визначаються за формулою:

$$H = R*l + \frac{V^2 * p}{2}$$

де Н - втрати тиску, Па; К - питомі втрати тиску на тертя у повітропроводі, Па/м; l - довжина повітропроводу, м; v-швидкість повітря, (v = 3 м /с); р - густина повітря, (р -1.2 кг/м3).

Необхідний діаметр повітропроводі для даної вентиляційної системи:

D=0.091(м)

Приймається як діаметр найближча велика стандартна величина - 0,45 м, при якій питомі втрати тиску на тертя у повітропроводі - R = 0,24 Па/м.

Місцеві утрати виникають у залізних ґратах (приблизний коефіцієнт 1,2), повітророзподільнику (1,4) і калорифері (2,2). Звідси, сумарний коефіцієнт місцевих втрат у системі:

$$x = 1,2 + 2,2 + 1,4 = 4,8$$

$$H = 26.28 \text{ (Па)}.$$

Тоді з врахуванням 10 %-го запасу:

$$H = 110\% * 26.28 = 28,01 \text{ (Па)}.$$

$$V_{вент} = 110\% * 1442 = 1586.2 \text{ (м3/год)}.$$

Маючи параметри вентиляційної системи, можна обрати потрібний вентилятор. Таким вентилятором може бути, наприклад, осьовий вентилятор ВЦ-4-70/

В таблиці 4.6 наведені його характеристики. Обрано другий варіант виконання з потужністю двигуна 0,25 кВт/год.

Таблиця 4.6 - Характеристики вентилятора ВЦ-4-70

Марка вентилятора	Потужність, кВт/год.	Частота обертання, об./хв.	Витрата повітря, тис. м /год.	Тиск, Па
ВЦ-4-70	0,25	1500	1,2-2,0	25-65
	0,55	3000	2,8 - 4,0	50-150

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було розроблено мобільну системи контролю несанкціонованого доступу до промислових приміщень. Великий "плюс" розробленої системи – те, що інформація про встановлення та відкривання пломби записана у хвилинах починаючи з 2000 року. Це зроблено для того, щоб ця інформація займала не багато памяті у мікроконтролерному пристрої. Спочатку роки, місяці, дні, години і хвилини записуються у хвилинах і передаються у пам'ять пломби. Пізніше програма зчитує всі дані з мікроконтролера, а потім вже у комп’ютері автоматично повертає кількість хвилин у відповідно рік, місяць, день, годину і хвилини.

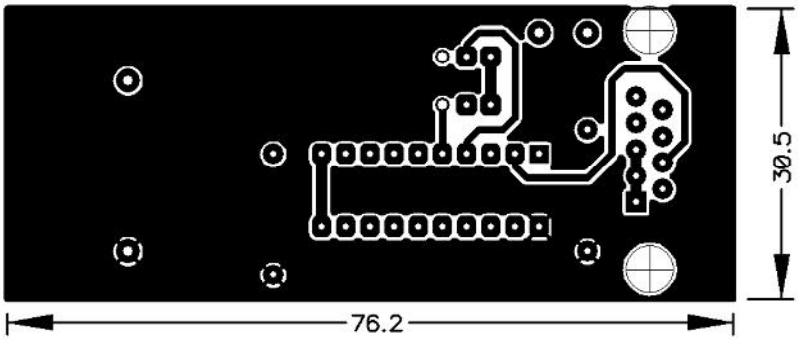
Як видно із вище сказаного дана захисна система є надійною. Щоб отримати доступ до роботи з пломбою потрібно знати первинні чи зашифровані паролі, які розшифрувати зможе не кожен зловмисник. Пломба є достатньо досконалою, адже вона видає інформацію про точний час її встановлення і відкривання. "Плюсом" даного пристрою є те, що це мобільна система, яку можна встановлювати у будь-якому приміщенні. Після використання на одному об’єкті її легко можна встановити на іншому. Ще один "плюс" є те, що пломба працює на батарейці.

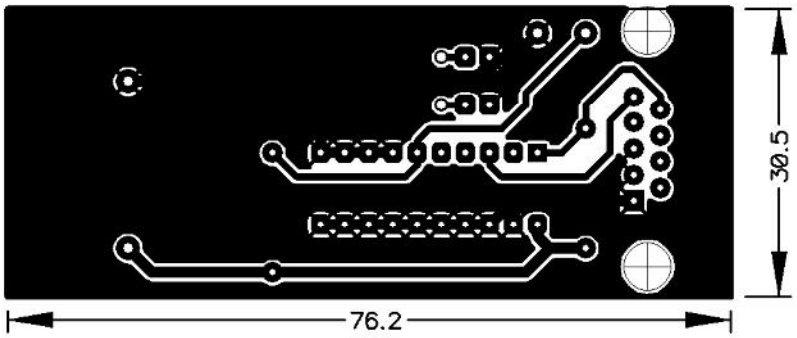
ПЕРЕЛІК ПОСИЛАНЬ

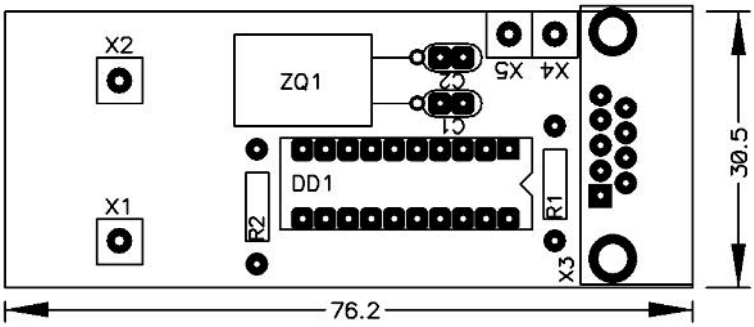
1. Бабенко Л.П., Лавріщева К.М. Основи програмної інженерії: Навч. посіб. – К.: Т-во “Знання”, КОО, 2001. – 269с.
2. Вильховченко С.Д. Модем. Выбор, настройка и использование. Сопутствующий справочник по телекоммуникациям. – М.: ABF, 1995. – 284с.
3. Тейксейра С., Пачеко К. Руководство разработчика, том 1. Основные методы и технологии: Пер. с англ.: Уч. пос. – М.: Издательский дом “Вильямс”, 2000.-832с.
4. Paradox для Windows: Практическое руководство. Под ред. Оспищева Д.А. Издательство АОЗТ “Алевар”, 1993.
5. Охорона праці: Навч. посібник для студентів вищих нвчальних закладів. За ред. Геврика Є.О. – Львів: - 2000.
6. Калічак О.В. Електроосвітлювальне та освітлювальне устаткування: Навч. посібник. – К.: ІСДО, 1995 – 64с.
7. Воллернер Н.Ф., Радиоприемные устройства: Навч. посібник. – К.: Вища шк., 1993. – 391 с.
8. Агуров П.В., Последовательные интерфейсы ПК. Практика програмирования. – СПб.: БХВ – Петербург, 2004. – 496с.: ил.
9. Архангельський А. Я. C++ BUILDER 6. Справочное пособие. Книга 1. Язык C++. – М.: Бином-Пресс, 2002 г. – 544 с.: ил.
10. М. Теллес. Borland C++ Builder: бібліотека програміста.- СПБ.: Пітер Ком, 1998.- 512с
11. Методичні вказівки до виконання кваліфікаційної роботи бакалавра спеціальності 151 «Автоматизація та комп’ютерноінтегровані технології»./ В.Б. Савків., ІО.Б. Капаціла, Р.І. Михайлишин//-: Тернопіль, Тернопільський національний технічний університет імені Івана Пулюя, 2021, – 46с.

ДОДАТОК А.

Друкована плата електронної пломби







ДОДАТОК Б.

Друкована плата узгоджуючого пристрою «пломба/ЕОМ»

(програматор)