МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю. М. ПОТЕБНІ

Кафедра електроніки, інформаційних систем
та програмного забезпечення
(повна назва кафедри)

Кваліфікаційна робота

перший бакалаврський
(рівень вищої освіти)

на тему *Розробка автономної системи контролю і управління доступом у приміщення*

Виконав: студент (ка) *IV* курсу, групи *6.1531*

Спеціальності *153 (176) Мікро- та наносистемна техніка*
(код і назва спеціальності)

освітньої програми *Мікро- та наносистемна техніка*
(код і назва освітньої програми)
С. С. Липницький
(ініціали та прізвище)

Керівник *доцент кафедри ЕІСПЗ, доцент, к.т.н.*
Верьовкін Л. .Л.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент *завідувач кафедри електричної інженерії та кібер-фізичних систем, професор, д.т.н.*
Коваленко В. Л.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

м. Запоріжжя
2025

МІНІСТЕРСТВО НАУКИ І ОСВІТИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю. М. ПОТЕБНІ

Кафедра *електроніки, інформаційних систем та програмного забезпечення*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *153 (176) Мікро- та наносистемна техніка*
(код і назва)

Освітня програма *Мікро- та наносистемна техніка*
(код і назва)

Спеціалізація _____

ЗАТВЕРДЖУЮ
Завідувач кафедри *ЕІСПЗ*
Критська Т. В.
"*10*" *червня* 20*25* року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ

Липницькому Сергію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка автономної системи контролю і управління доступом у приміщення*
керівник роботи *Верьовкін Леонід .Леонідовия, доцент, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від *"27" грудня 2024 року №2029-с*
2. Строк подання студентом роботи *10 червня 2025 року*
3. Вихідні дані до роботи *Обрати систему контролю і управління доступом у приміщення*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): *Системи охорони та запобігання проникнення у приміщення. Розробка системи контролю і управління доступом у приміщення. Охорона праці та техногенна безпека*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) *Функціональна схема електричного запобігання проникненню у приміщення. Структурна схема кодуючого пристрою. Аналіз функціонування схеми контролю і управління доступом у приміщення. Система електричного запобігання проникненню у приміщення*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата завдання прийняв
I	*Верьовкін Л. Л., доцент*	
II	*Верьовкін Л. Л., доцент*	
III	*Верьовкін Л. Л., доцент*	

7. Дата видачі завдання _____*10.02.2025 року*_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи бакалавра	Строк виконання етапів роботи	**Примітка**
1	*Дослідження систем контролю доступу у приміщення*	*28.02.2025*	
2	*Дослідження схем ідентифікаторів користувача*	*21.03.2025*	
3	*Дослідження контролерів обробки інформації*	*04.04.2025*	
4	*Логічне моделювання схеми функціонування приладу*	*25.04.2025*	
5	*Розробка пристрою ідентифікації*	*08.05.2025*	
6	*Розробка виконавчих пристроїв*	*16.05.2025*	
7	*Розробка кодонаборної кнопкової клавіатури*	*20.05.2025*	
8	*Охорона праці та техногенна безпека*	*23.05.2025*	
9	*Оформлення пояснювальної записки*	*10.06.2025*	
10	*Рецензування, нормоконтроль, підписання роботи*	*13.06.2025*	
11	*Оприлюднений захист магістерської роботи*	*17-18.06.2025*	

Студент _____ _____*Липницький С. С.*_____
(підпис) (прізвище та ініціали)

Керівник роботи (проекту) _____ _____*Верьовкін Л. .Л.*_____
(підпис) (прізвище та ініціали)

Нормоконтроль пройдено

Нормоконтролер _____ _____*Верьовкін Л. Л.*_____
(підпис) (прізвище та ініціали)

Реферат

Дипломна робота містить 69 сторінок, 34 рисунка, 7 таблиць, 8 джерел літератури.

Об’єкт дослідження – пристрої електричного запобігання проникненню у приміщення.

Мета роботи – розробка системи електричного запобігання проникненню у приміщення підвищеної надійності.

Задачі роботи: забезпечити відкриття електромагнітного замка натисканням трьох кнопок коду у відповідній послідовності; забезпечити економічну схемотехніку пристрою для підвищення надійності при виконанні функцій запобігання проникнення у приміщення; забезпечити підвищення секретності кодового замка підрахунком кількості натискань кодових кнопок.

Методика досліджень – моделювання пристрою за допомогою програмних забезпечень: Electronics Workbench 5.12, SPlan 5.0.

Короткий виклад результатів досліджень –схема може бути використана в якості кодового замка, відкриття якого проводиться набором відомого обмеженому колу осіб коду з 3 цифр, які необхідно натиснути в заданій послідовності.

Результати впроваджень – електронний макет пристрою пройшов випробовування на кафедрі ЕІСПЗ.

Прогнозні пропозиції – розроблена схема може знайти застосування в будь-яких пристроях, де потрібно обмежити доступ сторонніх до перемикання режимів чи налаштування електронних пристроїв.

ЕЛЕКТРОМАГНІТ, ЗАМОК, КОД, КЛАВІАТУРА, ГЕНЕРАТОР, РЕГІСТР, ЛІЧИЛЬНИК, КОЛОДКА, СИГНАЛІЗАЦІЯ, ТРИГЕР

Дипломну роботу виконано на кафедрі електроніки, інформаційних систем та програмного забезпечення, з 10.02.2025 по 10.06.2025.

Зміст

Стор.

Вступ …….. 6

1 Системи охорони та запобігання проникнення у приміщення ……. 8

1.1 Системи контролю доступу у приміщення …….. 11

1.1.1 Ідентифікатор користувача ……. 12

1.1.2 Контролери обробки інформації …… 13

1.1.3 Пристрої ідентифікації …… 15

1.1.4 Виконавчі пристрої …….. 19

1.2 Кодонаборні кнопкові клавіатури ……. 21

2 Розробка системи контролю і управління доступом у приміщення …. 25

2.1 Розрахунок алгоритму функціонування кодової клавіатури …….. 26

2.2 Схема послідовного натискання закодованих кнопок …… 31

2.2.1 Генератор числових послідовностей на регістрі зсуву …… 32

2.2.2 Паралельно – послідовний регістр для зберігання і перетворення закодованої інформації ……. 35

2.2.3 Кодування номерів та порядку натискання кнопок ……. 36

2.3 Виконавчий пристрій ……. 38

2.4 Схема підвищення секретності кодового замка …….. 39

2.5 Схема сповіщувачів …… 44

2.6 Схема електрична кодового пристрою запобігання проникнення у приміщення ……... 51

3 Охорона праці та техногенна безпека …….. 56

3.1 Характеристика потенційних небезпечних та шкідливих виробничих факторів …….. 56

3.2 Заходи з поліпшення умов праці. Виробнича санітарія ……. 58

3.3 Електробезпека ……... 61

3.4 Пожежна безпека. Техногенна безпека …….. 63

3.5 Розрахунок захисного заземлення ……. 65
Висновки та рекомендації …… 68
Перелік посилань …….. 69

Вступ

Системи електронних охоронних сигналізацій є одним з головних перешкод на шляху несанкціонованого проникнення на об'єкт. Існує цілий спектр цифрових охоронних сигналізацій для власного житла. Такі сигналізації, як правило, мають звукове або GSM оповіщення іноді вони встановлюються окремими охоронними фірмами. Їх основні недоліки полягають у завищеній ціні, закритості прошивки контролера, протоколів спілкування з датчиками.

Актуально що навіть наявність простої охоронної системи зменшує ймовірність зазіхань грабіжників на здійснення проникнення на територію, яка охороняється.

У зв'язку з широким використанням сучасних електронних компонентів і цифрових методів обробки інформації відбувається істотна "інтелектуалізація" технічних засобів охорони. Ці засоби перестають бути просто допоміжними і набувають нових властивостей, що робить істотний вплив на організацію охорони і її рівень. Сучасні технічні засоби охорони можуть бути використані у вигляді повністю інтегрованої системи або системи, що складається з функціонально незалежних компонентів:

- охоронна сигналізація,
- система контролю доступу в приміщення з перевіркою повноважень,
- система телевізійного спостереження,
- контрольні та інші пристрої.

Сучасні охоронні системи представляють з себе цілий проект з великим набором різноманітних датчиків з яких можна зібрати велику, надійну та безвідмовну охоронну сигналізацію, та такі типи сигналізацій будуть не по кишені більшості можливих покупців.

Принцип дії охоронної сигналізації дуже простий. Інсталятором (монтажною організацією) розглядаються місця можливого проникнення на об'єкт

і блокуються охоронними датчиками (в цьому плані найбільш уразливими з точки зору безпеки є вікна і двері). У приміщенні охорони встановлюється прилад охоронної сигналізації. У разі відкриття дверей, вікна, розбитті скла, несанкціоноване проникнення в офіс, спрацьовує відповідний датчик, і сигнал передається на прилад охоронної сигналізації в приміщенні охорони. Чи включається звукова і світлова сигналізація, оповіщаючи охорону про те, що на об'єкт, в такому то місці хтось проник. Найбільш поширеними датчиками, використовуваними в охоронної сигналізації є інфрачервоні датчики руху, акустичні датчики розбиття скла, геркони (магніто-контактні).

1 Системи охорони та запобігання проникнення у приміщення

Охоронна система – автономна система для забезпечення захисту різноманітного майна від не благочинних факторів та ситуацій різного характеру [1].

Висока відповідальність за виконання поставленого завдання, охорона майна та інформації, відповідальність, яка покладена на роботодавця за персонал і багато іншого постійно змушує сучасне суспільство удосконалювати систему контролю. Досконале зрозуміло, що подібні заходи безпеки не можливі без сучасних електронних «помічників».

Охоронні системи попереджують як можливі порушення кримінального характеру так і можливі трагедії наприклад пожежу.

Види охоронних систем:

– охоронно – тривожна сигналізація;

– пожежна сигналізація;

– системи інформаційної безпеки;

– системи охорони периметра;

- системи охоронного освітлення.

Системи контролю і управління доступом (СКУД) є невід'ємною частиною інтегрованих систем безпеки і допомагають захистити від небажаних вторгнень на об'єкт, відстежувати переміщення людей, контролювати ситуацію на об'єкті. СКУД є комплексом спеціального технічного і програмного забезпечення, призначеним для здійснення контролю і реєстрації доступу об'єктів (людей або транспорту) в приміщення або на території.

Дивлячись на неухильне зростання інтересу до СКУД і перспективу широкого їх застосування в найближчому майбутньому, не слід забувати, що СКУД лише спрощує процес ідентифікації, економить час і підвищує ефективність роботи служб безпеки підприємства, але, при цьому, все одно вимагає контролю з боку людини. Від рівня ймовірних загроз і поставлених перед

системою завдань, залежить необхідність підбору оптимального співвідношення між людьми і технічними ресурсами системи.

Найчастіше, в автоматизованих СКУД, застосовується контроль об'єктів різних категорій, при цьому територія поділяється на декілька автономних зон контролю, мають певні особливості доступу і свої види обмежень на відвідування [1].

Об'єкти СКУД являють собою:

- входи в окремі приміщення або групи приміщень;

- входи на ізольовані об'єкти або потребують обмеження в місцях масових скупчень людей;

- проходи на відгороджені або відкриті території;

- проїзди, або проходи, обладнані автоматичними воротами, турнікетами, шлагбаумами, або пристроями виконують обмеження для доступу;

- контрольні і пропускні пункти по периметру об'єкта;

- доступ до предметів мистецтва та художніх цінностей;

- доступ до приладів та обладнання, що забезпечує життєво-важливі функції.

При поділі об'єктів доступу на категорії, необхідно розрізняти.

1. Доступ в зону контролю. У даному випадку мова йде про доступ в окремо розташовану будівлю або на окремий поверх в будові, що знаходиться на території.

2. Доступ до приміщення. Передбачає можливість відвідування певного приміщення на території.

Основний принцип дії наступний: найбільш суворі вимоги до ідентифікації та обмеження режиму доступу мають об'єкти (приміщення, зони), відвідування яких дозволено лише вузькому колу осіб, які мають права доступу, видані відповідальним рівнем адміністрації. Для приміщень, як правило, застосовують, більш жорсткий режим доступу, ніж при відвідуванні зон контролю. Існують ситуації, в ряді яких правила на вхід і вихід, здійснюються за різними правилами.

Режими доступу, застосовувані для автоматизованого контролю, можна розділити.

1. Без обмежень доступу. Вільний прохід застосовується для приміщень, які мають необхідність постійного або тимчасового відвідування персоналом або в разі аварійних ситуацій. Може бути: абсолютно безконтрольним, що відповідає повному відключенню систем контролю; абсолютним і контрольованим - прохід вільний, але, проводиться реєстрація відвідувачів; умовним - пройти може будь-яка особа, що знає правила проходу або володіє ключем.

2. Доступ по праву доступу. Це основний вид режиму в СКУД. Для надійності в таких системах способи надання конкретним особам прав доступу здійснює адміністратор системи контролю доступу, діючий на підставі прийнятих організацією адміністративних процедур. Обов'язково відстежується і виключається можливість зміни прав іншими особами, використовується обмеження доступу до технічних засобів.

3. Заборона доступу. Застосовується при виникненні особливих ситуацій. Може бути як плановим так і екстреним. У цих випадках застосовуються режими заборони до всіх або деяких зон (приміщень) на постійній або тимчасовій основі для всіх, крім спеціально уповноважених співробітників.

Інтервали часу доступу мають на увазі під собою частину доби, під час якої відкривається електронний замок. Використовуються два види інтервалів, які призначаються для кожного дня тижня.

Іноді таких інтервалів декілька.

1. Групові. Застосовуються незалежно для кожного замку і у всій групі контролерів, які мають доступ до нього.

2. Індивідуальні інтервали. Використовуються для роботи з мережевими електронними замками. Призначаються для кожного контролера в залежності від конкретного замка для кожного дня тижня.

Автоматизовані системи контролю доступу починають більш широко застосовуватися в установах, де їх використовують для підвищення безпеки

об'єктів, збереження матеріальних цінностей та інформації, забезпечення дисципліни і порядку.

1.1 Системи контролю доступу у приміщення

На сьогоднішній день існує дуже багато різновидів СКУД різних виробників, а також її компонентів. Не дивлячись на унікальність кожної конкретної системи контролю доступу, вона містить 4 основних елемента: ідентифікатор користувача (карта-пропуск, ключ), пристрій ідентифікації, контроллер, що управляє, і виконавчі пристрої. Загальна схема СКУД показана на рисунку 1.1.

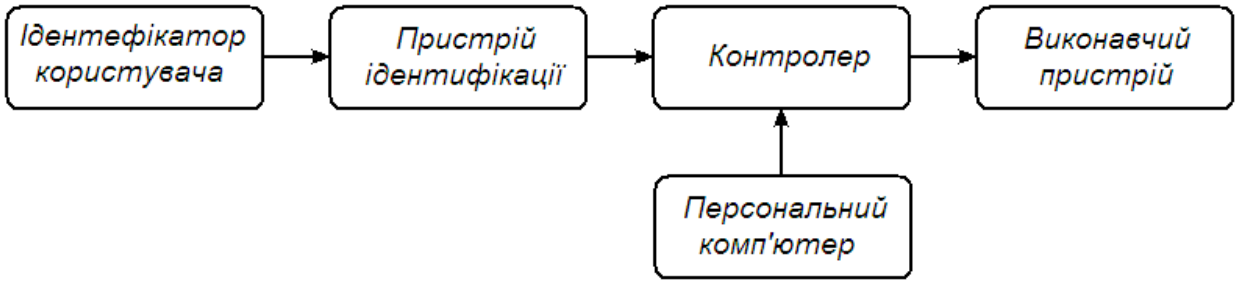


Рисунок 1.1 – Загальна схема СКУД

Системи контролю доступу бувають різній складності [2]. Проста СКУД є мережею електронних замків або автоматичною прохідною.

До СКУД відносяться зчитуватели і контролери, інтерфейсні модулі, програмне забезпечення, безперебійні блоки живлення.

До виконавчих пристроїв СКУД відносяться: електромагнітні замки, клямки ригелів, електроклямки, електромеханічні замки, турнікети, шлагбауми, шлюзи, і ін.

Для управління виконавчими пристроями використовуються кнопки.

Ідентіфікатори з правами доступу, призначеними відповідно до службових повноважень: безконтактні карти, відбитки пальців, смартфони з NFC-модулем.

Доступ розмежовується і за часом: наприклад, співробітники не зможуть попасти в службові приміщення у вихідні дні або після закінчення робочого дня.

Інформація про переміщення співробітників фіксується в системі, яка дозволяє легко визначити хто і де знаходився в заданий період часу.

Для посилення контролю вхід може здійснюватися за допомогою карт доступу із захистом від копіювання, смартфонів, біометричних даних: наприклад, відбитків пальців [2].

Для захисту від входу по чужому ідентифікатору використовується верифікація. Встановивши біля дверей кабінету відеокамеру, можна оперативно проводити порівняння відвідувача з фото власника пропуску з бази даних.

Підсилити контроль доступу в особливо важливі приміщення, наприклад, в серверну або на склад, можна за допомогою режимів «Охорона» і «Ідентифікація». При активованому режимі «Охорона» попасти всередину можна буде лише у присутності співробітника, наділеного відповідними повноваженнями. У режимі «Ідентифікація» доступ можливий лише при підтвердженні ідентифікатором відповідальної особи.

1.1.1 Ідентифікатор користувача

Ідентифікатор користувача - це пристрій або ознака, по якій визначається користувач. Для ідентифікації застосовуються атрибутні і біометричні ідентифікатори. Як атрибутні ідентифікатори використовують автономні носії ознак допуску: магнітні картки, безконтактні проксимити-карти, брелки «тач-мемори», різні радіобрелки, зображення веселкової оболонки ока, відбиток пальця, відбиток долоні, риси обличчя і багато інших фізичних ознак. Кожен ідентифікатор характеризується певним унікальним двійковим кодом. У СКД кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора. В даний час застосовуються [3]:

- безконтактні радіочастотні проксимити-карти (proxmity) - найбільш перспективний в даний час тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціювання, що забезпечує їх стійку роботу і зручність використання, високу пропускну спроможність;

- магнітні карти - найбільш широко поширений варіант. Існують карти з низькокоерцитивною і висококоерцитивною магнітною смугою і із записом на різні доріжки;

- карти Віганда (Wiegand) - названі по імені вченого, який відкрив магнітний сплав, що володіє прямокутною петлею гістерезису;

- кодові для штриха карти - на карту наноситься штриховий код. Існує складніший варіант - штрих-код закривається матеріалом, прозорим лише в інфрачервоному світлі, причитування відбувається в ІЧ-області;

- ключ-брелок «тач-меморі» (touch-memory) - металева пігулка, усередині якої розташований чіп ПЗП.

1.1.2 Контролери обробки інформації

Контролери - пристрої, призначені для обробки інформації від зчитувачів ідентифікаторів, ухвалення рішення і управління виконавчими пристроями. Саме контролери вирішують прохід через пропускні пункти. Контролери розрізняються ємкістю бази даних і буфера подій, обслуговуваних пристроїв ідентифікації [3].

Будь-який контролер СКУД складається з чотирьох основних частин (рис. 1.2): зчитувача, схем обробки сигналу, ухвалення рішення і схеми буфера подій.

Зчитувач карт (пристрій ідентифікації) передає інформацію на схему обробки сигналів контролера.

За способом управління (можливості об'єднання) контролери СКУД діляться на три класи: автономні, мережеві (централізовані) і комбіновані.

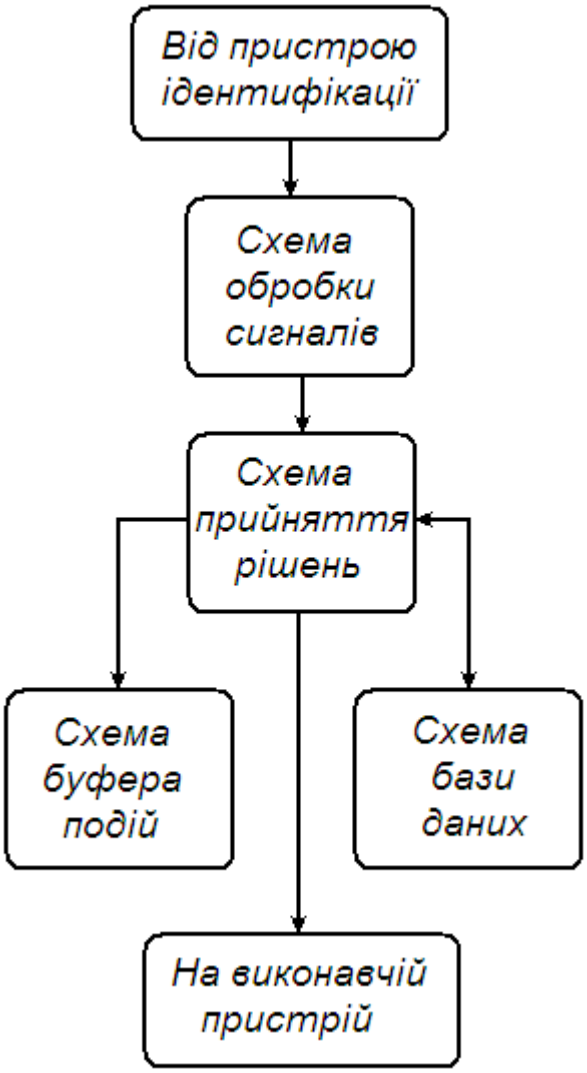


Рисунок 1.2 – Схема контролера СКУД

Незалежно від типа вживаних зчитувачів контролери повинні підтримувати наступні режими доступу:

- по одній карті і пін-коду;
- доступ з підтвердженням оператором;
- контроль кількості людей в приміщенні (мінімум і максимум).

Останнє важливе в ситуаціях коли, наприклад, за умовами служби в заданому приміщенні не повинно залишатися менш одної (двох, трьох) людини.

Основу сучасних СКУД складають автоматичні і автоматизовані. У них процедура перевірки може включати також зіставлення особи що перевіряється з відеопортретом на моніторі контролера. Сучасні автоматичні і авто-

матизовані СКУД залежно від способу управління підрозділяються на автономні, мережеві (централізовані) і розподілені (комбіновані) [3].

Автономні контролери - повністю закінчені пристрої, призначені для обслуговування, як правило, однієї точки проходу. Можливість об'єднання з іншими аналогічними контролерами не передбачена. Існує багато видів таких пристроїв: контролери, поєднані з зчитувачем, контролери, вбудовані в електромагнітний замок і так далі

У автономних контролерах застосовуються зчитувачі самих різних типів. Як правило, автономні контролери розраховані на обслуговування невеликого числа користувачів, звичайні не більше 500 чоловік. Вони працюють з одним виконавчим пристроєм без передачі інформації на центральний пункт охорони і без контролю з боку оператора. Прикладом подібної системи контролю доступу може служити досить проста комбінація: «електромагнітний замок і зчитувач карт ідентифікації». Якщо необхідно контролювати лише одну двері і в майбутньому розширення системи контролю доступу не планується, це оптимальне і досить недороге рішення.

1.1.3 Пристрої ідентифікації

Для ідентифікації особи сучасні електронні системи контролю доступу використовують пристрої декількох типів залежно від вживаного вигляду ідентифікатора користувача. У літературних джерелах, присвячених опису різних СКУД, часто можна зустріти підміну поняття аутентифікація, поняттям верифікація [3].

Пристрої ідентифікації (зчитувачі) розшифровують інформацію, записану на картках або ключах інших типів, і передають її в контролер частіше у вигляді цифрової послідовності. Зчитувачі карток доступу можуть бути контактні і безконтактні (рис. 1.3). Можливі наступні способи введення ознак:

- ручний, здійснюваний шляхом натиснення клавіш, повороту перемикачів і т. д.;



Рисунок 1.3 – Ідентифікатор зчитування інформації

- контактний - в результаті безпосереднього контакту між зчитувачем і ідентифікатором;

• дистанційний (безконтактний) при піднесенні ідентифікатора до зчитувача на певну відстань.

Для знімання інформації про біологічні ознаки людини використовують спеціальні біометричні зчитувачі (термінали), а введення пін-коду здійснюється з клавіатур різних типів

Зчитувачі можуть використовуватися не лише для контролю доступу, але і для обліку робочого часу співробітників. Пред'являючи ідентифікатор зчитувателю, співробітники одночасно відмічають час приходу на роботу і відходу з неї. Для обліку робочого часу також може застосовуватися спеціальний термінал LICON. LICON не лише реєструє події, але і показує співробітникові час його входу/виходу, інформує про порушення графіка або некоректні пред'явлення карти.

Для ідентифікації особи сучасні електронні СКУД використовують пристрої декількох типів. Найбільш поширеними є:

- кодонаборні пристрої пін-коду (кнопкові клавіатури);

- зчитувачі безконтактних смарт-карт (інтерфейс Віганда);

- зчитувачі проксиміті-карт;

- зчитувачі ключа «тач-меморі»;

- зчитувачі штрих-коду;

- біометричні зчитувачі.

В даний час найширшого поширення набули всілякі зчитувачі карт (проксиміті, Віганда, з магнітною смугою і тому подібне). Вони мають свої безперечні переваги і зручності у використанні, проте при цьому в автоматизованому пункті доступу контролюється «прохід картки, а не людини». В той же час картка може бути втрачена або вкрадена зловмисниками. Все це знижує можливість використання СКУД, заснованих виключно на зчитувачах карт, в додатках з високими вимогами до рівня безпеки. Незрівнянно вищий рівень безпеки забезпечують всілякі біометричні пристрої контролю доступу, біометричні параметри людини (відбиток пальця, геометрія руки, малюнок сітківки ока і т. п.), що використовують ідентифікуючі ознаки, які однозначно надають доступ лише певній людині. На сьогоднішній день подібні пристрої все ще залишаються досить дорогими і складними, і тому знаходять своє вживання лише в особливо важливих пунктах доступу [3].

Зчитувачі штрих-коду в даний час практично не встановлюються, оскільки підроблювати пропуск надзвичайно просто на принтері або на копіювальному апараті.

Розглянемо принципи роботи і використання представлених пристроїв ідентифікації.

Кодонаборні пристрої (клавіатури) є досить простими і недорогими пристроями із зрозумілим і таким, що легко сприймаються різними категоріями користувачів інтерфейсом. Принцип дії кнопкових клавіатур досить ясний: якщо набраний на клавіатурі код доступу вірний, то прохід на територію, що захищається, дозволений.

Клавіатури СКУД можна вважати «псевдобіометричними» пристроями СКУД, оскільки носієм пін-коду є пам'ять людини. Відповідальність за його збереження і використання неповноважною особою покладається на користувача СКУД. Тим самим використання клавіатур контролю доступу робить користувача СКУД активним учасником програми безпеки. При цьому, оскільки носієм коду є людина, необхідно розглянути можливість введення пін-

коду користувачем під загрозою йому або його близьким (що відноситься і до використання карт або біометричних зчитувачів). У випадку з клавіатурами користувач СКУД може бути забезпечений так званим «кодом під вимогою» (найчастіше це додаткова цифра, що вводиться після основного коду), при використанні якого доступ надається, але при цьому на пости (станції) охорони подається сигнал тривоги. Проте, не дивлячись на всі свої безперечні достоїнства, переважна більшість клавіатур СКУД мають один серйозний недолік - пін-код, що вводиться з них, може бути легко перехоплений як людиною, що стоїть рядом, так і зловмисником, що знаходиться на видаленні і озброєним пристроями візуального знімання інформації [3].

Для підвищення рівня безпеки контролю доступу може використовуватися подвійна технологія, що має на увазі спільне використання клавіатури для введення пін-коду і зчитувача якого-небудь типу (залежно від необхідного рівня забезпечення безпеки і фінансових або організаційних обмежень). Проте подібне рішення ускладнює процедури використання СКУД, є дорожчим у виконання і складнішим в обслуговуванні. У зв'язку з цим розглянемо можливості захисту пін-коду, який вводиться, безпосередньо на клавіатурі.

Перший варіант - передбачити такий спосіб установки клавіатури, при якому можливість побачити пін-код, що набирає користувачем, буде якщо не виключена повністю, то мінімізована. Цей результат також може бути досягнутий використанням різних екранів, що прикривають цифри на клавіатурі. При цьому таке рішення не може бути оптимальним, оскільки інколи немає можливості сильно варіювати місце розташування клавіатури або її зовнішній вигляд. Існує ще одна загроза - тільки що введений пін-код може бути знятий з кнопок клавіатури зловмисником за допомогою спецзасобів.

Ширші можливості надають не кнопкові клавіатури з нанесеними цифрами, а з електронним кодонаборним пристроєм, що використовує для відображення інформації світлодіодні індикатори. В цьому випадку для захисту від підглядання пін-коди, що вводиться, можуть бути застосовані поляризаційні фільтри, що обмежують кут огляду, при якому можна розрізнити циф-

ри, що відображуються на клавіатурі. Наступна перевага подібних кодонаборних пристроїв полягає в тому, що цифри, що відображуються на клавіатурі, не прив'язані до певного місця розташування. Використовуючи ефект скремблювання (змішування), можна добитися того, що при кожному використанні клавіатури цифри розташовуватимуться в новому, випадковому порядку. А якщо цифри спалахуватимуть лише при активації клавіатури користувачем і гаснутимуть відразу після введення пін-коду, то зняття тільки що введеного пін-коду стане неможливим.

Усі розглянуті методики захисту пін-коду на етапі введення знайшли своє вживання в сучасних кодонаборних пристроях високозахищених систем контролю і управління доступу. Для захисту від перехоплення інформації, зрадженої по лініях зв'язку між пристроєм контролю доступу і пристроєм СКУД, що управляє, використовуються шифрування даних, циркулюючих в системі, інші безпечні способи передачі інформації і контроль за несанкціонованим підключенням до ліній зв'язку [3].

1.1.4 Виконавчі пристрої

Серед виконавчих пристроїв контролю доступу найбільш розповсюджені наступні замочні або керовані перегороджуючи пристрої: замки, клямки, турнікети (поясні, повноростні, «квиткові», розсувні, які обертаються, шлюзові кабіни (тамбурного типу, ротанги, шлагбауми), автоматичні ворота (орні ворота, ворота які зрушуються, ворота які складаються, ролетні ворота), ліфти.

Електричні замки рекомендується використовувати як основний замикаючий пристрій в денний час. Ці замки на відміну від механічних відкриваються дистанційно по електричному сигналу і використовуються спільно з домофонами, кодовими панелями, зчитувачами карток різних типів. Електрозамки діляться на два класи: електромагнітні і електромеханічні [2].

Електромагнітні замки є корпусом з електромагнітом і у відповідь металевою пластиною. Пластина кріпиться на дверному полотні, а сам замок - на косяці. Електромагнітний замок утримує двері в закритому стані за рахунок зусилля потужного електромагніту. При знеструмленні замку двері залишаються відкритими, тому для забезпечення роботи в умовах відключення напруги живлення необхідно застосовувати блоки гарантованого живлення.

Електромеханічний замок має механічний ригель (засув), що утримує двері в закритому стані, а управління цим ригелем здійснюється відносно малопотужним соленоїдом. При закритті дверей ригель замку зводить присутню в замку пружину, при цьому робочий ригель входить у відповідну частину замку і утримує двері в закритому стані. При подачі напруги соленоїд відпускає фіксатор пружини і робочий ригель, під дією пружини, втягується в замок - двері можуть бути відкриті. Після того, як двері будуть відкриті, а потім закриті, вони знов виявляться в замкнутому стані. Передбачається режим, який виключає автоматичне замикання замків і випадкове закривання дверей.

У соленоїдних електрозамках ригель наводиться в рух зусиллям електромагніту. Обладнана таким замком двері можуть бути відкриті лише в період дії сигналу, що управляє. Після зняття цього сигналу закриті двері залишаться замкнутими незалежно від того, чи відкривалася вони.

Існують також інші різновиди електромеханічних замків: електромотори (ригель наводиться в рух електромотором з редуктором), з ручним приводом ригеля (ригель наводиться в рух поворотом ручки, а електромагніт розблоковує механізм приводу). Електромеханічні замки можуть бути накладного і врізного типів.

Електроклямки являються відповідною частиною замку і використовуються спільно із звичайним механічним замком. При подачі напруги, що управляє, розблоковується фіксатор електроклямки, і двері можуть бути відкриті при висунутому положенні ригеля механічного замку. При цьому використовуваний механічний замок не повинен відкриватися зовні поворотом ручки. За наявності ручки з внутрішньої сторони дверей вона може бути від-

крита зсередини поворотом ручки без подачі напруги, що управляє, на клямку. Спеціальні моделі соленоїдних замків і електроклямок призначені для устаткування аварійних виходів. Такі замки відкриваються при відключення напруги живлення.

При виборі моделі замку необхідно враховувати, які приміщення і для яких цілей передбачається обладнати замком. При цьому необхідно враховувати: масу, конструкцію, матеріал дверей, необхідну інтенсивність використання, різні функціональні особливості системи, що включає замок. Все це визначає надійність і довговічність роботи електрозамку.

Доводчики дверей служать для примусового закривання дверей і забезпечують надійну роботу електрозамків. Регулюючі клапани дозволяють вибрати необхідну швидкість закривання дверей. Для дверей різного розміру можна підібрати відповідний доводчик. Моделі також відрізняються конструктивного виконання, дизайну, ряду додаткових функцій: фіксація дверей в положенні «відкрито», прискорення в завершуючій фазі закривання - «плескання» і ін.

1.2 Кодонаборні кнопкові клавіатури

Розрізняють два типи клавіатур: що кодують і що не кодують. У клавіатурах першого типа при натисненні на клавішу, схемою контролера клавіатури, формується відповідний цій клавіші код. До даного типа належать комп'ютерні клавіатури, зокрема клавіатура IBM PC AT. У керівних мікроконтролерних системах використовуються прості і дешеві некодуючі клавіатури, які являють скановану матрицю кнопок. Вироджений варіант матриці – один рядок або стовпець утворює позиційний код, де кожній кнопці відповідає свій розряд [4].

Сигнал за допомогою кнопкових перемикачів формується шляхом замикання – розмикання ними електричного кола (рис. 1.4).

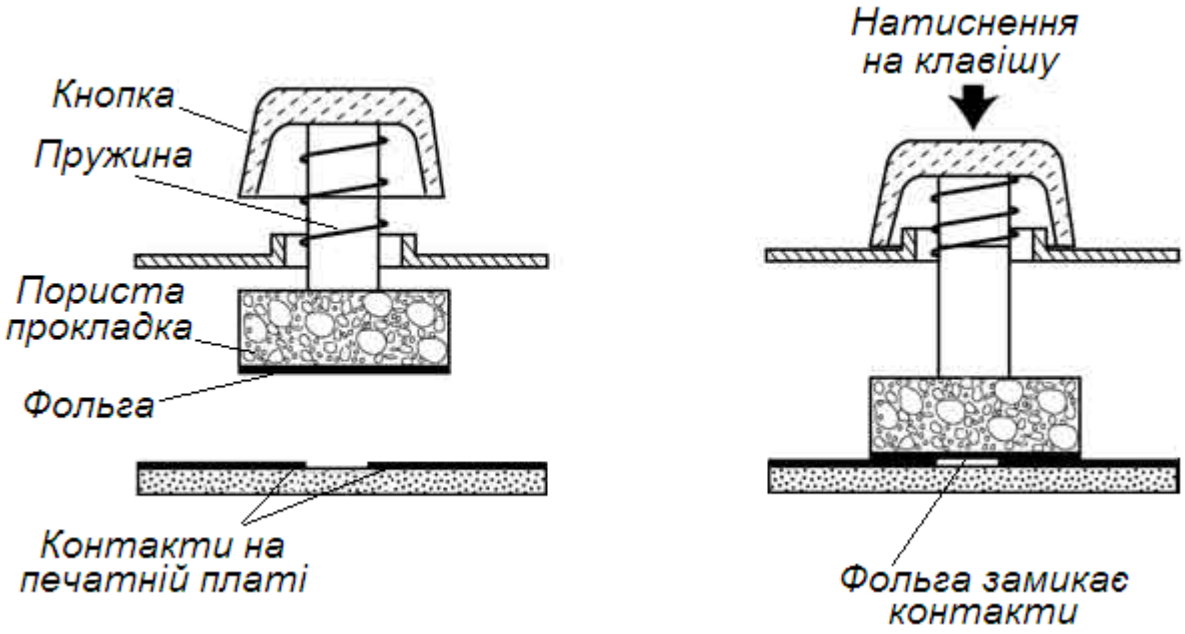


Рисунок 1.4 - Методи здобуття електричного контакту у кодонаборних клавіатурах

При натисненні клавіші фольга замикає печатні контакти на платі. Коли клавіша відпускається, пружина повертає її у вихідне положення. При цьому пориста прокладка пом'якшує удар, але клавіатура стає дуже “м'якою”. Основний недолік цієї конструкції – відсутність клацання при натисненні (немає зворотного зв'язку), тому в системах з такою клавіатурою часто доводиться програмним чином виводити на вбудований динамік які-небудь звуки, що свідчать про наявність контакту. Клавіатура чутлива до корозії фольги і забруднення контактів на печатній платі.

Клавіатура з гумовими ковпачками схожа на попередню конструкцію, але перевершує її у багатьох відношеннях. Замість пружини в ній використовується гумовий ковпачок із замикаючою вставкою з тієї ж гуми, але з вугільним наповнювачем. При натисненні клавіші шток натискає на гумовий ковпачок, деформуючи його. Деформація ковпачка спочатку відбувається пружно, а потім він “провалюється”. При цьому вугільний наповнювач замикає провідники на печатній платі. При відпусканні гумовий ковпачок набуває первинної форми і повертає клавішу у вихідний стан.

Замикаючі вставки робляться з очищеного вугілля, тому вони не схильні до корозії і самі по собі очищають металеві контакти, до яких притискаються. Ковпачки зазвичай пресуються всі разом у вигляді листів гуми, що покривають плату цілком і що захищають її від пилу, грязі і вологи. Кількість деталей в такій конструкції мінімальна. Все це забезпечує високу надійність клавіатури і її широке поширення.

Мембранна клавіатура є різновидом попередньої, але в ній немає окремих клавіш: замість них використовується аркуш з розміткою, який укладається на пластину з гумовими ковпачками. Мембранні клавіатури часто використовуються в пультах управління (верстатами, агрегатами і тому подібне), тобто там, де необхідно вводити великі об'єми даних.

Покращеним варіантом електромеханічних контактів є геркони – герметизовані контакти, що розташовуються в герметичному скляному балоні. Спрацьовування відбувається при дії на контакти магнітного поля від маленького магніта або електромагнітної котушки.

У безконтактних клавішах використовуються перемикачі, керовані магнітним полем, світловим випромінюванням, або дією від індукційних датчиків. До безконтактних відносяться і сенсорні перемикачі.

Формування кодових сигналів виконується в кодуючих пристроях. Додатковими функціями кодуючого пристрою є: формування сигналу «Гот.» (готовність) для управління перезаписом сформованого коду, блокування роботи при одночасному натисненні декількох клавіш і захист від брязкоту.

Кодуючий пристрій, функціональна схема якого показана на рисунку 1.5, містить: клавіатуру введення (КЛ); блок кодування (БК); вузол захисту і формування вихідних сигналів (ВФС) (знак n на шині показує число ліній в цій шині). Найбільшого поширення набули комбінаційні кодуючи пристрої і пристрої із сканованою клавіатурою. Перевагами пристрою із сканованою клавіатурою, в порівнянні з комбінаційними, є: менші апаратурні витрати, скорочення міжелементних зв'язків, наявність захисту від формування помилкового коду, при одночасному натисненні декількох клавіш клавіатури.

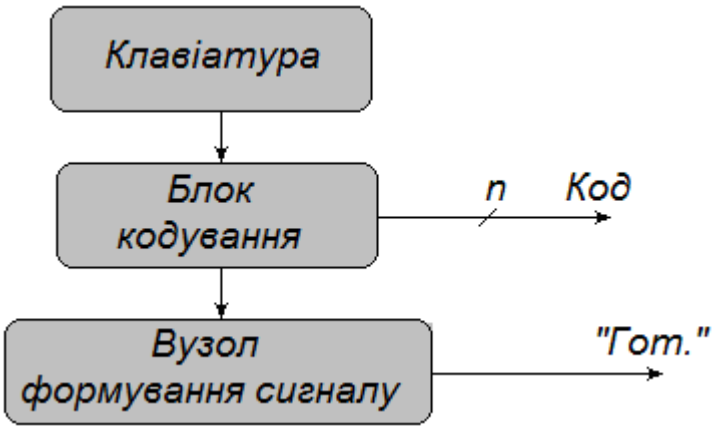


Рисунок 1.5 – Структурна схема кодуючого пристрою

Метою роботи являється розробка системи електричного запобігання проникненню у приміщення підвищеної надійності.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- забезпечити відкриття електромагнітного замка натисканням трьох кнопок коду у відповідній послідовності;

- забезпечити економічну схемотехніку пристрою для підвищення надійності при виконанні функцій запобігання проникнення у приміщення.

- забезпечити підвищення секретності кодового замка підрахунком кількості натискань кодових кнопок.

2 Розробка системи контролю і управління доступом у приміщення

Електронний замок – електронний пристрій, призначений для того, щоб запобігти доступу в приміщення сторонніх осіб, або навпаки, обмежити вихід з приміщення. Рішення про доступ осіб в приміщення приймається на основі сигналів від різних датчиків: зчитувачів магнітних карт, штрих-коду, датчиків контактної пам'яті, біометричних датчиків, набірної клавіатури, комбінаторних флуоресцентних молекулярних датчиків, дистанційного керування і т.д. Часто є частиною складної електронної системи контролю доступу, інколи невідємні від неї. Як виконавчі механізми використовуються електромеханічні і електромагнітні замочні пристрої.

Звичайні механічні замки мають невисоку міру захисту через обмежене число комбінацій. Також можлива втрата ключа або зняття з нього зліпка. Електронні кодові замки дозволяють забезпечити індивідуальний або колективний доступ в приміщення, до устаткування, сейфів і інших об'єктів без вживання традиційних механічних замків і ключів.

У електронних кодових замках, як і в механічних, часто використовують принцип збігу ознак. Вочевидь, що найбільш простий і, відповідно, гранично надійною схемою збігів є задана користувачем послідовність включення елементів комутації.

Доступ у приміщення здійснюється відкриттям електромагніту замка, згідно з набором відомого обмеженому колу осіб коду. Код складається з 3 цифр (з 10 можливих). Кнопки з певними цифрами необхідно натиснути в заданій послідовності. Це дозволяє отримати 10! = 3628800 комбінацій можливих варіантів коду. Код легко і оперативно можна змінити, переставивши роз’ємні контакти кнопок в будь-якій послідовності. При установці коду небажано займати цифри послідовного ряду (1, 2, 3). Краще, якщо код буде складатися з цифр врозкид, наприклад: 6, 2, 5.

Функціональна схема електричного запобігання проникненню у приміщення представлена на рисунку 2.1.

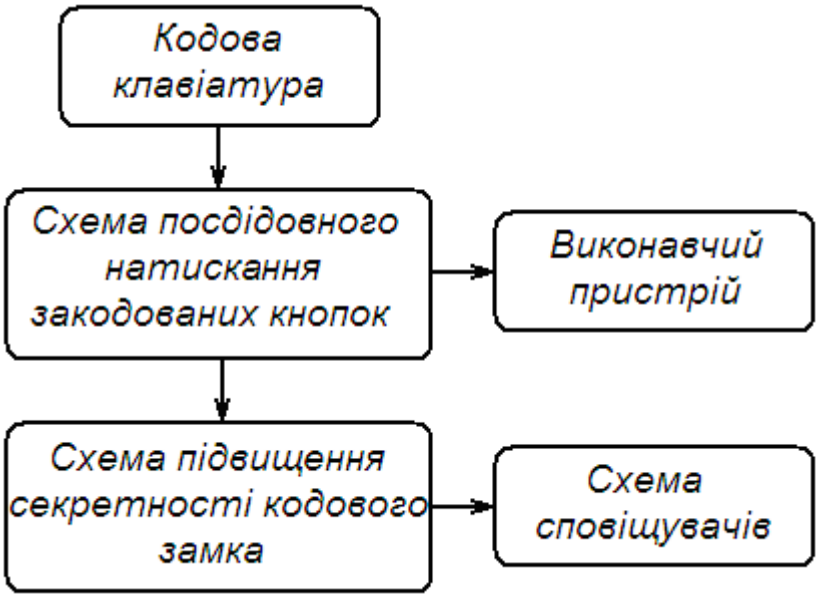


Рисунок 2.1 - Функціональна схема електричного запобігання проникненню у приміщення

2.1 Розрахунок алгоритму функціонування кодової клавіатури

Кодові панелі призначені для управління (розблокування) електромагнітними замками за допомогою набору загального і індивідуального цифрового чотиризначного коду. Панелі встановлюються в службові, житлові і виробничі приміщення і будівлі як система обмеження доступу.

Розрізняють два типи клавіатур: кодуючі і некодуючі. У клавіатурах першого типа при натисненні на клавішу, схемою контролера клавіатури формується відповідний цій клавіші код. До даного типа належать комп'ютерні клавіатури, зокрема клавіатура IBM PC AT. У керуючих мікроконтролерних системах використовуються прості і дешеві некодуючі клавіатури, які являються сканованою матрицею кнопок. Вироджений варіант матриці – один

рядок або стовпець утворює позиційний код, де кожній кнопці відповідає свій розряд.

Сигнал за допомогою кнопкових перемикачів формується шляхом замикання – розмикання ними електричного кола.

У сучасних клавіатурах використовується декілька типів клавіш. У більшості клавіатур встановлені механічні перемикачі, в яких відбувається замикання електричних контактів при натисненні клавіш. У деяких клавіатурах високого класу використовуються безконтактні ємнісні датчики.

Найширше поширені контактні клавіатури. Існують наступні їх різновиди: з механічними перемикачами; із замикаючими накладками; з гумовими ковпачками; мембранні.

У чисто механічних перемикачах відбувається замикання металевих контактів. У них для створення “дотикового” зворотного зв'язку встановлюється додаткова конструкція з пружини і пом'якшувальної пластинки. При цьому відчувається опір клавіші і чутне клацання.

Механічні перемикачі дуже надійні, їх контакти зазвичай самоочищаються. Вони витримують до 20 мільйонів спрацьовувань і стоять другими по довговічності після ємкісних датчиків. Клавіатури з механічними перемикачами, не дивлячись на свою довговічність і тактильний зворотний зв'язок, набули значно меншого поширення, ніж мембранні клавіатури.

У клавішах із замикаючими накладками прокладка з пористого матеріалу з приклеєною знизу фольгою з'єднується з кнопкою клавіші (рис. 2.2).

При натисненні клавіші фольга замикає печатні контакти на платі. Коли клавіша відпускається, пружина повертає її у вихідне положення. При цьому пориста прокладка пом'якшує удар, але клавіатура стає дуже “м'якою”. Основний недолік цієї конструкції – відсутність клацання при натисненні (немає зворотного зв'язку), тому в системах з такою клавіатурою часто доводиться програмним чином виводити на вбудований динамік комп'ютера якінебудь звуки, що свідчать про наявність контакту. Клавіатура чутлива до корозії фольги і забруднення контактів на печатній платі.

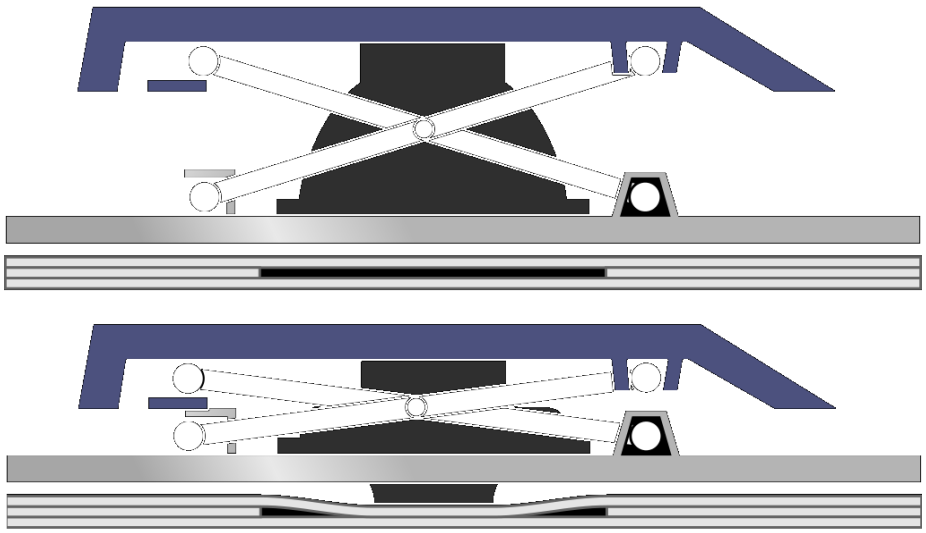


Рисунок 2.2 – Конструкція механізму ножничного типа з накладкою з фольги, яка замикає

Клавіатура з гумовими ковпачками схожа на попередню конструкцію, але перевершує її у багатьох відношеннях. Замість пружини в ній використовується гумовий ковпачок із замикаючою вставкою з тієї ж гуми, але з вугільним наповнювачем. При натисненні клавіші шток натискає на гумовий ковпачок, деформуючи його. Деформація ковпачка спочатку відбувається пружно, а потім він “провалюється”. При цьому вугільний наповнювач замикає провідники на печатній платі. При відпусканні гумовий ковпачок набуває первинної форми і повертає клавішу у вихідний стан.

Замикаючі вставки робляться з очищеного вугілля, тому вони не схильні до корозії і самі по собі очищають металеві контакти, до яких притискаються. Ковпачки зазвичай пресуються всі разом у вигляді листів гуми, що покривають плату цілком і що захищають її від пилу, грязі і вологи. Кількість деталей в такій конструкції мінімальна. Все це забезпечує високу надійність клавіатури і її широке поширення.

Мембранна клавіатура є різновидом попередньої, але в ній немає окремих клавіш: замість них використовується аркуш з розміткою, який укладається на пластину з гумовими ковпачками. Мембранні клавіатури часто використовуються в пультах управління (верстатами, агрегатами і тому подібне), тобто там, де необхідно вводити великі об'єми даних.

Покращеним варіантом електромеханічних контактів є геркони – герметизовані контакти, що розташовуються в герметичному скляному балоні. Спрацьовування відбувається при дії на контакти магнітного поля від маленького магніта або електромагнітної котушки.

У безконтактних клавішах використовуються перемикачі, керовані магнітним полем, світловим випромінюванням, або дією від індукційних датчиків. До безконтактних відносяться і сенсорні перемикачі.

Формування кодових сигналів виконується в кодуючих пристроях. Додатковими функціями кодуючого пристрою є: формування сигналу «Гот.» (готовність) для управління перезаписом сформованого коду, блокування роботи при одночасному натисненні декількох клавіш і захист від брязкоту.

Кодуючий пристрій, функціональна схема якого показана на рисунку 2.3, містить: клавіатуру введення (КЛ); блок кодування (БК); вузол захисту і формування вихідних сигналів (ВФС) (знак n на шині показує число ліній в цій шині). Найбільшого поширення набули комбінаційні кодуючи пристрої і пристрої із сканованою клавіатурою.

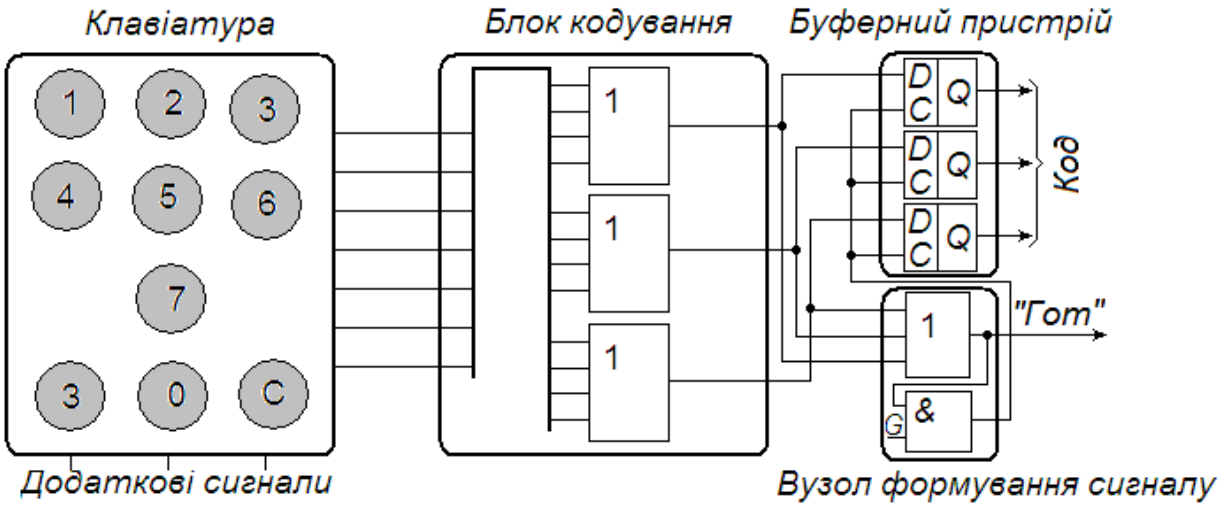


Рисунок 2.3 – Структурна схема кодуючого пристрою

Комбінаційний кодуючий пристрій побудовано по схемі неприоритетного шифратора, який здійснює перетворення десяткового номера активного входу в двійковий еквівалент цього номера. Клавіатура з 10 клавіш формує 10 двійкових чотирьохрозрядних кодів (табл. 2.1).

Таблиця 2.1 - Таблиця істинності кодуючого блоку «10 в 4»

Входи	Виходи			
SA_i	F4	F3	F2	F1
SA0	×	×	×	×
SA1	0	0	0	1
SA2	0	0	1	0
SA3	0	0	1	1
SA4	0	1	0	0
SA5	0	1	0	1
SA6	0	1	1	0
SA7	0	1	1	1
SA8	×	×	×	×
SA9	×	×	×	×

Рівняння функціонування шифратора:

$$F1 = SA1 + SA3 + SA5 + SA7 + SA9;$$

$$F2 = SA2 + SA3 + SA6 + SA7;$$

$$F3 = SA4 + SA5 + SA6 + SA7.$$

Блок кодування створюють три чотирьохвходових елемента АБО (рис. 2.4).

У загальному випадку, при використанні двійкового коду, можна закодувати 2^n вхідних сигналів. У розглянутій вище схемі вихідний код «0000» присутній на виході при подачі сигналу на вхід SA0, а також у разі, якщо вхідний сигнал взагалі не подається ні на один з входів. Для однозначної ідентифікації сигналу SA0 в схемі формується ще один вихідний сигнал – ознака подачі вхідного сигналу (×), який використовується і для інших цілей. Клавіші SA8 та SA9 використовуються для скидання інформації та примусового відкриття електромагнітного замка. Вузол формування сигналу «Готовий» включає елемент АБО DD4 та елемент І DD5. З «натисканням» будь-якої з клавіш клавіатури введення інформації вихідні сигнали з елементів DD1-DD3 утворюють відповідний трьохрозрядний код.

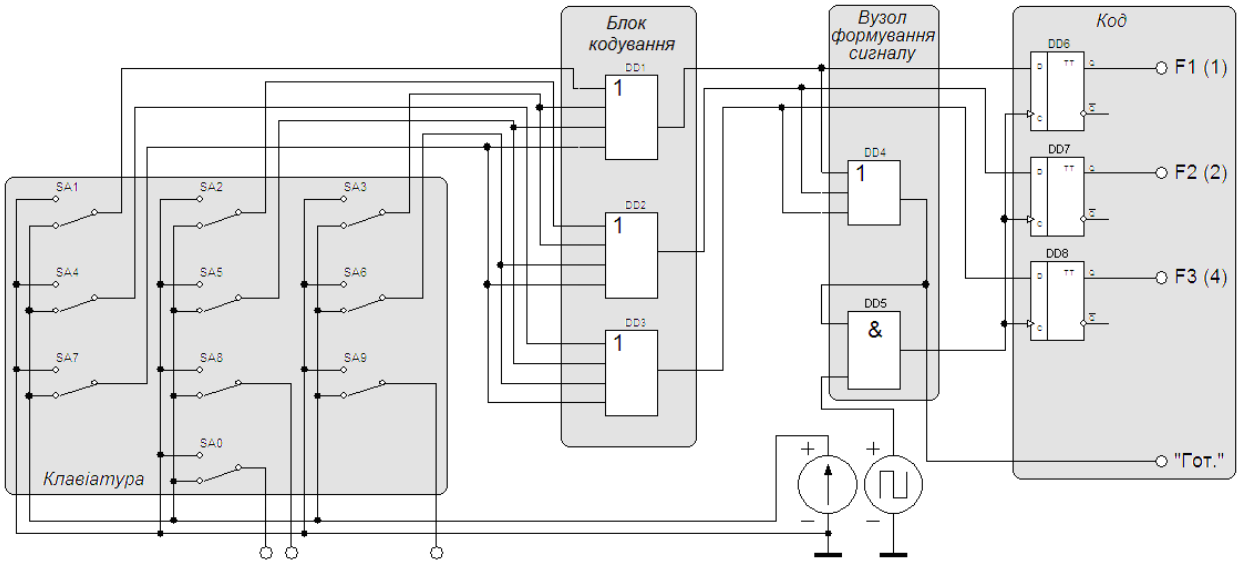


Рисунок 2.4 – Комбінаційний кодуючий пристрій

Формується сигнал «Готовий» з виходу елемента 3-АБО на якому відтворюється логічна «1». Цей сигнал дозволяє проходження імпульсів генератора скрізь елемент 2-І на тактові входи елементів буферного регістра на D-тригерах DD6-DD8. Якщо відповідна клавіша віджата на виході елемента 3-АБО формується логічний «0». Відсутній сигнал «Готовий» та блокується прходження імпульсів генератора скрізь елемент 2-І. На виході буферного регістра зберігається код раніш натиснутої клавіши. З натисканням наступної клавіши процес формування вихідного коду повторюється.

2.2 Схема послідовного натискання закодованих кнопок

Програмована клавіатура розроблена для видаленого управління окремими зонами (шлейфами) центральних блоків охоронної сигналізації, а також для управління доступом в приміщення.

Можливості розробленої клавіатури:

- цифрове електронне управління;

- повна сумісність з блоками схеми електричного запобігання проникненню у приміщення;

- захист всіх кодів і установок при втраті живлення;

- трьохрозрядні програмовані коди доступу;

- два релейних виходи - основний і допоміжний;

- три світлодіода індикації стану контактів реле або зовнішніх пристроїв;

- вбудована клавіша тривоги;

Є два програмовані режими роботи: режим внутрішньої індикації і режим зовнішньої індикації. У режимі внутрішньої індикації світлодіоди показують наявність живлення і стан реле; у режимі зовнішньої індикації світлодіоди відображають стан зовнішніх пристроїв.

2.2.1 Генератор числових послідовностей на регістрі зсуву

Перевагою генераторів даного типу є використання регістра зсуву, побудованого з однотипних тригерів, завдяки чому істотно спрощується схемотехнічне проектування генератора. В такий спосіб можна реалізувати генератори циклічних послідовностей чисел, в яких кожне подальше число утворюється шляхом зсуву попереднього числа, записаного в регістрі, на один розряд і введенням в перший розряд, що звільнився, 0 або 1. Для цього до входу першого розряду регістра підключається комбінаційна схема, що створює необхідний управляючий сигнал. Якщо є n-розрядний регістр зсуву, то можна генерувати циклічні послідовності завдовжки L_n.

Проведемо структурне проектування генератора коду відкриття електромагнітного замка системи контролю і управління доступом у приміщення.

Проектування такого генератора по звичайній методиці проектування недвійкових лічильників зажадало б в два рази більше лічильників і додаткової логіки.

Синтез структури генераторів послідовностей на регістрах зсуву в першу чергу полягає в знаходженні вигляду функцій входів.

Код відкриття електромагнітного замка 6-2-5.

Складемо таблицю переходів станів розрядів генератора (табл. 2.2).

Таблиця 2.2 – Таблиця станів генератора

x^n	Q_3^n	Q_2^n	Q_1^n	Q_3^{n+1}	Q_2^{n+1}	Q_1^{n+1}
6	1	1	0	0	1	0
2	0	1	0	1	0	1
5	1	0	1	1	1	0

Складемо карти Карно для функцій переходів тригерів кожного розряду (рис. 2.5).

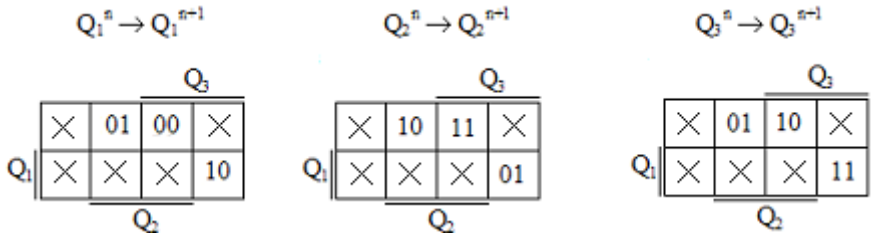


Рисунок 2.5 – Карти функцій переходів тригерів генератора

Зазвичай, в зрухових регістрах використовуються D-тригери (рис. 2.6).

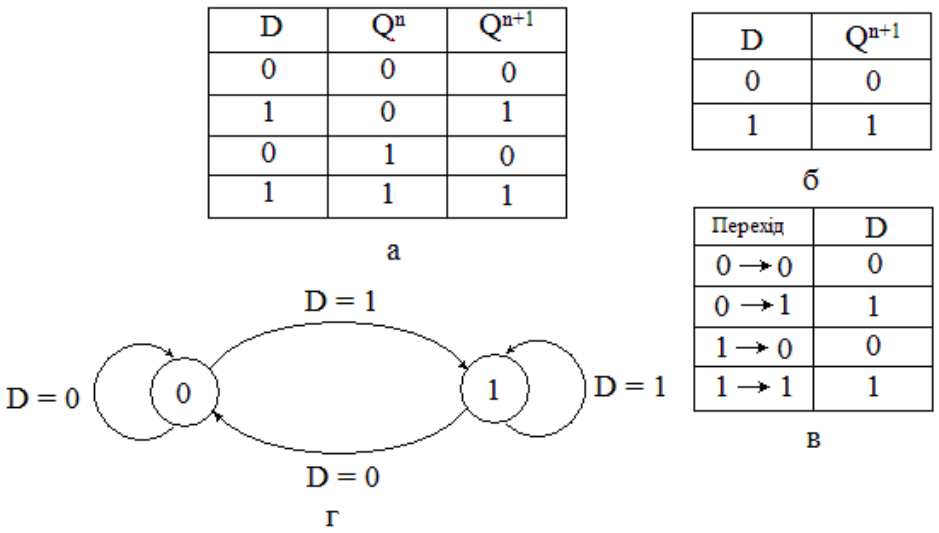


Рисунок 2.6 – Таблиця істинності (а), таблиця перемикань (б), словник переходів (в), діаграма станів (г) D-тригера

Використовуючи словник переходів D-тригера, для кожного входу тригера складаються карти Карно, в клітках яких проставляються сигнали, необхідні для забезпечення переходів тригерів, вказаних в однойменних клітках карт функцій переходів (рис. 2.7).

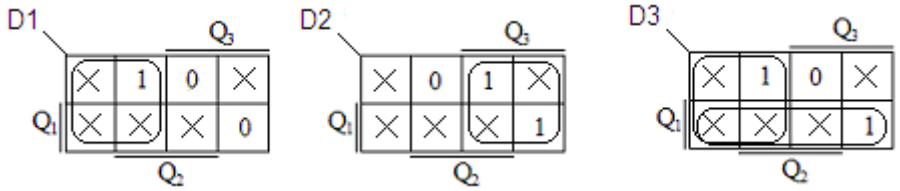


Рисунок 2.7 – Карти Карно функцій входів тригерів генератора

Проведемо мінімізацію логічних функцій входів в картах Карно з метою здобуття їх аналітичних вистав.

В результаті виходять наступні функції входів тригерів генератора:

$$D1 = \overline{Q_3};\ D2 = Q_3;\ \ D3 = \overline{Q_3} + Q_1.$$

Складання логічної схеми генератора виконується побудовою управляючої комбінаційної схеми, яка реалізовує функцію входів, і її підключенням до входу першого розряду зрухового регістра (рис. 2.8)

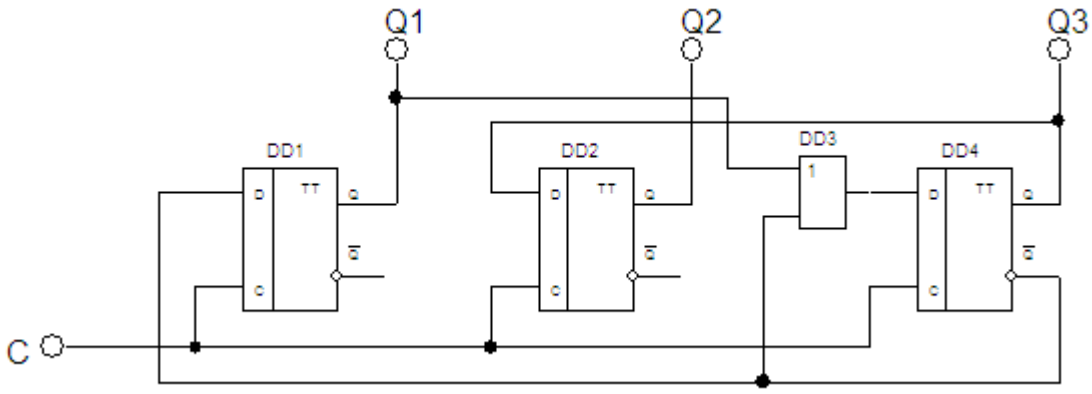


Рисунок 2.8 – Логічна схема генератора послідовності на основі регістра зрушення

Проведемо аналіз функціонування схеми у програмному забезпеченні Electronics Workbench (рис. 2.9).

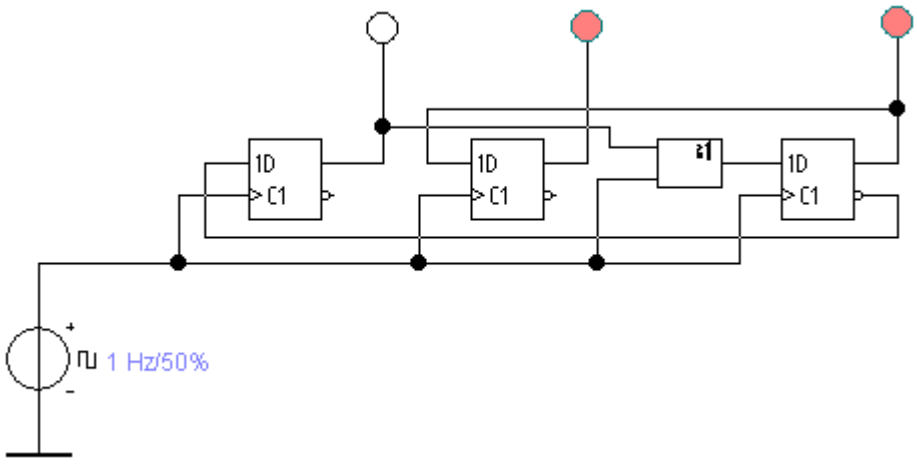


Рисунок 2.9 - Аналіз функціонування схеми генератора послідовності на основі регістра зрушення

Аналіз функціонування схеми показує, що на основі регістрів зрушення утворюються лише циклічні послідовності чисел. Для реалізації будь-яких нециклічних послідовностей потрібне використання додаткових комбінаційних перетворювачів коду, які включаються на входах тригерів паралельно – послідовного регістра.

2.2.2 Паралельно – послідовний регістр для зберігання і перетворення закодованої інформації

У паралельно – послідовному регістрі запис інформації відбувається в паралельному коді, а зчитування в послідовному. На рисунку 2.10 показаний варіант побудови такого регістра на D – тригерах для кодової послідовності натиснутих кнопок 6-2-5.

Код натиснутої кнопки у прямому (якщо одиниця) або інверсному (якщо нуль) вигляді поступає на елементи DD4-DD6. Туди ж приходять сигнали логічної одиниці від натиснутих кнопок 6-2-5 у заданому порядку. Інформація записується послідовно у тригери DD10-DD12 імпульсами генератора через елементи DD7-DD9. З виходу тригера DD12 сигнал поступає на виконавчий пристрій.

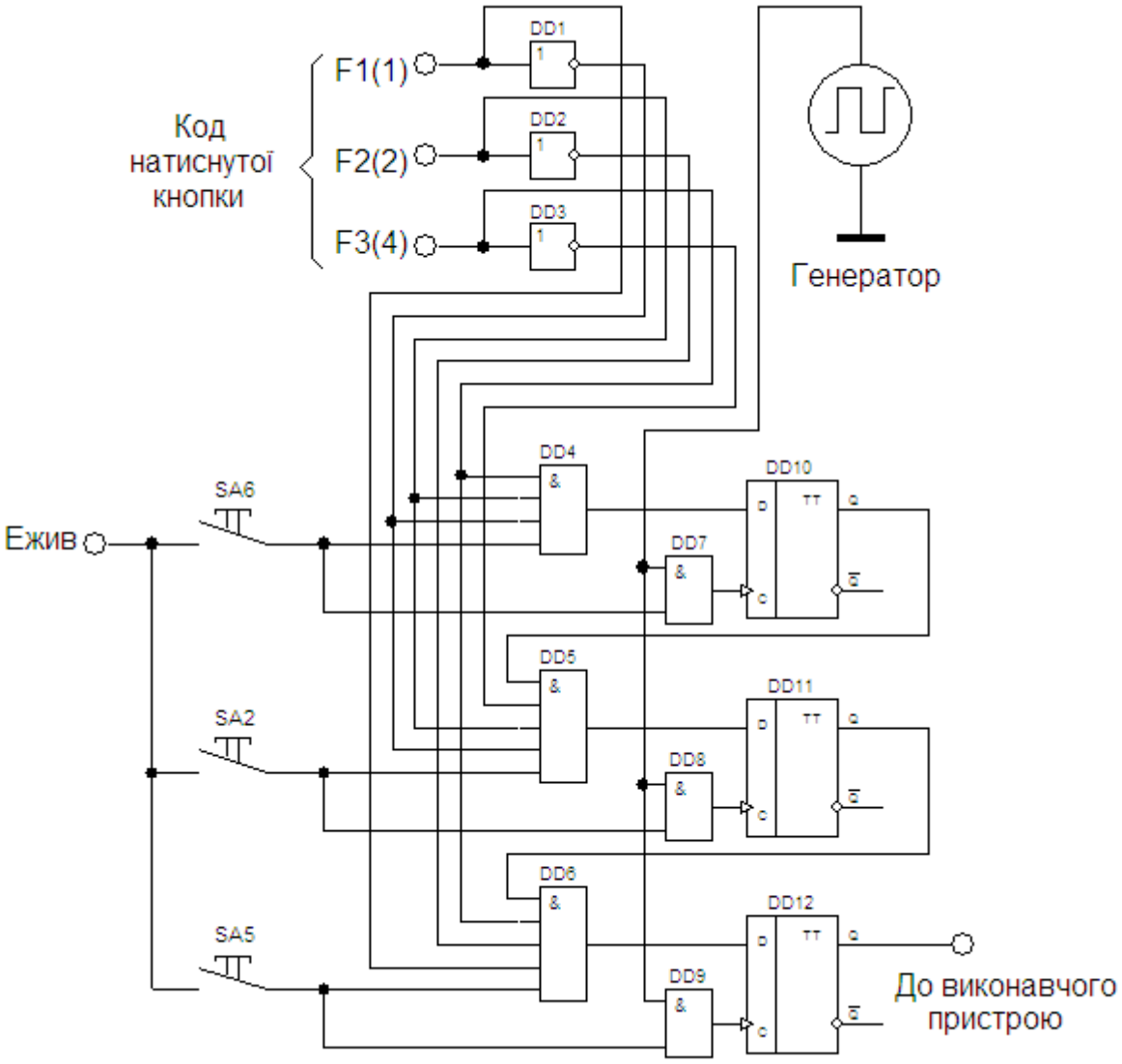


Рисунок 2.10 - Паралельно – послідовний регістр натискання закодованих кнопок

Будь який інший код натиснутої кнопки, або порушення обраного порядку натискання кнопок коду приводить до блокування проходження сигналу через тригери регістра.

2.2.3 Кодування номерів та порядку натискання кнопок

Кодування номерів та порядку натискання кнопок виконується за допомогою двох колодок: порядку натискання кнопок клавіатури і двійкового коду чисел набраних на клавіатурі (рис 2.11).

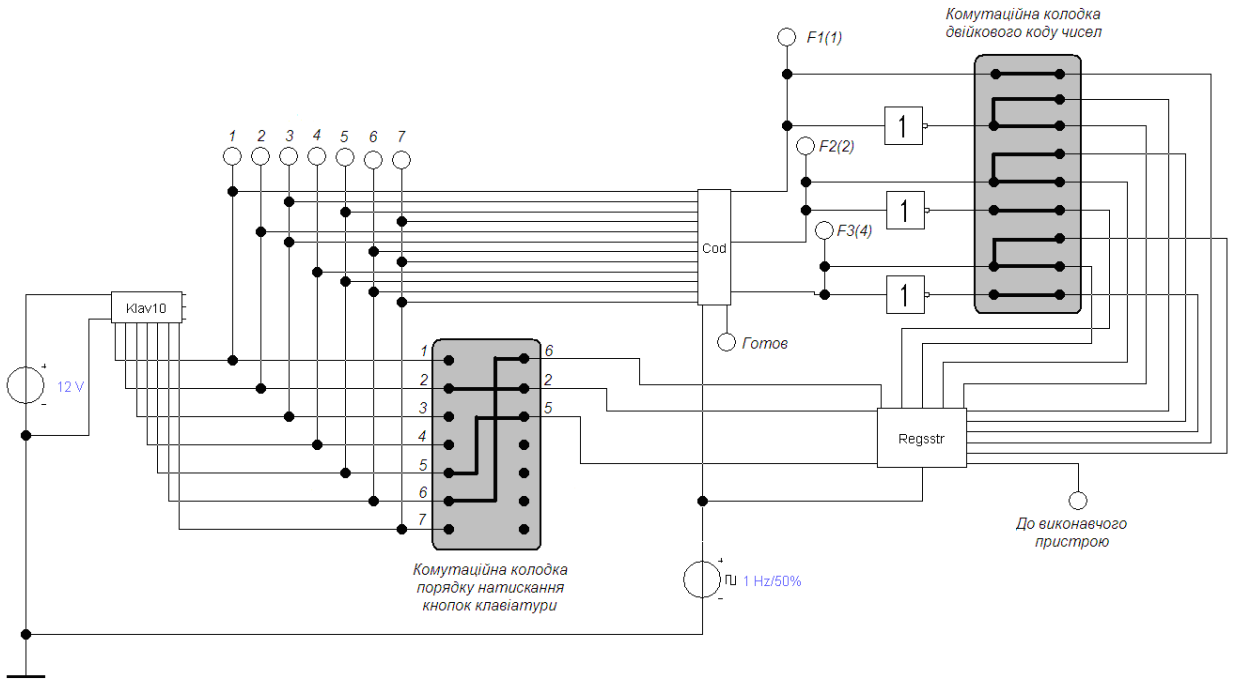


Рисунок 2.11 - Кодування номерів та порядку натискання кнопок

Програмування порядку натискання кнопок виконується користувачем. До колодки порядку натискання кнопок клавіатури приходять сигнали натиснутих кнопок (логічна 1) від наборної панелі. У заданому порядку ці сигнали приходять на відповідні додаткові комбінаційні схеми на входах тригерів регістра. До колодки комутації двійкового коду чисел поступають сигнали натиснутих кнопок у заданому порядку, у двійковому еквіваленті. З колодки ці сигнали також приходять на відповідні додаткові комбінаційні схеми на входах тригерів регістра. При правильному наборі інформація послідовно проходить через регістр і з’являється на виході «До виконавчого пристрою».

Для розширення варіантів кодування інформації та функціональних можливостей схеми контролю і управління доступом у приміщення розглянута можливість збільшення контактних груп комутаційних колодок.

Комутаційні колодки встановлюються у антивандальному захищеному корпусі з внутрішньої сторони приміщення, мають захист від несанкціонованого доступу і легко програмуються за допомогою перемикачів або перемичок.

2.3 Виконавчий пристрій

При правильному набраному коді останнім спрацьовує тригер регістра DD12 (рис.2.10). Проведемо аналіз функціонування виконавчого пристрою з використанням D-тригера з додатковими функціями запису та скидання інформації [4]. Для того щоб схема не залишилася в такому стані надовго, використовується транзистор VT1 який керується інверсним виходом останнього тригера (рис. 2.12). Він забезпечує затримку обнуління тригерів регістра.

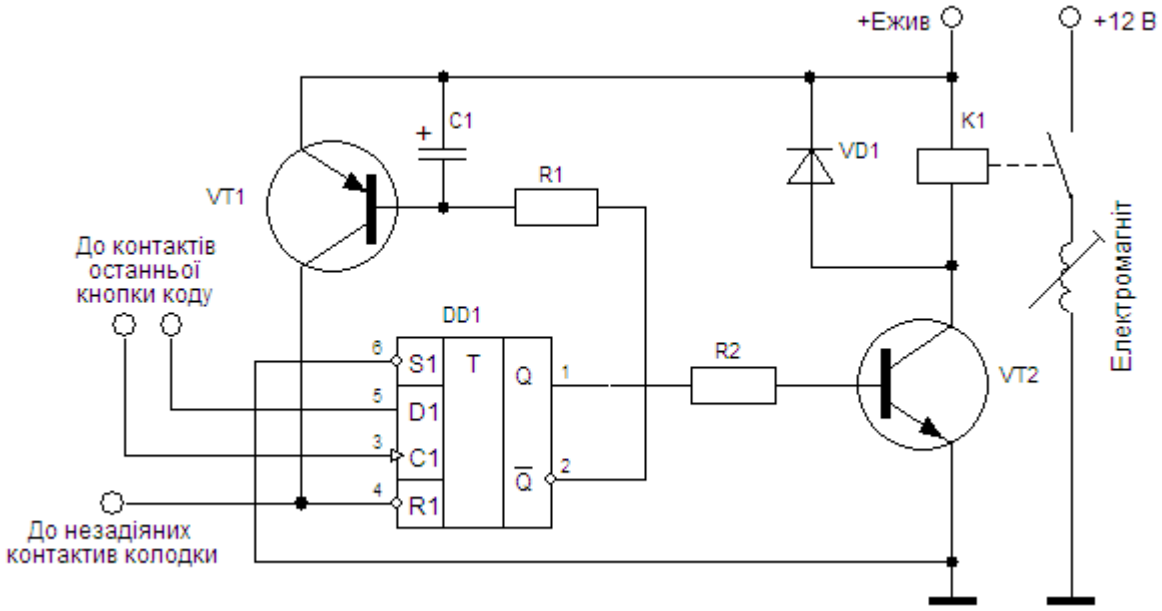


Рисунок 2.12 – Схема підключення виконавчого пристрою

Затримка формується за рахунок кола заряду конденсатора С1 через резистор R1. З цієї причини на виході DD1 сигнал логічної "1" буде присутній певний час, що визначатиметься сталою часу заряду. Цього часу цілком достатньо для спрацьовування реле К1 або електромагніту. Час, при бажанні, легко можна зробити значно більше, застосувавши конденсатор С2 більшої ємності.

Електромагнітний замок призначений для використання в системах контролю доступу і автоматики, а також в приміщеннях, де пред'являються найжорсткіші вимоги до виконавчого механізму:

- висока надійність;

- виняткова зносостійкість.

Згідно з параметричними дослідженнями обрано електромагнітний замок ATIS AM-280 (рис. 2.13).



Рисунок 2.13 – Електромагнітний замок ATIS AM-280

Замок поєднується з будь-якими типами кодових панелей, контролерами, картковими зчитувачами.

Замок встановлюється на двері будь-якого типу усередині приміщення, спільно з дверним доводчиком.

Замок володіє наступними параметрами:

- сила утримання 300 кг;
- напруга живлення DC12V;
- струм спрацювання 500 мА;
- споживана потужність 6 Вт

2.4 Схема підвищення секретності кодового замка

Для підвищення секретності кодового замка розрахована схема, яка передбачає підрахунок кількості натискань кодових кнопок.

Схема заснована на використанні синхронного лічильника Джонсона (кільцевого лічильника) [4]. У цих лічильниках вхід регістра сполучений не з

прямим виходом Q, а з інверсним виходом $\overline{Q}$. В результаті, коли на вхід лічильника поступають тактові імпульси, то спочатку всі розряди лічильника заповнюються одиницями, а потім – нулями. Лічильник Джонсона має коефіцієнт перерахунку, удвічі більший числа складових його тригерів. Зокрема, якщо лічильник складається з трьох тригерів (m = 3), то він матиме шість стійких станів. Лічильники Джонсона використовуються в системах автоматики, наприклад, як розподільники імпульсів. Схема чотирьохрозрядного лічильника Джонсона приведена на рисунку 2.14, а стан його виходів приведений в таблиці 2.3.

Таблиця 2.3 – Стан виходів чотирьохрозрядного лічильника Джонсона

n	Q1	Q2	Q3	Q4	n	Q1	Q2	Q3	Q4
0	1	0	0	0	4	0	1	1	1
1	1	1	0	0	5	0	0	1	1
2	1	1	1	0	6	0	0	0	1
3	1	1	1	1	7	0	0	0	0

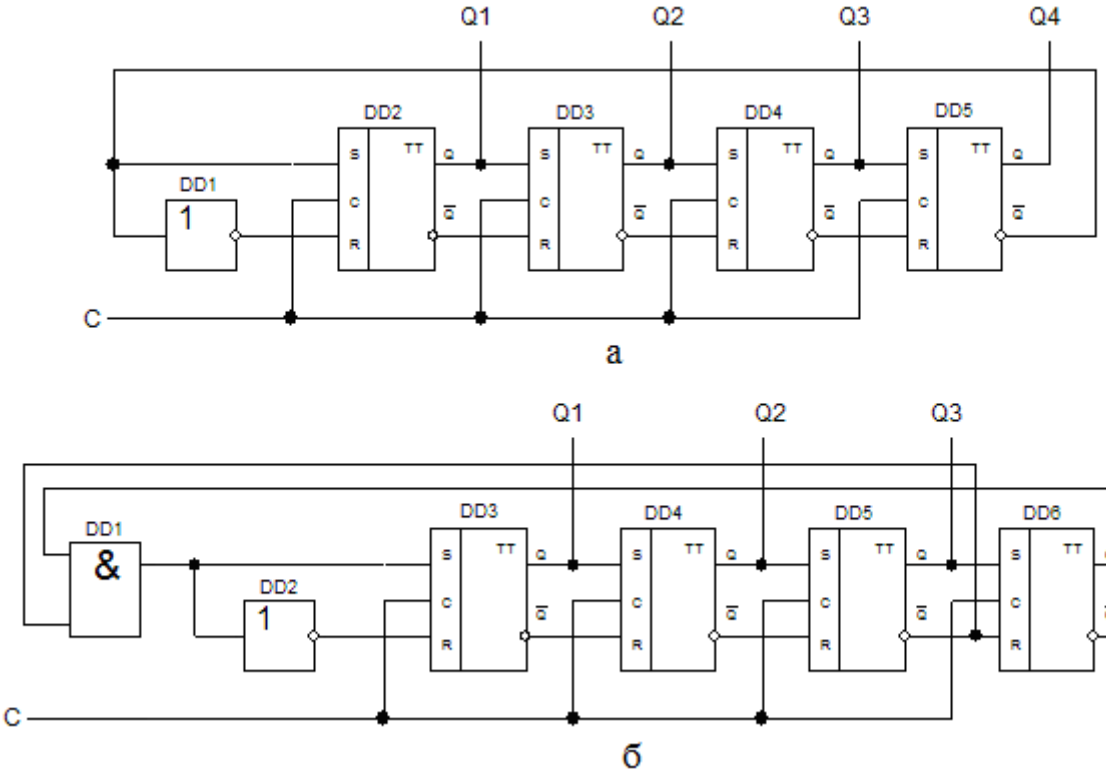


Рисунок 2.14 - Схема чотирьохрозрядного лічильника Джонсона з парним (а) і непарним (б) модулем рахунку

Як випливає з таблиці 2.3, модуль рахунку лічильника Джонсона в два рази більше модуля рахунку простого кільцевого лічильника. У лічильнику Джонсона, як і в інших кільцевих лічильниках, можуть бути збої, викликані завадами. Для корекції порушень, викликаних збоями, також використовуються способи, за допомогою яких виконується перехід з будь-якої забороненої комбінації в одну із дозволених.

Лічильники Джонсона широко використовуються в дільниках частоти імпульсів, генераторах випадкових чисел, в пристроях пам'яті та ін. На базі лічильника Джонсона можна легко реалізувати лічильники з будь-яким парним модулем рахунку. Якщо є необхідність мати непарне значення модуля рахунку, то можна на вхід першого розряду подавати сигнал $\overline{Q}_{n-1}\overline{Q}_n$, замість сигналу $\overline{Q}_n$, як це показано на рисунку 2.14 (б). При цьому з набору вихідних станів лічильника Джонсона виключається одна кодова комбінація, складена з нулів.

Аналіз спрацювання схеми підрахунок кількості натискань кодових кнопок показує необхіднфсть застосування кільцевого лічильника побудованого на регістрі зсуву (рис. 2.15).

Інверсний вихід $\overline{Q}$ останнього тригера сполучений з прямим входом D першого тригера і на ньому присутня логічна 1. Після натиснення першої кнопки коду логічна 1 записується у перший тригер і елемент І, який формує вихід першого розряду регістра. У всі останні тригери записано логічний 0. На інверсному виході другого тригера логічна 1, яка також поступає на елемент І виходу першого розряду регістра. Таким чином на першому розряді регістра формується логічна 1. Після натискання другої кнопки коду одиниця з виходу першого тригера перезаписується у другий тригер і відповідний елемент І виходу другого розряду регістра. На другому вході елемента І присутня логічна 1 з інверсного виходу третього регістра у який записано логічний 0. На другому розряді регістра формується логічна 1, а на першому логічний 0. Натискання третьої кнопки коду приводить у стан логічної 1 третій розряд регістра і у стан логічного 0 перші два розряди.

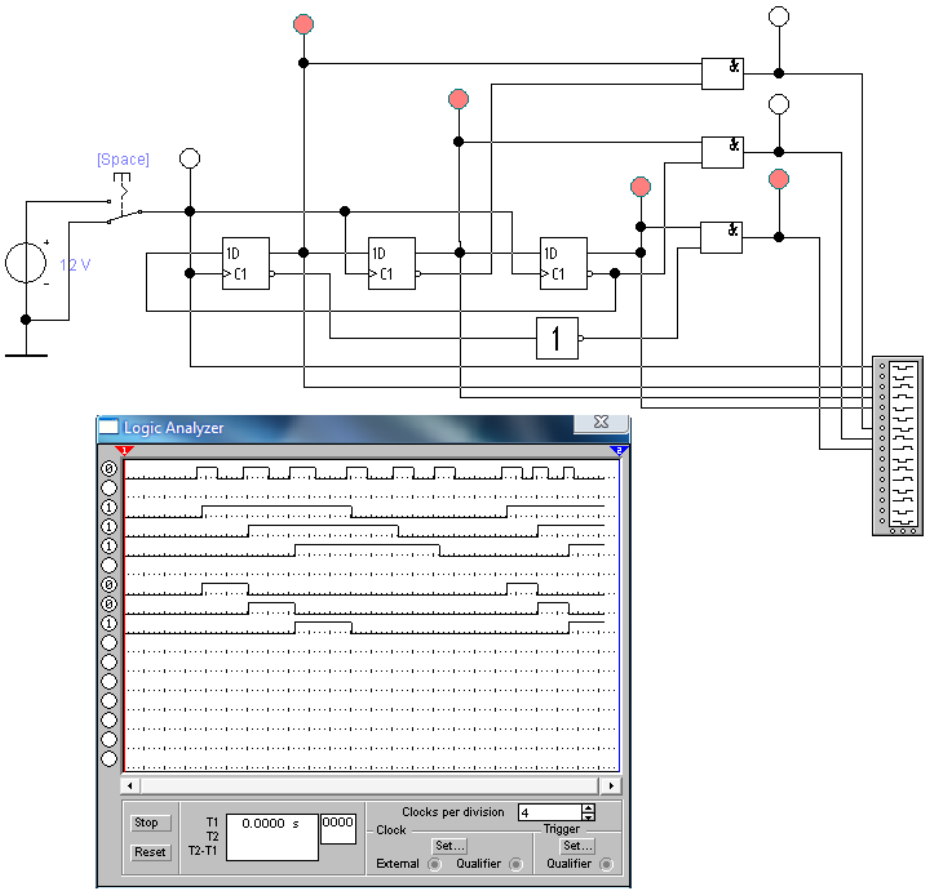


Рисунок 2.15 – Схема підрахунок кількості натискань кодових кнопок

Використаємо мікросхему лічильника-дільника на 8. Цей лічильник має в основі синхронний лічильник Джонсона (використовується чотири тригера), який дає підвищення швидкості рахунку. При цьому у вихідних сигналах відсутні списи перешкод. Дешифратор переводить стани тригерів лічильника у вісім вихідних станів, які відповідають рахунку від 0 до 7. Мікросхема має входи заборони рахунку і скидання. Сигнал вихідного перенесення CR завершує цикл рахунку при восьмому тактовому імпульсі. Позитивні фронти імпульсів CR використовуються як тактова послідовність для подальшого лічильника. Таким чином, двохкаскадне з'єднання виходить асинхронним (другий лічильник працює від пульсацій CR), хоча кожен з лічильників – синхронний. При натисканні будь-якої закодованої кнопки на вхід одновібратора DD2, DD4 через діоди VD1-VD3 надходить напруга високого рівня (рис. 2.16). Одновібратор виробляє короткий імпульс, який, вступаючи на вхід C1, змінює стан лічильника DD5.

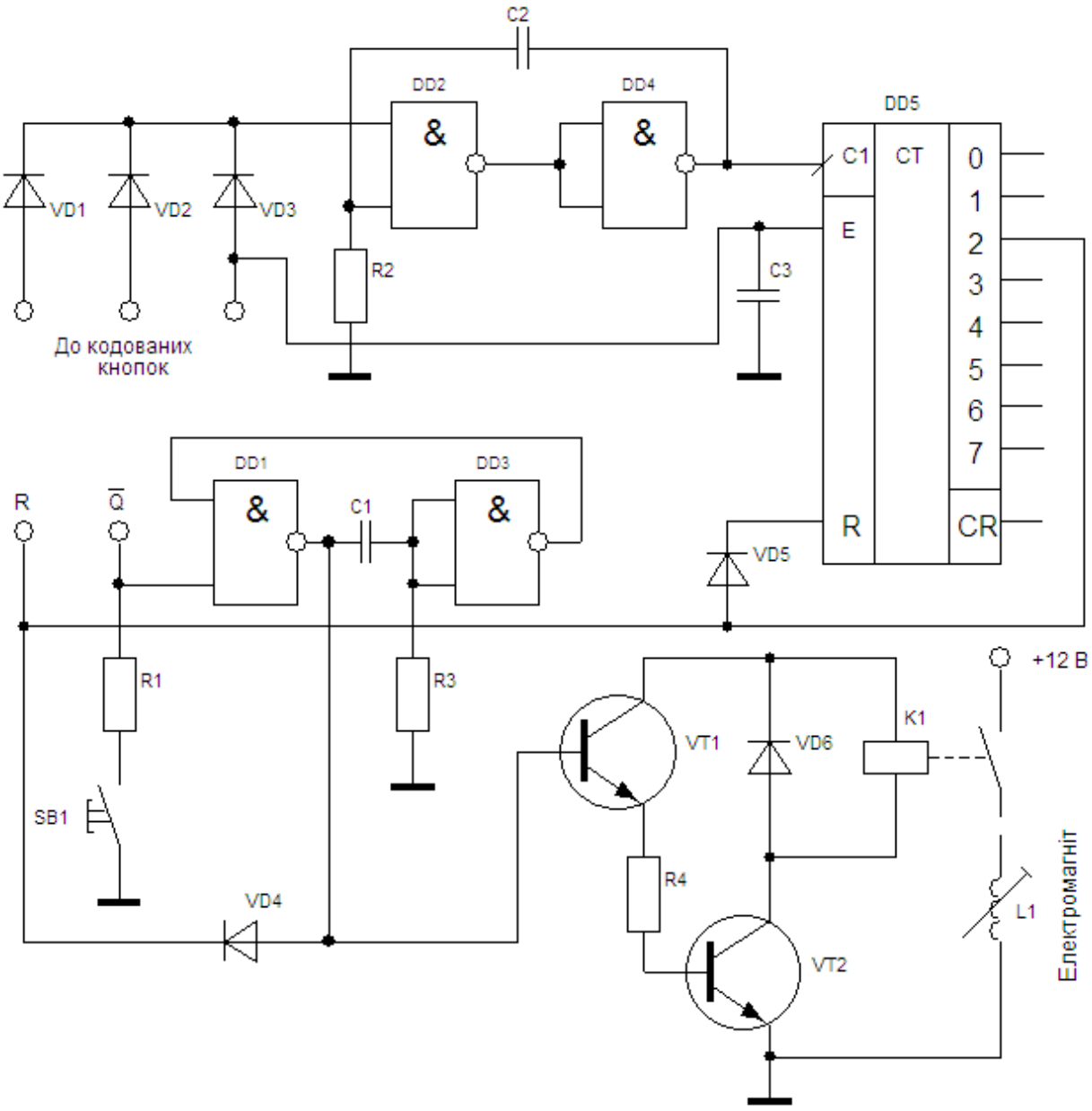


Рисунок 2.16 – Схема підвищення секретності кодового замка

Після третього натискання напруга високого рівня з виходу лічильника через діод VD5 переключить тригери і лічильник в початковий стан. Таким чином, запобігається спрацьовування замка при повторному натисканні кнопок правильного коду. Якщо третьою натиснута кнопка з правильною цифрою коду, то на вхід Е лічильника деякий час надходить напруга високого рівня з конденсатора С2, тому перемикання лічильника та генерація імпульсу скидання станеться з затримкою, необхідною для того, щоб встиг переключитися тригер DD12 (рис. 2.10) і запуститися одновібратор DD1, DD3.

Кнопка SB1 призначена для відкриття замку зсередини приміщення.

2.5 Схема сповіщувачів

Інформація номеру натиснутої кнопки відображається семисегментним світлодіодним індикатором. Операція зміни коду числа називається його перекодуванням. Інтегральні мікросхеми, які виконують ці операції, називаються перетворювачами коду. Вагові перетворювачі коду перетворюють інформацію для її подальшого відображення [4].

Розрахуємо перетворювач двійкового коду 4-2-1 в код управління семисегментним світлодіодним індикатором (рис. 2.17). На рисунку також приведені зображення цифр. Такий перетворювач повинен мати три входи, оскільки для кодування десяткових цифр від 0 до 7 вистачає трьох двійкових розрядів і сім виходів, поодинці на кожен сегмент.

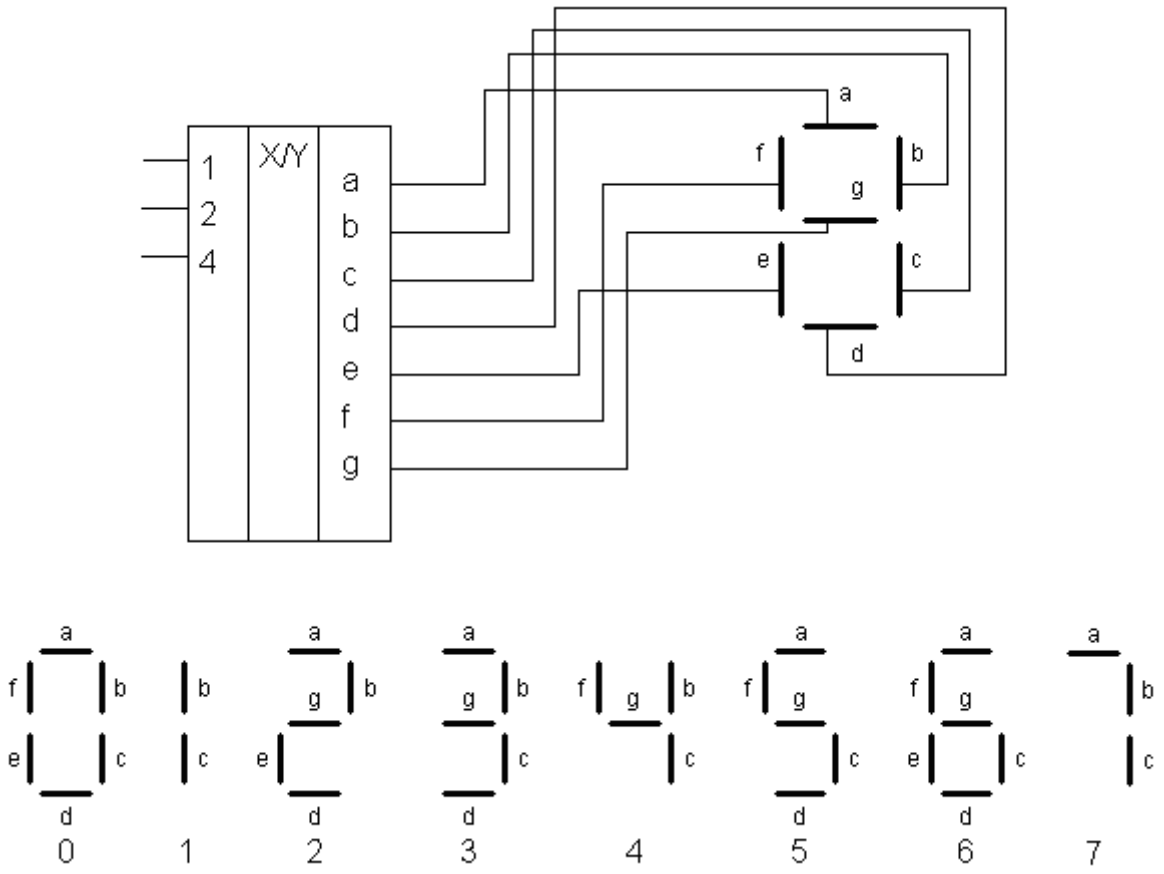


Рисунок 2.17 - Перетворювач двійкового коду в код управління семисегментними світлодіодними індикаторами

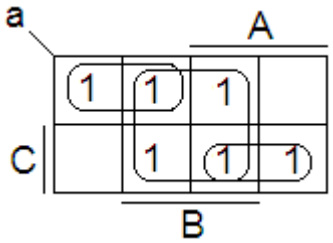
З таблиці істинності перетворювача коду (табл. 2.4) видно, що, наприклад, в цифрі 0 повинні світитися всі сегменти за винятком сегменту g, в цифрі 1 світяться лише два сегменти b і c і т. д. Вагові коефіцієнти двійкових розрядів дорівнюють $(421)_2$. Нулі проставлені для тих цифр, в яких сегмент не світиться.

Таблиця 2.4 – Таблиця істинності перетворювача двійкового коду в код управління семисегментними світлодіодними індикаторами

DEC цифра	Входи			Виходи						
	A	B	C	a	b	c	d	e	f	g
0	0	0	0	1	1	1	1	1	1	0
1	0	0	1	0	1	1	0	0	0	0
2	0	1	0	1	1	0	1	1	0	1
3	0	1	1	1	1	1	1	0	0	1
4	1	0	0	0	1	1	0	0	1	1
5	1	0	1	1	0	1	1	0	1	1
6	1	1	0	1	0	1	1	1	1	1
7	1	1	1	1	1	1	0	0	0	0

Вихідна функція для сегменту a:

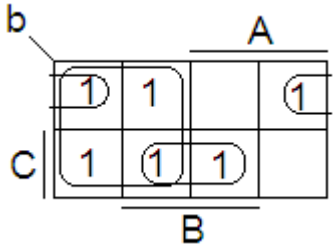
$$Fa = \overline{A}\overline{B}\overline{C} + \overline{A}B\overline{C} + \overline{A}BC + A\overline{B}C + AB\overline{C} + ABC$$



Після спрощення отримаємо: $Fa = B + \overline{A}\overline{C} + AC$.

Вихідна функція для сегменту b:

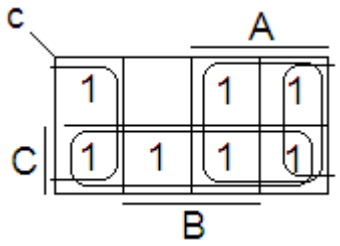
$$Fb = \overline{A}\overline{B}\overline{C} + \overline{A}\overline{B}C + \overline{A}B\overline{C} + \overline{A}BC + A\overline{B}\overline{C} + ABC$$



Після спрощення отримаємо: $Fb = \overline{A} + BC + \overline{B}\overline{C}$.

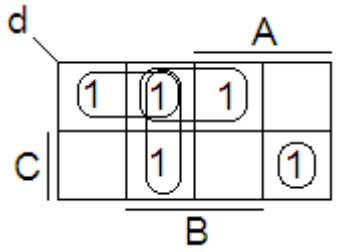
Вихідна функція для сегменту c:

$$Fc = \overline{A}\overline{B}\overline{C} + \overline{A}\overline{B}C + \overline{A}BC + A\overline{B}\overline{C} + A\overline{B}C + AB\overline{C} + ABC$$



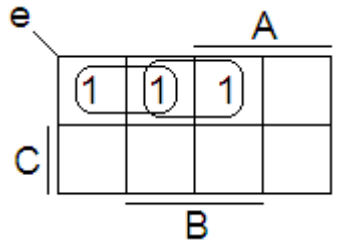
Після спрощення отримаємо: $Fc = A + C + \overline{B}$.

$$Fd = \overline{A}\overline{B}\overline{C} + \overline{A}BC + \overline{A}BC + A\overline{B}\overline{C} + AB\overline{C}$$



Після спрощення отримаємо: $Fd = \overline{A}B + \overline{A}\overline{C} + B\overline{C} + A\overline{B}C$.

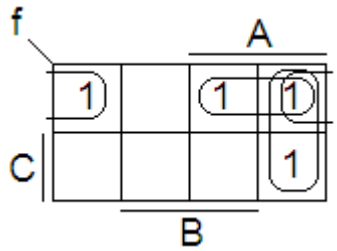
$$Fe = \overline{A}\overline{B}\overline{C} + \overline{A}B\overline{C} + AB\overline{C}$$



Після спрощення отримаємо: $Fe = \overline{A}\overline{C} + B\overline{C}$.

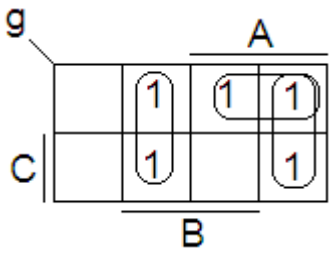
Вихідна функція для сегменту f:

$$Ff = \overline{A}\overline{B}\overline{C} + A\overline{B}\overline{C} + A\overline{B}C + AB\overline{C}$$



Після спрощення отримаємо: $Ff = A\overline{C} + A\overline{B} + \overline{B}\overline{C}$.

$$Fg = \overline{A}B\overline{C} + \overline{A}BC + A\overline{B}\overline{C} + A\overline{B}C + AB\overline{C}$$



Після спрощення отримаємо: $Fg = A\overline{C} + \overline{A}B + A\overline{B}$.

Проведемо аналіз функціонування схеми в програмному застосуванні EWB на елементах елементарної логіки (рис. 2.18).

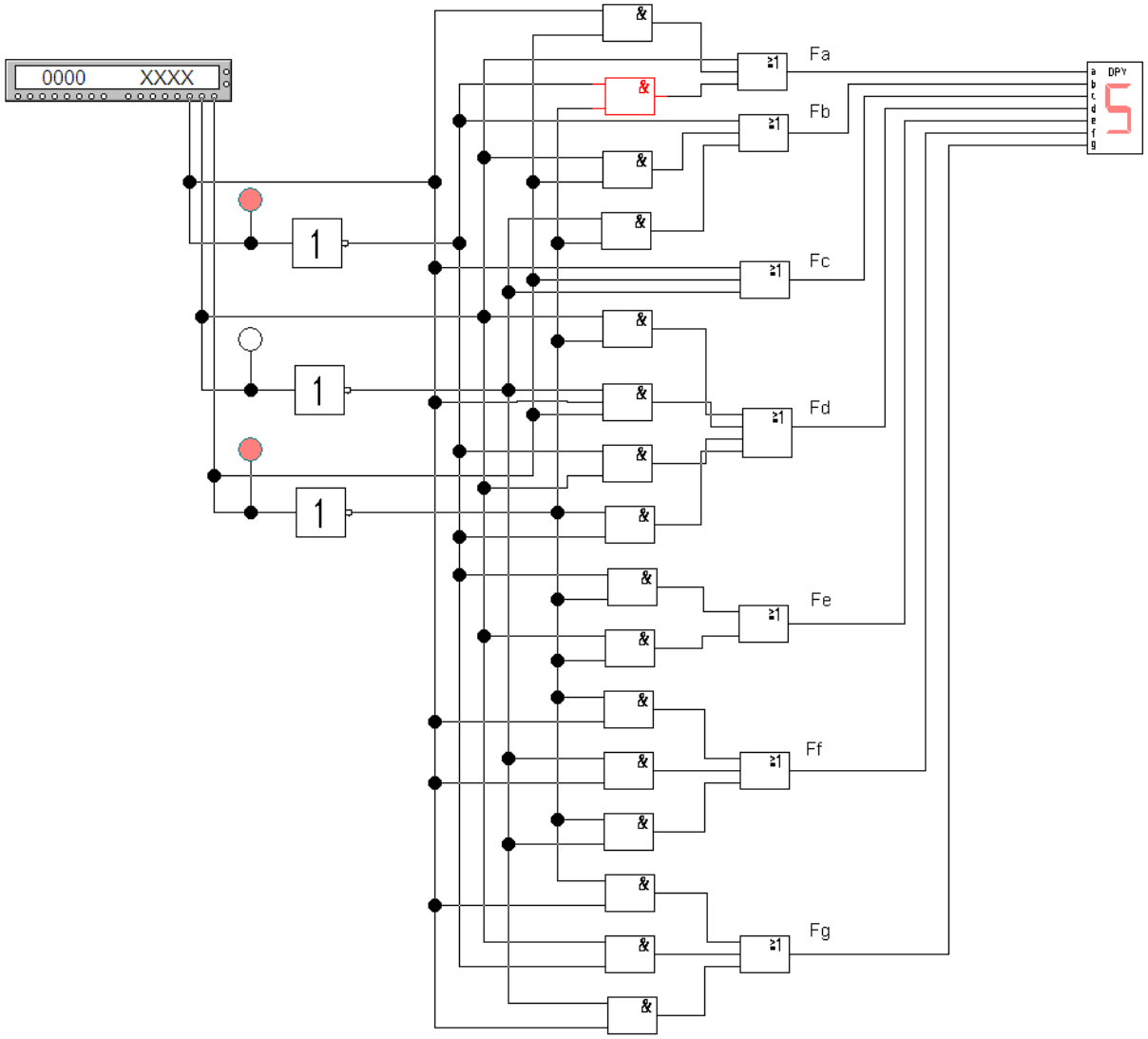


Рисунок 2.18 - Аналіз функціонування схеми індикатора натиснутої кнопки

Схема електрична принципова перетворювача двійково-десяткового коду чисел в коди семисегментних індикаторів може бути виконана на мікро-

схемах ТТЛ логіки. Мікросхема 7447РС являє собою перетворювач логічних сигналів з двійкового коду 8-4-2-1 в код семисегментного індикатора з загальним анодом (рис. 2.19) [5].

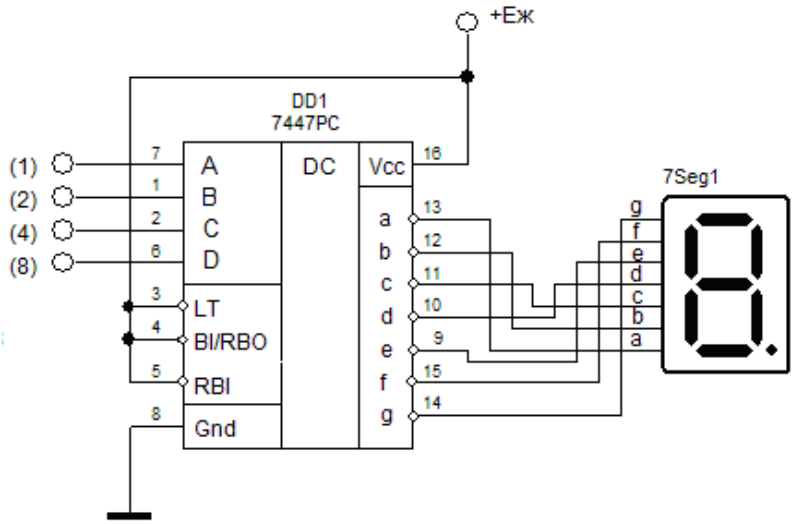


Рисунок 2.19 – Схема перетворення двійкового коду 8-4-2-1 в код семисегментного індикатора на мікросхемі 7447РС

Мікросхема має виходи з відкритим колектором і підвищеною навантаженою здатністю. Призначення виводів представлено в таблиці 2.7. Схема знаходиться в працездатному стані, коли на виводі управління BI/RBO присутній високий рівень. Для перевірка роботоздатності мікросхеми на вивід LT подається низький рівень сигналу. При цьому на усіх вихідах з’являється логічний 0. Складемо таблицю функціонування перетворювача двійкового коду 8-4-2-1 в код семисегментного індикатора на мікросхемі 7447РС (табл. 2.5). Проведемо аналіз функціонування перетворювача в програмному забезпеченні Electronics Workbench (рис. 2.20).

Активний рівень сигналу на виходах мікросхеми 7447 логічний 0, так як схема з відкритим колектором. В програмному забезпеченні Electronics Workbench використовується семисегментний індикатор з загальним катодом, тому виходи мікросхеми (OA OB OC OD OE OF OG) необхідно інвертувати.

Таблиця 2.5 – Призначення виводів мікросхеми 7447РС

№ вивода	Призначення
1	Вхід з вісовим значенням розряду (2)
2	Вхід з вісовим значенням розряду (4)
3	Вхід контроля індикатора (LT)
4	Вихід сигналу схеми послідовного погашення (BI/RBO)
5	Вхід сигналу схеми послідовного погашення (RBI)
6	Вхід з вісовим значенням розряду (8)
7	Вхід з вісовим значенням розряду (1)
8	Загальний (Gnd)
9	Вихід сегменту (e)
10	Вихід сегменту (d)
11	Вихід сегменту (c)
12	Вихід сегменту (b)
13	Вихід сегменту (a)
14	Вихід сегменту (g)
15	Вихід сегменту (f)
16	Напруга живлення (+Vcc)

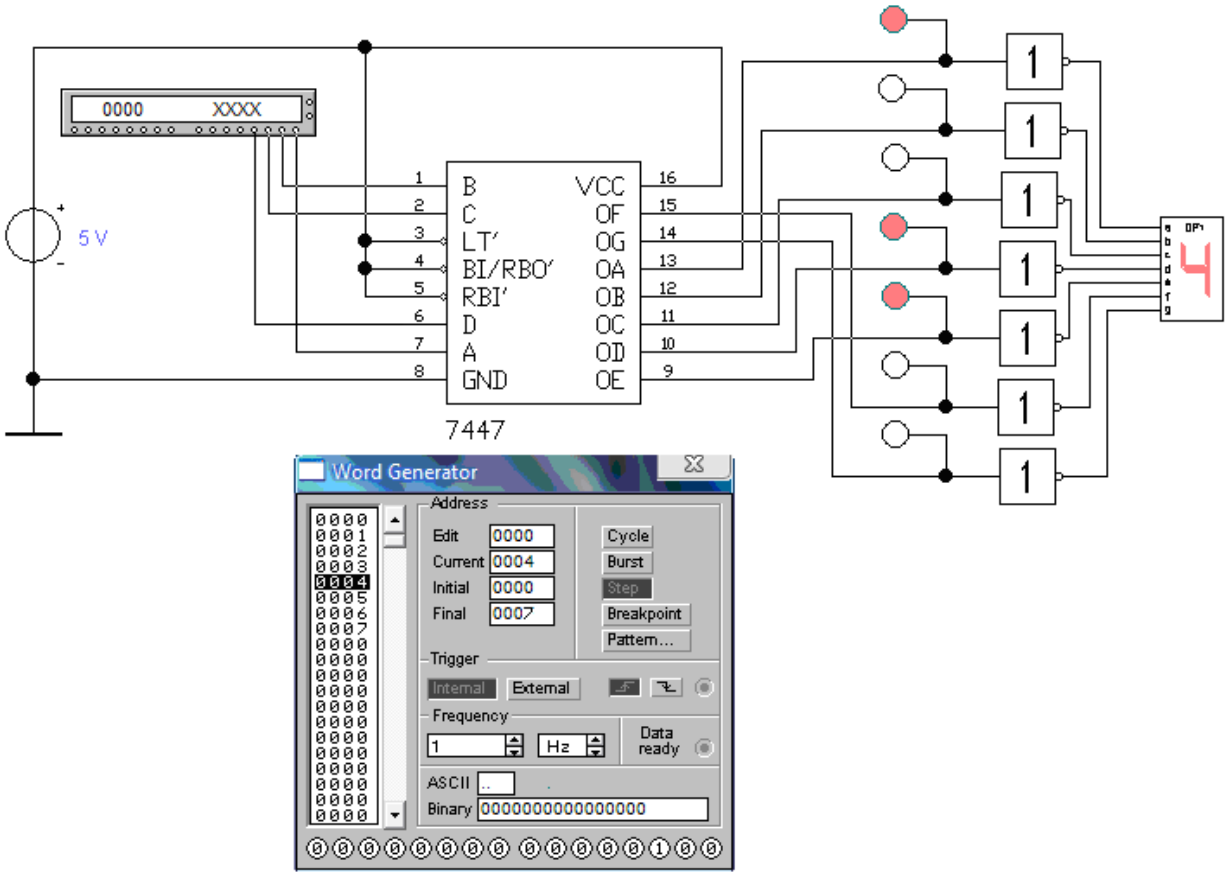


Рисунок 2.20 - Аналіз функціонування перетворювача двійкового коду 4-2-1 в код семисегментного індикатора

В розробленому пристрої використано відеовічко з інфрачервоним підсвічуванням компанії KIVOS моделі KDB01 призначене для установки на вхідні двері, замість звичайного оптичного вічка (рис. 2.21).



Рисунок 2.21 - Відеовічко компанії KIVOS моделі KDB01

Відеовічко має функцію дверного дзвінка з можливістю вибору однієї з 12 мелодій дзвінка, а так само дозволяє записувати фотографії і відео відвідувача на карту пам'яті. Запис здійснюється автоматично при натисненні на кнопку виклику відвідувачем.

Електронне відеовічко заряджається від загального з кодовим пристроєм блоку живлення а працює від акумуляторної батарей, якої при звичайному використанні повинно вистачити на 1 місяць. Коли заряд батареї закінчуватиметься - на екрані з'явиться відповідне повідомлення і панель почне видавати періодичні гудки, нагадуючи що потрібно зарядити батарею.

Особливості відевіочка Kivos KDB01:

- можливість наближення зображення відвідувача до 8 разів;

- можливість фотографування і відеозапису як в ручному, так і в автоматичному режимі (при натисненні на кнопку дзвінка відвідувачем);

- налаштування відображення дати і часу в збережених файлах відео і фото записів;

- можливість налаштування часу автоматичного відео запису (10/20/30 секунд) або кількості фотографій (5/10/15 штук) при натисненні на кнопку дзвінка відвідувачем;

- підтримує запис на micro SD карти пам'яті, ємкістю до 32 ГБ;

- можливість перегляду записаних відео і фото файлів відвідувачів як на самому моніторі відеовічка, так і на комп'ютері через USB кабель;

- можливість у будь-який час проглянути обстановку за дверима і уручну включити відео або фото запис за допомогою кнопок на блоці монітора;

- має широкий горизонтальний 120º і вертикальний 170º градусів кути огляду;

- має ІЧ підсвічування з дальністю до 1,5 м для роботи при поганому освітленні за дверима;

- автоматичне включення ІЧ підсвічування при поганому освітленні;

- автоматична функція «циклічного запису» при браку пам'яті, тобто автоматично стиратимуться найстаріші записи;

- має функцію дверного дзвінка з можливістю вибору однієї з 12 мелодії дзвінка;

- літієва батарея BP-6M високої ємкості 1100 мАч і енергозбережний режим роботи дозволяють пропрацювати в автономному режимі до 30 діб;

- можливість одночасної роботи і зарядки батареї;

2.6 Схема електрична кодового пристрою запобігання проникнення у приміщення

Аналіз функціонування схеми кодового пристрою запобігання проникнення у приміщення, показує відповідність спрацювання вузлів згідно з поставленим завданням (рис. 2.22).

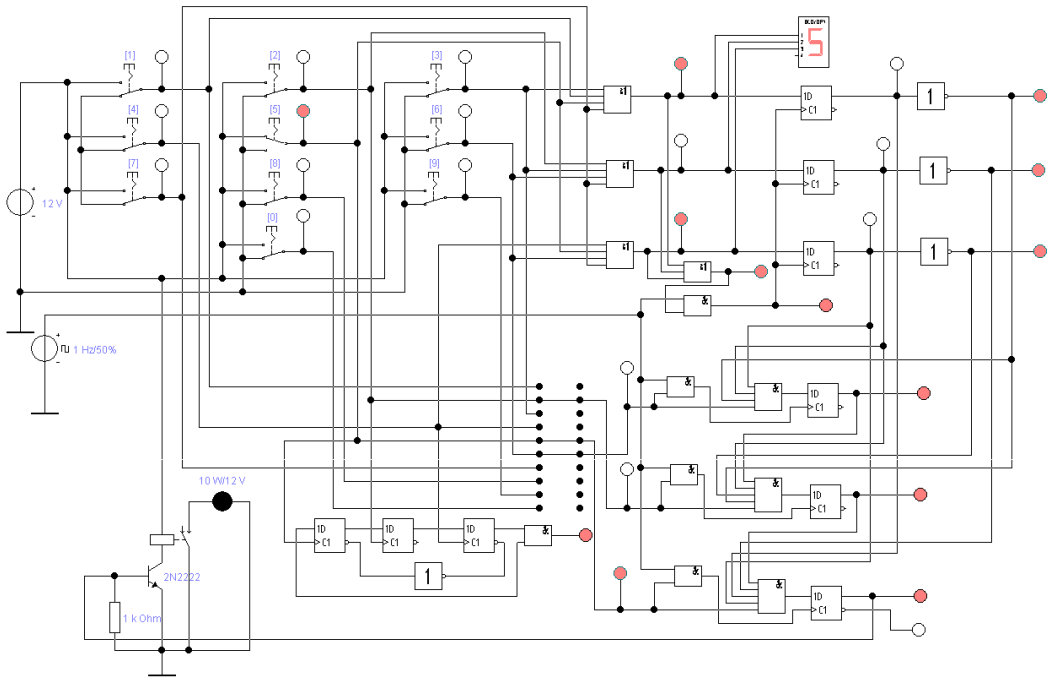


Рисунок 2.22 – Аналіз функціонування схеми контролю і управління доступом у приміщення

Схема кодового пристрою зібрана КМОН мікросхемах. що забезпечує високу надійність і економічність роботи. Споживання схемою малих струмів дозволяє забезпечити, при необхідності, автономне живлення, що підвищує надійність при виконанні функцій запобігання проникнення у приміщення. Для живлення використовується стабілізоване джерело постійної напруги 12 В (рис. 2.23).

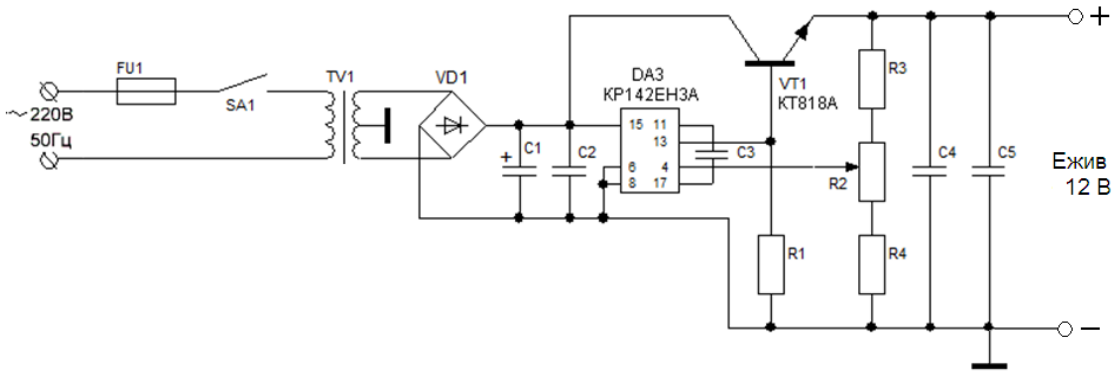


Рисунок 2.23 - Джерело живлення системи контролю і управління доступом у приміщення

Система контролю і управління доступом у приміщення представлена на рисунку 2.24.

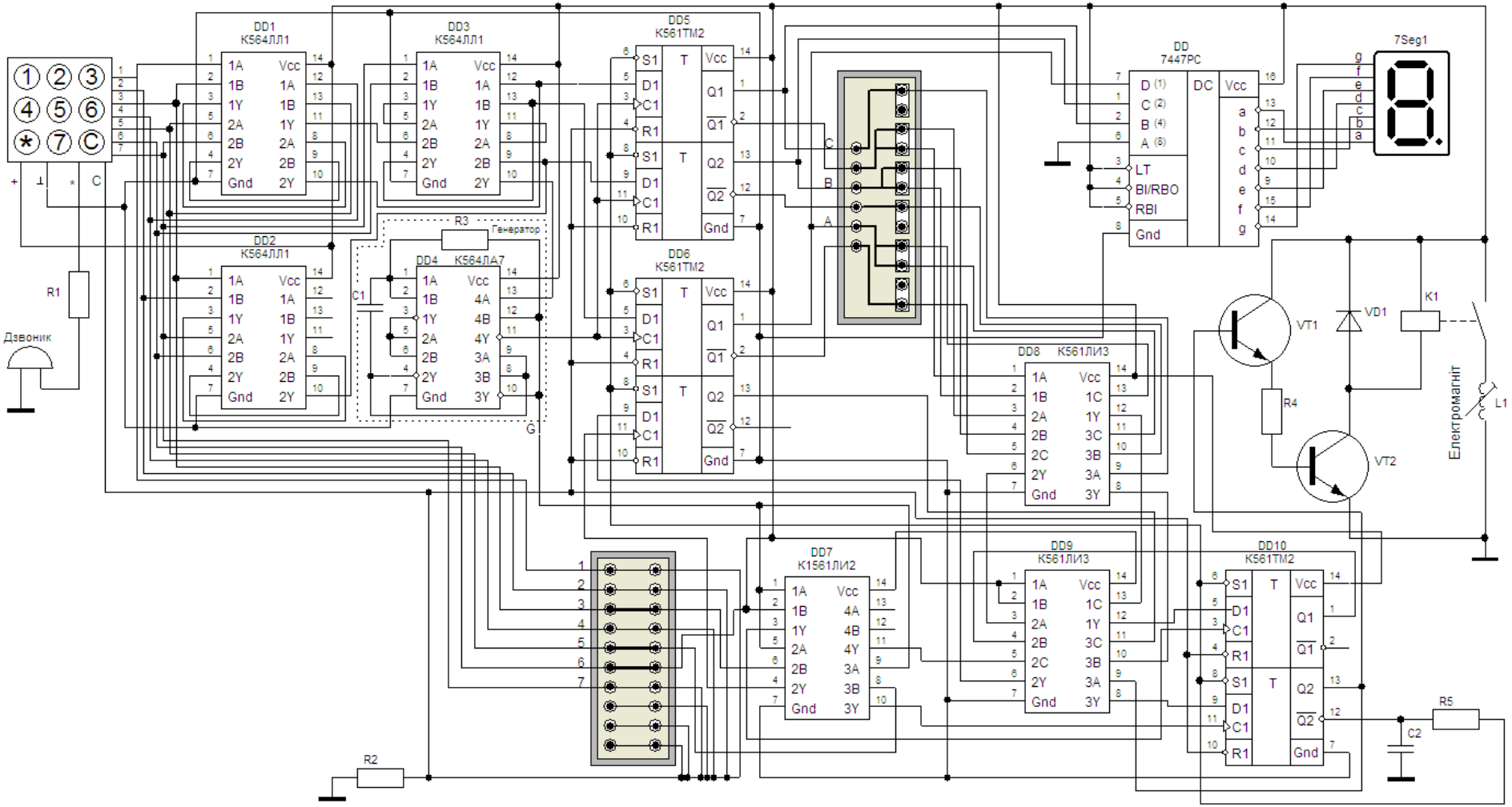


Рисунок 2.24 - Система електричного запобігання проникненню у приміщення

Працює електрична схема наступним чином. У початковий момент, при подачі живлення, коло з конденсатора і резистора формує імпульс обнуління тригерів.

При натисканні на кнопку першої цифри коду (на схемі – SA6), в момент її відпускання перший тригер мікросхеми DD10 переключиться, тобто на його неінвертуючому виході з'явиться сигнал логічної "1", так як на вході даних є логічна "1". При натисканні наступної кнопки SA2, якщо на вході D другого тригера DD6 присутній сигнал логічної "1" на виході тригера встановиться високий логічний рівень, тобто кожний наступний тригер спрацьовує за умови спрацювання попереднього тригера.

В процесі набору коду натискання будь якої помилкової цифри обнуляє всі тригери. Якщо сигнал керування транзистором VT1 знімати з виходу не останнього тригера (наприклад з першого), то буде обмежено необхідний час на натискання цифр коду. У цьому випадку навіть при правильному, але повільному наборі коду вихідний сигнал не з'явиться.

Розміщується схема поблизу кнопкової панелі. Всі використовувані деталі, за винятком транзистора VT2, можуть бути будь-якого типу. Транзистор VT2 застосований з великим коефіцієнтом підсилення, і в разі використання в якості навантаження замість реле електромагніту його потрібно замінити на більш потужний. Для відкривання засувки дверного замка краще використовувати не електромагніт, а серводвигун з редуктором.

При натисканні кнопки першої цифри коду SA6 тригер DD10 переключиться і на вході D тригера DD10 з'явиться напруга високого рівня. Тому при натисканні черговий кнопки коду SA2 тригер DD6 змінює свій стан і готує до перемикання наступний тригер. У разі подальшого правильного набору SA5 останнім спрацює другий тригер мікросхеми DD10 і відкриваються транзистори VT1 і VT2, що викличе спрацьовування виконавчого пристрою. Напруга низького рівня з виходу другого тригера мікросхеми DD10 встановить тригери і лічильник DD4 в початковий стан.

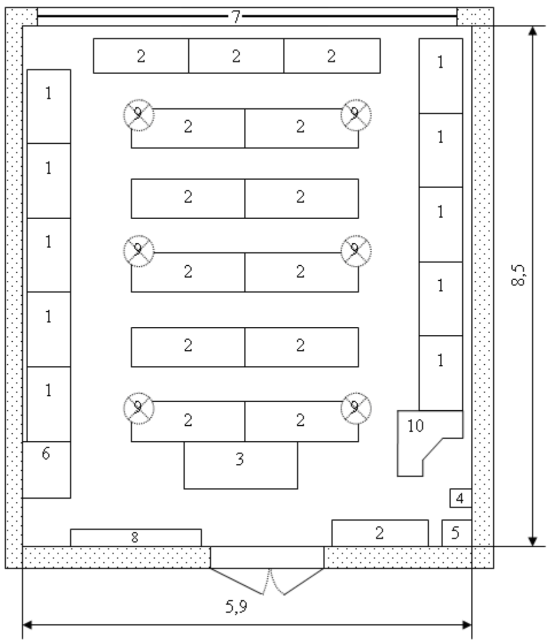
Натискання будь-якої кнопки з цифрою, що не входить до складу коду та підключеної до першої комутаційної колодки, призводить до перемикання тригерів в нульовий стан.

Якщо після набору правильного коду замок не спрацював, значить, раніше була зроблена невдала спроба його відкриття, лічильник і тригери перебувають не в початковому стані. У цьому випадку необхідно перед відкриттям замку натиснути будь-яку кнопку з цифрою, що не входить до складу коду.

3 Охорона праці та техногенна безпека

3.1 Характеристика потенційних небезпечних та шкідливих виробничих факторів

При виконанні дипломної роботи комп'ютерне моделювання та розрахунок пристрою вимірювання швидкості газу проводилися в приміщенні кафедри МЕІС, макет якого представлено на рисунку 3.1 [6].



1 - стіл комп'ютерний; 2 - стіл аудиторний; 3 - стіл викладача; 4 - автомат відключення електричного живлення; 5 - шафа силова; 6 - шафа універсальна; 7 - вікно; 8 - дошка аудиторна; 9 - світильник 4-х ріжковий; 10 - стіл адміністратора мережі

Рисунок 3.1 – Макет приміщення в якому проводилися роботи

Лабораторія є приміщенням легкої категорії (виконуються легкі фізичні роботи), тому повинні дотримуватися такі вимоги (період року – холодний) [7]:

- оптимальна температура повітря – 22…24 °С (допустима – 20…24 °С);

- оптимальна відносна вологість – 40…60% (допустима не більше 75%);

- швидкість руху повітря не більше 0,1 м/с.

Оцінка шкідливих і небезпечних факторів та карта умов праці для робочого місця працівника лабораторії представлені в таблиці 3.1.

Таблиця 3.1 – Оцінка факторів виробничого та трудового процесу працівника лабораторії

№ п/п	Фактори виробничого середовища та трудового процесу	Нормативне значення	Фактичне значення	III клас: шкідливі та небезпечні умови, характер праці			Час дії фактора
				I ступінь	II ступінь	III ступінь	
1	Шкідливі хімічні речовини, мг/м^3: I клас небезпеки _____ II клас небезпеки _____ III-IV клас небезпеки _____						
2	Пил переважно фіброгенної дії, мг/м3						
3	Вібрація (загальна і локальна), дБ						
4	Шум, дБА						
5	Інфразвук, дБ						
6	Ультразвук, дБ						
7	Неіонізуючі випромінювання: - радіочастотний діапазон, В/м - діапазон промислової частоти, кВ/м - оптичний діапазон (лазерне випромінювання), Вт/м^2						
8	Мікроклімат в приміщенні: - температура повітря, °С (тепл. п) - швидкість руху повітря, м/с - відносна вологість повітря, % - інфрачервоне випромінювання, Вт/м^2	 23 – 25 ≤ 0 ,2 40 – 60 100	 23 0,1 60				 100 100 100
9	Важкість і напруженість праці	категорія важкості праці - легка, категорія напруженості праці - мало напружена					

Аналіз шкідливих і небезпечних факторів дозволяє зробити висновок, що умови праці в лабораторії характеризуються наявністю нешкідливих виробничих чинників, які не призводять до зростання захворюваності з втратою працездатності та проявом початкових ознак професійної патології.

На ділянці проведення експерименту значна частина моделювання вироблялася на персональному комп'ютері IBM PC і макетному стенді, оснащеному блоками живлення, програмованими пристроями вхідних дій, реєструючим і вимірювальним устаткуванням. Печатні плати виготовлялися за технологією травлення фольгованого текстоліту на спеціальному стенді з витяжною шафою, розташованому в науково-дослідній лабораторії кафедри.

Тривала робота перед екраном монітора наводить до різних функціональних розладів організму, навантаження на очі. Захворювання поступово накопичуються. В основному страждають кисті, зап'ястя, плечі, шийна область.

3.2 Заходи з поліпшення умов праці. Виробнича санітарія

При проведенні моделювання схеми приладу, якість експерименту багато в чому залежить від освітлення, тому в лабораторії має бути передбачене штучне освітлення.

Незадовільне освітлення може спотворити інформацію, крім того, викликає стомлення організму в цілому. Неправильне освітлення може з'явитися причиною травматизму [7].

Залежно від класу приміщення по вибухонебезпеці і від чистоти середовища виробничих приміщень, визначається схема розташування світильників, їх марка і конструктивного виконання.

Для освітленості приміщення з розмірами А = 8,5 м, В = 5,9 м та висотою Н = 3,5 м використовуються 6 світильників з чотирма лампами розжарювання. Коефіцієнти віддзеркалення світлового потоку від стелі, стін і підлоги відповідно рівні: $p_{стелі}$ = 70%, $p_{ст.}$ = 50%, $p_{полу}$ = 10%. Затінювання робо-

чих місць немає. Висота світильника h_c = 0,9 м, висота робочої поверхні над рівнем підлоги h_p = 0,8м. Нормативна величина освітленості робочих місць з відео-терміналами складає $E_н$ = 300…500 лк.

В даному приміщенні освітленість 350…500 лк.

При монтажі компонентів на плату і формуванні топологічного рисунка струмопровідного шару виникає потенційна небезпека небажаної дії на організм речовин, що звертаються в технологічному процесі, і матеріалів. Всі речовини, що забруднюють повітря, надають шкідливу дію, якщо вони потрапляють в організм в кількостях, що перевищують деяку порогову величину (ГДК). У виробництві плат застосовують певні речовини, які шкідливі для організму. Клас небезпеки шкідливих речовин встановлюється залежно від гранично допустимої концентрації речовин в повітрі робочої зони. Це та концентрація яка переноситься без відхилень від нормального стану в перебігу робочого дня при щоденному диханні. Згідно СН 245-71 встановлюють чотири класи шкідливих речовин: 1-й клас – речовини надзвичайно небезпечні; 2-й клас – речовини високо небезпечні; 3-й клас – речовини помірно небезпечні; 4-й клас – речовини мало небезпечні. Дія токсичних речовин виявляється в гострих і хронічних отруєннях .

При монтажі електронних плат застосовують ацетон, етиловий спирт для знежирення і очищення від пилу мікросхеми, а також олово і каніфоль для припаювання ніжок напівпровідникового приладу до плати. Спирт, ацетон викликає сухість шкіри. При систематичному вдиханні можливі захворювання сітківки ока. Також можливі нервово - психічні захворювання.

Каніфоль дратівливо діє на слизисті оболонки дихальних шляхів і на шкіру, що наводить до дерматитів.

Основні засоби техніки безпеки – герметизація апаратури і устаткування, наявність припливний витяжній вентиляції в приміщенні проведення робіт і витяжна шафа для виготовлення печатних плат і монтажу компонентів паянням (рис. 3.2).

Витяжна шафа оснащена вентилятором моделі CE 140L-125. Вентилятор має крильчатки із заломленими вперед лопатками і двигун із зовнішнім ротором. Корпус виготовлений з листової сталі, що гальванізується. Для захисту двигуна від перегріву вентилятор оснащений вбудованими термоконтактами з ручним перезапуском.

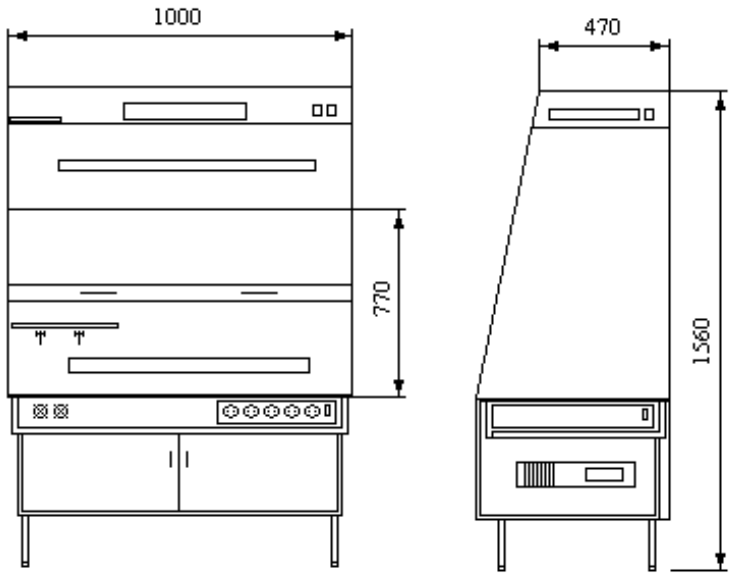


Рисунок 3.2 – Витяжна шафа для виготовлення печатних плат

У виробничих приміщеннях, в яких робота на відео терміналах і персональних комп'ютерах є допоміжною, температура, відносна вологість і швидкість руху повітря на робочих місцях повинні відповідати діючим санітарним нормам мікроклімату виробничих приміщень.

У виробничих приміщеннях, в яких робота на відео терміналах і персональних комп'ютерах є основною, повинні забезпечуватися оптимальні параметри мікроклімату відповідно до таблиці 3.2 [8].

До категорії 1а відносяться роботи, які виконуються сидячи і що не вимагають фізичної напруги, при яких витрата енергії складає до 120 ккал/ч. До категорії 1б відносяться роботи, які виконуються сидячи, стоячи або пов'язані з ходьбою і супроводяться деякою фізичною напругою, при яких витрата енергії складає від 120 до 150 ккал/год.

Таблиця 3.2 - Оптимальні норми мікроклімату для приміщень з відеотерміналами і персональними комп'ютерами

Період року	Категорія робіт	Температура повітря, °С (не більше)	Відносна вологість повітря %	Швидкість руху повітря м/с
Холодний	Легка – 1а	22-24	40-60	0.1
Теплий	Легка – 1а	23-25	40-60	0.1

У приміщенні проведення експерименту підтримується мікроклімат відповідний нормативам, для категорії робіт «Легка – 1а»

Ергономічне розташування робочого міста за персональним комп’ютером оцінюється вимогами:

- до візуальних параметрів засобів відображення інформації індивідуального користування;

- до емісійних параметрів ПК - параметрів випромінювань дисплеїв, системних блоків, джерел живлення, зокрема безаварійного, і ін.

Робота з дисплеями при неправильному виборі яскравості і освітленості екрану, контрастності знаків, квітів знаку і фону, за наявності відблисків на екрані, тремтіння і мигтіння зображення - приводить до зорового стомлення, головних болів, до значного фізіологічного і психічного навантаження, до погіршення зору [8].

Візуальні параметри і світловий клімат визначають зоровий дискомфорт, який може виявлятися при використанні будь-яких типів екранів дисплеїв, - на електронно-променевих трубках, рідкокристалічних, газорозрядних, електролюмінесценціях панелях або на інших фізичних принципах.

3.3 Електробезпека

Для забезпечення захисту від поразки електричним струмом у використовуваних електроустановках повинні застосовуватися технічні способи і засоби захисту [7].

Приміщення за ступенем небезпеки ураження людей електричним струмом відповідно до ПВЕ являється приміщенням без підвищеної небезпеки. Приміщення сухе, добре опалюване з струмонепровідною підлогою, з температурою 18…24 °С, з вологістю 40…50%. З електроустаткувань в ньому знаходяться відео термінальні пристрої та учбові стенди, які знаходяться під напругою U = 220 В, частотою f = 50 Гц.

Вибір того або іншого способу або засобу захисту (або їх поєднань) в конкретному електроприладі, і ефективність його вживання залежать від цілого ряду чинників, у тому числі від:

- номінальної напруги;

- роду, форми і частоти струму використовуваного приладу;

- способу електропостачання (від стаціонарної мережі, від автономного джерела живлення електроенергією);

- вигляду виконання (стаціонарні, пересувні, переносні);

- умов зовнішнього середовища;

- схеми можливого включення людини в ланцюг протікання струму (прямий однофазний, прямий двофазний дотик; включення під напругу кроку);

- вигляду робіт (монтаж, наладка, випробування) і ін.

Основними технічними засобами захисту є:

- захисне заземлення;

- автоматичне відключення живлення (занулення);

- пристрої захисного відключення;

- ізоляція струмопровідних частин.

Принцип роботи ПЗВ (рис. 3.3) полягає в тому, що воно постійно контролює вхідний сигнал і порівнює його з наперед заданою величиною. Якщо вхідний сигнал перевищує встановлене значення, то пристрій спрацьовує і відключає захищену електроустановку від мережі. Як вхідні сигнали пристроїв захисного відключення використовують різні параметри електричних

мереж, які несуть в собі інформацію про умови поразки людини електричним струмом.

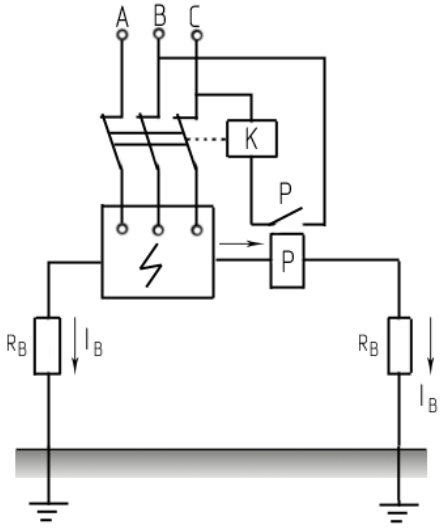


Рисунок 3.3 - Проста схема пристрою захисного відключення

Основними елементами будь-якого пристрою захисного відключення є датчик, перетворювач і виконавчий орган.

Основними параметрами, по яких підбирається те або інші ПЗВ є: номінальний струм навантаження, тобто робочий струм електроустановки, який протікає через нормально замкнуті контакти ПЗВ в черговому режимі; номінальна напруга; встановлене значення напруги; час спрацьовування пристрою.

3.4 Пожежна безпека. Техногенна безпека

Виробництво напівпровідникових приладів, згідно ДБН В.1.1–7–2002, відноситься до категорії Б, оскільки це виробництво зв'язане із застосуванням речовин спирту і ацетону з температурою спалаху пари від 28 до 60°С горючих газів. Для зниження пожежної небезпеки використовують обмежену кількість матеріалів які обертаються в процесі, зберігаються, здатні горіти [8].

Характерними причинами виникнення пожеж в лабораторії є необережне поводження з вогнем, порушення технологічних процесів, неправильні

електропроводки і устаткування, неправильне користування електричними приладами і ін. Для лабораторії встановлена категорія пожежної небезпеки В.

Основні будівельні конструкції будівлі, в якій знаходиться ділянка, виконані з тих, що не згорають і важко згорають матеріалів, що цегельних і виштукатурюють. Отже, вогнестійкість будівлі має 2 рівень. Для евакуації людей на випадок пожежі, згідно ДБН В.1.1–7–2002, в лабораторії є два евакуаційні виходи, розташованих в протилежних кінцях приміщення ділянки. Ширина дверей і сходів рівна 1,6 м, що відповідає нормі.

Відстань від найбільш видаленого робочого місця до найближчого виходу – 15 м. Швидкість пересування людей при евакуації – 16 м/мін.

Згідно правилами влаштування електроустановок ПВЕ, будівля, в якій знаходиться ділянка по заходах захисту від блискавок, відноситься до категорії 3 і захищається від прямих ударів блискавок, і від замету високих потенціалів через землю, тобто підземні металеві комунікації приєднуються при введенні в об'єкт, що захищається, до заземлювачів електроустаткування. Отже, грозозахист заснований на стержневих громовідводах.

Для попередження пожеж на ділянці необхідно створити строгий протипожежний режим. Створюється загально об'єктова і лабораторна інструкція по ПБ, проводиться первинний протипожежний інструктаж на робочому місці; створюється план протипожежних заходів і евакуації людей на випадок пожежі.

Як вогнегасні речовини можна застосовувати воду, вуглекислоту, хімічну і повітряно-механічну піну. Для гасіння вогнищ усередині будівлі на майданчиках сходових кліток, в коридорах і отворі встановлюють пожежні крани, які розміщені в шафах, де знаходиться і рукав з протипожежним стволом. Для гасіння пожеж електроустановок використовується вуглекислий вогнегасник ОУ-2, в кількості двох вогнегасників на приміщення. Існують пожежна електрична сигналізація, яка забезпечує прямий зв'язок пожежної охорони з охоронним об'єктом. У даній будівлі застосовують звукову систему сигналізації. При появі сигналу сповіщення про пожежу співробітники лабо-

раторії № 216 організовано без паніки покидають лабораторію і, залежно від місця спалаху, слідують або вліво через лабораторний корпус для виходу на вулицю Добролюбова, або управо для виходу на вулицю Незалежної України (рис. 3.4).

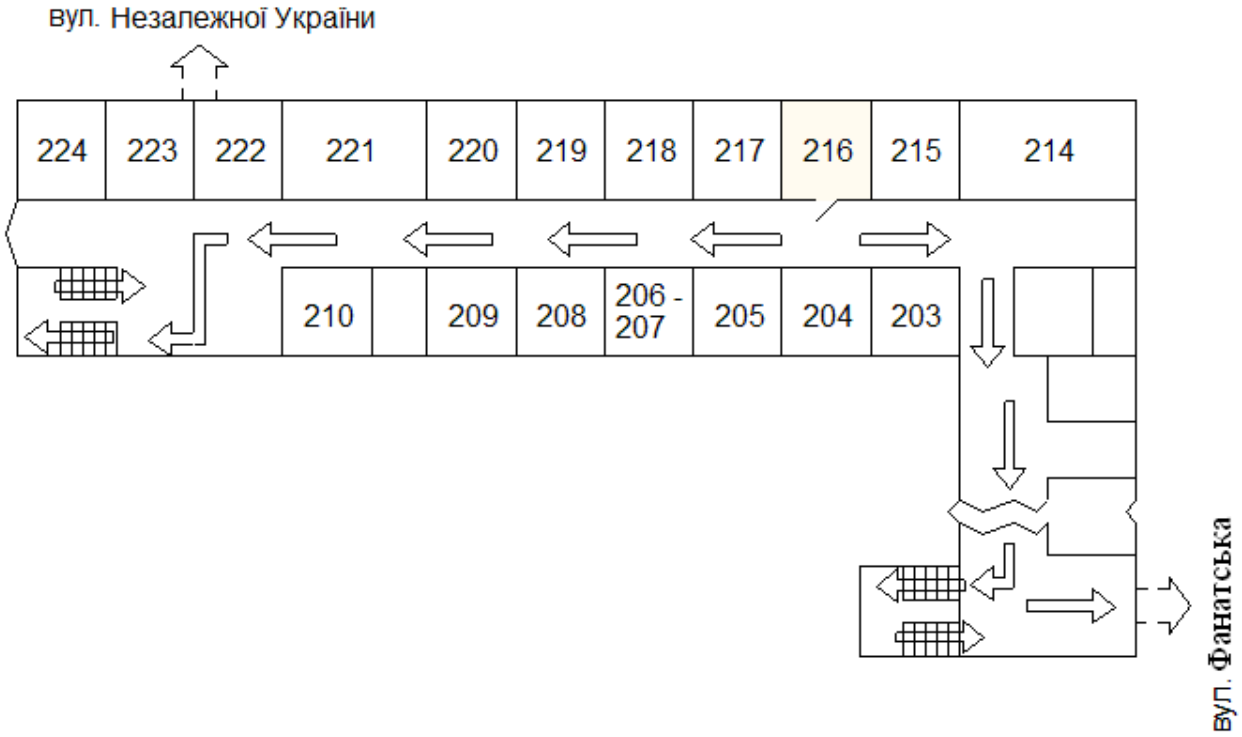


Рисунок 3.4 – План евакуації при пожежі із аудиторії № 216

3.5 Розрахунок захисного заземлення

Заземленню підлягають вимірювальні установки, напруга живлення яких 220 В. У якості заземлювача візьмемо сталеві вертикальні стержні довжиною l = 2,5 м, діаметром d = 0,04 м, діаметр сполучної смуги b = 0,04 м. Контур заземлення розташовано на горизонтальному майданчику біля корпусу академії. Грунт – суглинок. Допустимий опір заземлюючого пристрою ($R_н$) дорівнює 4 Ом. Визначимо питомий електричний опір ґрунту (суглинку), ρ якого дорівнює 100 Ом·м [8].

Розрахуємо опір розтікання струму одного вертикального стержня:

$$R_{в} = \frac{\rho}{2\pi\pi} \cdot \ln\frac{4 \cdot l}{d} = \frac{100}{2 \cdot 3{,}14 \cdot 2{,}5} \ln\frac{4 \cdot 2{,}5}{0{,}04} = 35{,}1О5$$

Приймемо число заземлювачів:

$$n = \frac{R_{l}}{R_{n}} = \frac{35{,}1}{4} = 8{,}775 \approx 9$$

Визначимо довжину горизонтальної смуги (по контуру):

$$l_{г} = a \cdot n,$$

де а – відстань між вертикальними електродами (а = 2 м)

$$l_{г} = 2 \cdot 9 = 18 \text{ м}$$

Опір горизонтальної смуги:

$$R_{2с} = \frac{\rho}{\pi \cdot l_{г}} \cdot \frac{4 \cdot l_{г}}{b} = \frac{100}{3{,}14 \cdot 18} \cdot \ln\frac{4 \cdot 18}{0{,}04} = 13{,}2 \text{ Ом}$$

Коефіцієнт екранування для вертикального заземлювача:

$$\eta_{в} = \frac{0{,}68 + 0{,}56}{2} = 0{,}62$$

і для горизонтальної смуги

$$\eta_{г} = \frac{0{,}34 + 0{,}4}{2} = 0{,}37$$

Опір групи вертикальних заземлювачів:

$$R_{гр} = \frac{R_{вз}}{n \cdot \eta_{в}} = \frac{35{,}1}{9 \cdot 0{,}62} = 6{,}3 \text{ Ом}$$

Опір горизонтальної смуги з врахуванням екранування:

$$R_{г} = \frac{R_{го}}{\eta_{г}} = \frac{13{,}2}{0{,}37} = 35{,}6 \text{ Ом}$$

Опір заземлювача в цілому:

$$R_{з} = \frac{R_{гр} \cdot R_{г}}{R_{гр} + R_{г}} = \frac{6{,}3 \cdot 35{,}6}{6{,}3 + 35{,}6} = 5{,}3 \text{ Ом}$$

Як видно, опір заземлювача перевищує нормативний (4 Ом), тому збільшимо кількість заземлювачів:

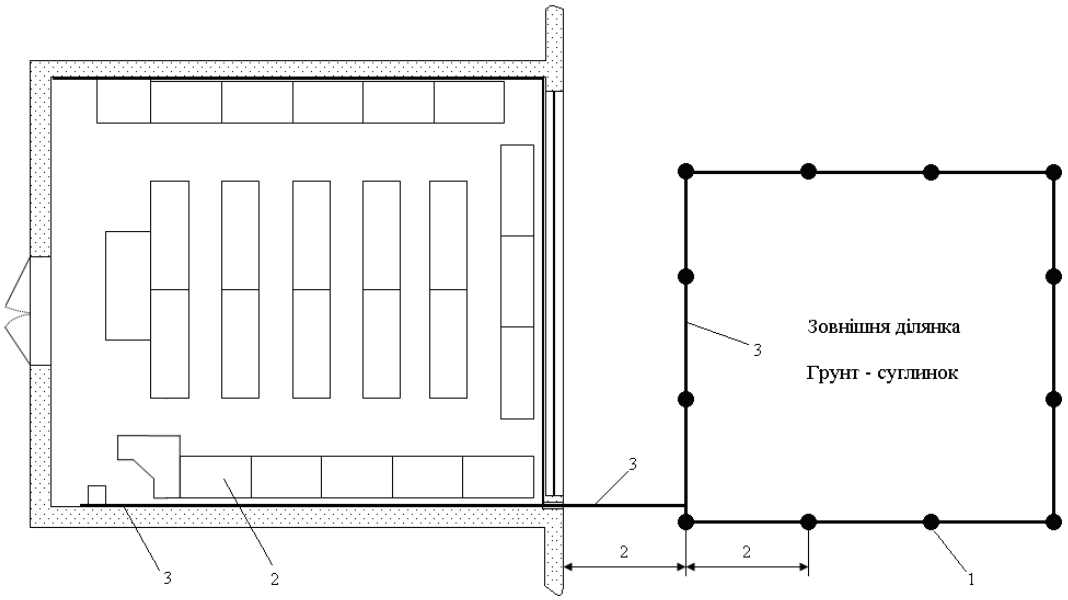
$$n = 10,$$

тоді опір заземлювача в цілому складе $R_з = 4,6$ Ом, що теж більше $R_н$.

Якщо n = 11, то $R_з = 4,2 > R_н$.

Якщо n = 12, то $R_з = 3,99 < R_н$.

Число заземлювачів дорівнює 12, які розміщені по контуру зовнішньої ділянки, як показано на рисунку 3.5.



1 – заземлювачі

2 – електроустаткування що заземлюється

3 – сполучна смуга

Рисунок 3.5 – Розміщення заземлюючих електродів на зовнішній ділянці та сполучної смуги лабораторії проведення експерименту

Таким чином, для виконання захисного заземлення використовується 12 вертикальних стержнів діаметром 0,04 м, завдовжки 2,5 м, кожен з яких має опір 31,5 Ом. Опір сполучної смуги 13,2 Ом. Опір заземлювачів в цілому складе 3,99 Ом, що забезпечує безпечну роботу на установках лабораторії.

Висновки та рекомендації

1. Розроблена конструкція світлочутливої матриці з використанням чотирьох фото транзисторів забезпечує отримання трекером сигналів позиціювання прийомних панелей на сонце з більшою ефективністю в зрівнянні з існуючими аналогами.

2. Розроблена схема трекера з логічним керуванням направлення обертання електродвигунів дозволяє орієнтувати прийомні панелі геліоустановки на сонце, незалежно від їх розташування в період затемненого часу доби.

3. Автономне живлення дозволяє функціонувати трекеру незалежно від зовнішніх мереж.

4. Аналіз функціонування схеми електричної трекера дозволяє переконатися в правильності перемикання сигналів, що управляють направленням обертання електродвигунів.

Рекомендується використовувати розроблену схему та конструкцію трекера в промислових та побутових приладах перетворення сонячної енергії.

Перелік посилань

1. Рябенький В.М., Жуйков В.Я., Гулий В.Д.. Цифрова схемотехніка: навчальний посібник. Львів : "Новий Світ-2000", 2019. 736 с. ISBN 978-966-418-067-9.

2. Сєдов С. О. Аналогове оброблення сигналів. Схемотехніка. Розрахунки : підручник. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. 298 с.

3. Воробйова. О. М., Іванченко В. Д.. Основи схемотехніки: підручник. [2-е вид.]. Одеса : Фенікс, 2009. 388 с.

4. Верьовкін Л.Л., Світанько М.В., Кісельов Є.М., Хрипко С.Л. Цифрова схемотехніка: Підручник. Запоріжжя : ЗДІА, 2016. 214 с. ISBN 978-617-685-023-6

5. Pedroni V., Circuit Design and Simulation with VHDL, 2nd ed., MIT Press, 2010. 345 p.

6. Кожемякін Г.Б., Рижков В.Г., Бєлоконь К.В. Охорона праці та техногенна безпека: методичні вказівки до виконання розділу магістерських робіт для студентів ЗДІА всіх спеціальностей денної та заочної форм навчання. – Запоріжжя : ЗДІА, 2012. 48 с.

7. Ткачук К.Н. Охорона праці і довкілля в радіоелектронній промисловості. Київ : Вища шк., 1988. 240 с.

8. Горобець А.И., Степаненко А.И. Охорона праці в радіоелектронній промисловості. Київ : Техніка, 1987. 345 с.