МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Інженерний навчально-науковий інститут ім. Ю. М. Потебні

Кафедра мікроелектронних та електронних інформаційних систем

Пояснювальна записка

до кваліфікаційної роботи

рівень вищої освіти_____*перший (бакалаврський) рівень*_____
(перший (бакалаврський) рівень)

на тему *Розробка генератора випадкових чисел*_____
_____
_____

Виконав: студент (ка) __*IV*__ курсу, групи *МН-17-1бд*

_____*Полуєктов К.В.*_____
(прізвище та ініціали) (підпис)

Напряму підготовки_____
(шифр)

Спеціальності _____*153*_____

_____*Мікро- та наносистемна техніка*_____
(назва)

Керівник _____*доцент, к.т.н., доцент*_____

_____*Ніконова Аліна Олександрівна*_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент _____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

м. Запоріжжя - 20*22* рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Інженерний навчально-науковий інститут ім. Ю. М. Потебні

Кафедра *Мікроелектронних та електронних інформаційних систем*

Рівень вищої освіти *перший (бакалаврський) рівень*
(перший (бакалаврський) рівень, другий (магістерський) рівень)

Напрям підготовки _____
(шифр)

Спеціальність *153 Мікро- та наносистемна техніка*
(назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри *MEEIC*

Критська Т. В.

"*28*" *травня* *2022* року

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

Полуєктов Кирило Віталійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Розробка генератора випадкових чисел*

керівник проекту (роботи) *Ніконова Аліна Олександрівна, доцент, к.т.н.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "*17*" *січня 2022* року *№90-с*

2. Строк подання студентом проекту (роботи) *28 травня 2022 р.*

3. Вихідні дані до проекту (роботи) *Генератор чисел від 0 до 15, лічильник імпульсів, перетворювач двійкового коду чисел в код семисегментних індикаторів, 155 серія мікросхем ТТЛ логіки*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Дослідження загальних принципів функціонування та побудови генераторів випадкових чисел. Розробка схеми генератора випадкових чисел. Охорона праці та техногенна безпека при розробці генератора випадкових чисел*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) *Функціональна схема генератора випадкових чисел. Моделювання функціонування лічильника генератора випадкових чисел. Схема генератора випадкових чисел.*

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата завдання прийняв
I	*Ніконова А. О., доцент*	*20.05.2022*
II	*Ніконова А. О., доцент*	*24.05.2022*
III	*Ніконова А. О., доцент*	*26.05.2022*

7. Дата видачі завдання *14 лютого 2022 року*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	*Схемні рішення генераторів чисел*	*27.02.2022*	
2	*Особливості теорії випадкових чисел*	*06.03.2022*	
3	*Схеми генераторів випадкових чисел*	*13.03.2022*	
4	*Розрахунок схеми генератора тактових імпульсів*	*27.03.2022*	
5	*Розрахунок схеми лічильника*	*03.04.2022*	
6	*Розрахунок схеми перетворювача коду*	*17.04.2022*	
7	*Розрахунок схеми генератора випадкових чисел*	*08.05.2022*	
8	*Охорона праці та техногенна безпека*	*15.05.2022*	
9	*Оформлення пояснювальної записки*	*22.05.2022*	
10	*Підготовка графічного матеріалу*	*27.05.2022*	
11	*Оприлюднений захист дипломної роботи*	*21.06.2022*	

Студент _____ *Полуєктов К. В.*
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ *Ніконова А. О.*
(підпис) (прізвище та ініціали)

Нормоконтроль пройдено _____ *Верьовкін Л. Л.*
(підпис) (прізвище та ініціали)

Реферат

Дипломна робота містить 64 сторінки, 39 рисунків, 11 таблиць, 14 джерел літератури.

Об’єкт дослідження – схеми генераторів випадкових чисел.

Мета роботи – розрахунок схеми генератора випадкових чисел з діапазоном від 0 до 15 та фіксацією результату на індикаторах.

Задачі роботи – розробити функціональну схему генератора; розробити електричну схему генератора; провести аналіз функціонування розробленого пристрою.

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

Короткий виклад результатів досліджень – проведений аналіз проблем, які виникають при рішенні задач отримання випадкової інформації, дозволив розробити оптимальну функціональну схему генератора випадкових чисел.

Результати впроваджень – електронна модель приладу пройшла випробовування на кафедрі МЕЕІС.

Прогнозні пропозиції – рекомендується для впровадження в системах кодування інформації.

ДЕШИФРАТОР, ГЕНЕРАТОР, МОДЕЛЮВАННЯ, ЛІЧИЛЬНИК, ПЕРЕТВОРЮВАЧ КОДУ, ІНДИКАТОР, МІКРОСХЕМА

Дипломну роботу виконано на кафедрі мікроелектронних та електронних інформаційних систем з 14.02.2022 р. по 28.05.2022 р.

Зміст

Вступ

Генератор випадкових чисел (Random number generator) – обчислювальний або фізичний пристрій, розроблений для генерації послідовності номерів чи символів, які не відповідають будь-якому шаблону, тобто є випадковими.

Випадкові числа використовуються у наступних областях науки і техніки.

1. Соціологічні та наукові дослідження. Підготовка випадкових вибірок при зборі даних, опитуванні думок або в дослідженні фізичних явищ з випадковим вибором результатів експериментів.

2. Моделювання. У комп'ютерному моделюванні фізичних явищ. Крім того, математичне моделювання використовує випадкові числа як один з інструментів чисельного аналізу.

3. Криптографія та інформаційна безпека. Випадкові числа можуть використовуватися в тестуванні коректності або ефективності алгоритмів і програм. Багато алгоритмів використовують генерацію псевдовипадкових чисел для вирішення прикладних завдань (наприклад, криптографічні алгоритми шифрування, генерація унікальних ідентифікаторів та ін.).

4. Прийняття рішень в автоматизованих експертних системах. Використання випадкових чисел є частиною стратегій прийняття рішень.

5. Оптимізація функціональних залежностей. Деякі математичні методи оптимізації використовують стохастичні методи для пошуку екстремумів функцій.

6. Розваги та ігри. Випадковість в іграх має значну роль. У комп'ютерних або настільних іграх випадковість допомагає урізноманітнити ігровий процес.

З появою електронних схем з'явилися електронні генератори випадкових чисел. Один з перших таких генераторів, запропонований А. М. Тьюрингом, використовував резисторний генератор шуму для отримання 20 випадкових біт, які надходили на суматор. Однак генератори випадкових чисел не

завжди давали якісні результати. Крім того, апаратні генератори випадкових чисел нерідко давали збої. Таблиці випадкових чисел, обчислених заздалегідь, були вкрай незручні у використанні у зв'язку з обмеженістю комп'ютерної пам'яті.

Зростання можливостей комп'ютера, збільшення щільності запису на магнітних і оптичних носіях дозволило скласти досить великі таблиці випадково згенерованих бітів.

Актуальним являється розробка цифрових пристроїв для прийняття рішень інформаційної безпеки алгоритмів спрацювання автоматизованих приладів мікро- та наносистемної техніки.

1 Дослідження загальних принципів функціонування та побудови генераторів випадкових чисел

Двійковим (булевим) n-мірним вектором називають набір з n чисел (b^0, b^1, b^2, ..., b^n),, кожне з яких може приймати тільки значення в двійковій системі числення 0 або 1 [1].

Двійковий вектор називають зворотним (інвертованим) до, якщо він утворений з заміною всіх нулів одиницями, а одиниць - нулями.

Наприклад: якщо (0, 1, 1, 1, 0, 1), то (1, 0, 0, 0, 1, 0).

Якщо в запису двійкового вектора довжиною n усунути коми, то його можна розглядати як двійковий запис деякого цілого числа. Найменшим таким числом є нуль. Йому відповідає вектор (0, ..., 0). Найбільшим є число 2^n-1, якому відповідав би вектор (1, ..., 1). Отже, за допомогою повного набору двійкових векторів довжиною n можна записати все 2^n цілих чисел з відрізка [0, 2^n - 1]. Такі числа називають порядковими номерами векторів. Їх використовують як в двійковому вигляді, так і в десятковій системі числення. Двійковий запис довільного числа можна розглядати як послідовність двійкових чисел [1].

Послідовність називається випадковою, якщо відтворити її, знаючи алгоритм і всі вихідні дані не представляється можливим (двічі запустивши генератор в тих же умовах ми отримаємо різні послідовності). Але комп'ютерні системи детерміновані, тобто вони можуть мати лише кінцеву кількість станів. Це призводить до того, що послідовності які генеруються ними і будуть періодичні - такі послідовності називаються псевдовипадковими.

Зважаючи на вище зазначене отриману двійкову послідовність довжиною n можна розглядати як двійковий запис випадкового або псевдовипадкового двійкового вектору. Вектор буде випадковим або псевдовипадковим яким чином була здійснена генерація вектору.

Генерація може бути здійснена двома основними способами [1]:

- шляхом використання пристроїв в основу роботи яких покладено використання різноманітних фізичних явищ таких як дробовий шум, радіоактивний розпад та інші;

- використання програмного забезпечення або цифрових апаратів які реалізують детерміновані алгоритми знаходження всіх чисел, які складають двійковий запис вектору.

В залежності від методу генерації двійкових векторів, алгоритмів роботи генераторів (програмних чи апаратних) будемо отримувати або випадкові або псевдовипадкові двійкові вектори.

Види генераторів випадкових чисел:

- апаратні;

- табличні;

- алгоритмічні.

Табличні генератори в якості джерела випадкових чисел використовують заздалегідь підготовлені таблиці, які містять перевірені некорельовані числа і не є генераторами в суворому розумінні цього поняття. Недоліки такого способу очевидні: використання зовнішнього ресурсу, обмеженість послідовності, зумовленість значень.

Апаратні генератори (істинно) випадкових послідовностей повинні володіти джерелом ентропії. Розробка генераторів, які використовують джерела ентропії, генеруючих не корельовані і статистично незалежні числа - досить складне завдання. Крім того, для більшості криптографічних додатків такий ГПВЧ не повинен бути предметом вивчення і впливів іншої сторони.

Алгоритмічний генератор є комбінацією фізичного генератора і детермінованого алгоритму. Такий генератор використовує обмежений набір даних, отриманих з виходу фізичного генератора, для створення довгої послідовності чисел ляхом перетворення вихідних чисел.

1.1 Апаратні генератори випадкових чисел

З ряду причин всі програмні реалізації генераторів випадкових чисел варто правильно називати виняткова генераторами псевдовипадкових чисел. Навіть якісний програмний генератор завжди буде підпадати під визначення Гейла Гесрема, автора одного із самих потужних програмних інструментальних комплектів, призначених для тестування апаратних генераторів випадкових чисел (АГВЧ): «Ніщо не випадкове, а тільки не визначене». Для розроблювачів систем шифрування з високої кріптостійкістю це твердження є синонімом. Для цього необхідні незвичайні периферійні пристрої – апаратні генератори випадкових чисел. Найпростіші АГВЧ засновані на тих властивостях елементів електронних схем, з якими так довго й завзято боролися інженери-схемотехніки. Це властивість - власні шуми електронного приладу - завжди доставляло чимало турбот при проектуванні високочутливої електроніки. Але при розробці АГВЧ "шумливий" елемент є ключовим. Будь то незграбно виготовлений резистор, фотодіод або звичайний діод - він у тому або іншому ступені придатний для створення АГВЧ (рис. 1.1) [2].

Рисунок 1.1 - АГВЧ на основі мікросхеми підсилювача й формувача сигналів інтерфейсу RS-232

Досить забезпечити цьому елементу такий режим роботи, при якому його шумові параметри по класиці електроніки будуть найгіршими, і можна чекати дуже непоганого результату: посилення сигналів власного шуму елемента й перетворення їх з аналогової в цифрову форму. Засновані на подібних принципах апаратні ГВЧ малосерійно виробляються фірмами самих різних країн (правда, не варто зваблюватися елементарністю їхньої конструкції

- як і у всіх випадках, тут ціна кінцевого виробу визначається не стільки витратами на його розробку й виготовлення, скільки співвідношенням останніх з місткістю ринку, так що коштують вони недешево) [2].

В окремий підклас подібних АГВЧ варто винести розробки засновані на тому ж принципі (використання власних шумів електронного приладу), але які радикально відрізняються складністю цього приладу. Тут замість дискретного електронного компонента застосовується куди більше складне джерело природної випадковості. Наприклад, в "відокремившемуся" від лабораторій SGI проекті Lavarnd як джерело шуму застосовується ПЗС-матриця звичайної побутової комп'ютерної відеокамери QuickCam. Поміщена в спеціальний футляр при повній відсутності світла ПЗС-матриця камери "заганяється" керуючою програмою в найгірший (як для відеокамери) режим, при якому шумові характеристики максимальні й картинка чистого, природного хаосу (для неї достатня тільки одна складова сигналу - яскравість) придатна до подальшої обробки. Нетривіальне технічне рішення дозволяє мінімізувати витрати на апаратні засоби, реалізувавши програмно весь тракт подальшого формування послідовності випадкових чисел із двомірної картини хаосу.

Другому великому класу АГВЧ найкраще підійде назва "функціональний". Тут у якості "джерела ентропії" використаються фундаментальні функціональні властивості електронних приладів, наприклад лічильників Гейгера - Мюллера. В іншому технічні нюанси побудови АГВЧ залишаються такими ж, як й у класі "паразитних" АГВЧ (хіба що можуть відрізнятися вимірювані величини, на підставі яких формуються випадкові числа, але в даній ситуації це несуттєво). Неприємною особливістю подібних пристроїв є необхідність застосування радіоізотопних джерел [2].

Третій клас АГВЧ найбільш екзотичний. Настільки екзотичний, що комерційні вироби, які можна до нього віднести, практично відсутні на ринку. Він представлений усього декількома експериментальними розробками академічної науки. "Фундаментальний" - ніяких інших підходящих слів для його назви знайти просто неможливо [1].

Найбільш яскравий представник "фундаментальних" АГВЧ - розробка групи дослідників Женевського університету "оптичний квантовий генератор випадкових чисел". Треба віддати належне академічній науці Швейцарії - незважаючи на всю "екзотику", цей АГВЧ з'єднується з комп'ютером інтерфейсом USB. У цьому АГВЧ випромінюваний надто слабким імпульсом лазерного світлодіода потік фотонів направляється у двометровий сегмент звичайного одномодового оптоволокна, що забезпечує фактично незалежність потоку фотонів на протилежному "виході" такої системи від різних флуктуацій параметрів випромінювача (рис. 1.2).

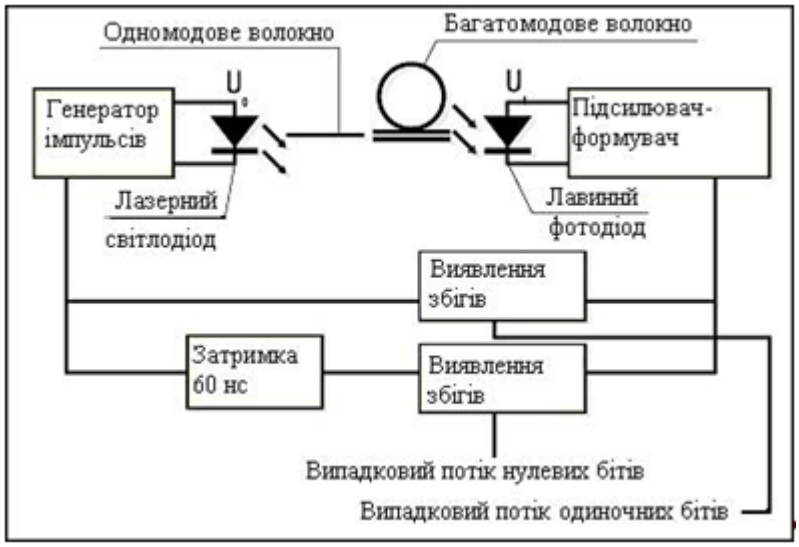


Рисунок 1.2 - Генерація випадкових чисел на фотонному рівні - блок-схема швейцарської експериментальної розробки

За "вихідним зрізом" першого сегмента оптоволокна на відстані декількох міліметрів розташовуються один до одному два оптоволоконних сегмента різної довжини, на "виході" одного з яких фотон з'являється на 60 нс пізніше. Ця затримка дозволяє "виявити хаос" – вона дає можливість визначити, по якому відрізку (короткому або довгому) багатомодового оптоволокна "пробіг" фотон, а це є справа чистого випадку. Виявлення окремих фотонів покладено на пасивно охолоджуваний кремнієвий лавинний фотодіод (Si APD). Ще один, нетривіальний пристрій, у якому фундаментальні фізичні принципи, наносекундна синхронізація й найсучасніша електроніка підлеглі

рішенню самого утилітарного завдання - одержанню випадкових чисел, які обновляються 100 тис. раз у секунду.

Четвертий клас АГВЧ можна умовно назвати "паразитним персональним-комп'ютерним". У його представниках використаються нюанси "поводження" фактично стандартних компонентів звичайного сучасного ПК (у першу чергу - звукових адаптерів. До цих нюансів ставляться, насамперед, теплові шуми й флуктуації в підсистемі аналогового вводу/виводу звукового адаптера. Привабливість представників такого класу полягає у характеристиці "cost for nothing" і в можливості розвиненої програмної реалізації самих витончених механізмів обробки для одержання майже ідеального ГВЧ. Але подібні АГВЧ (одна з найрозвиненіших розробок цього класу - АГВЧ turbid Джона Денкера) мають потребу в ретельних процедурах настроювання й калібрування [2].

В окремий клас "курйозних" АГВЧ можна виділити самі немислимі серед існуючі розробки, наприклад спеціалізованих роботів, які методично кидають звичайної грального кістки й оснащених системою технічного зору для зчитування очків, які випали. Втім, курйозність цих проектів (більші витрати на реалізацію, наднизька частота відновлення інформації на "виході" пристрою) іноді виправдується. А саме, у виробах останнього, розглянутого класу – АГВЧ-файли й АГВЧ-сервери.

АГВЧ-файли – це записані в великі файли результати роботи апаратних генераторів випадкових чисел і висококласних фахівців математичної статистики й теорії ймовірностей і потужних інструментальних засобів.

ГВЧ-сервери – це сервери публічного доступу, які дозволяють розроблювачу прикладного ПЗ не використати власний АГВЧ (наприклад, на етапах тестування й налагодження). Найбільш відомий подібний ресурс - www.random.org - надає в розпорядження програмістів сервіс АГВЧ за допомогою HTTP-протоколу або як вилучений CORBA-компонент, а також багато готових фрагментів клієнтських програм у вихідних текстах (від Perl до C#) [2].

1.2 Генератор псевдовипадкових чисел

Послідовність називається псевдовипадковою, якщо вона виглядає, як безсистемна і випадкова, хоча насправді вона створювалась з допомогою суто детермінованого процесу, відомого під назвою псевдовипадкового генератора. Подібні генератори переважно задаються деяким початковим значенням і за допомогою певних алгоритмів отримують з нього випадкові послідовності. В цьому сенсі псевдовипадкові генератори можна розглядати як розповсюджувачі випадковості [3].

Комп'ютери є детермінованими машинами, що завжди роблять саме те на що вони запрограмовані і це усуває можливість звертатися до комп'ютерів як до джерела істинної випадковості. Саме краще, на що здатний комп'ютер - це згенерувати псевдовипадкову послідовність, яка хоча і виглядає випадковою, але, насправді, такою не є. Згенерувати дійсно випадкову послідовність можна лише при апаратній реалізації генератора, який би для отримання випадкових чисел використовував деяке фізичне явище, наприклад, шум, який генерують напівпровідникові прилади, молодші біти оцифрованого звуку, інтервали між перериванням пристроїв або натисканням клавіш, температуру повітря і т.д. В сучасних потужних криптосистемах військового призначення використовують генератори випадкових чисел (ГВЧ), які є платами або зовнішніми пристроями, які підключаються до ЕОМ через порт вводу/виводу. а основними джерелами білого Гаусівського шуму є високоточне вимірювання теплових флуктуацій і запис радіоефіру на частоті вільній від радіомовлення.

Незважаючи на труднощі, які виникають при проектуванні генераторів псевдовипадкових чисел (ГПВЧ), вони широко використовуються в прикладних комп'ютерних програмах і легко компонуються з усіма типами комп'ютерних систем. Тому, на сьогоднішній день, більшість прикладних комп'юте-

рних програм використовують ГПВЧ для генерації потрібних випадкових даних.

ГПВЧ широко застосовуються в багатьох галузях, а особливо в тих, які пов'язані з використанням електронної та електронно-обчислювальної техніки. Основними сферами використання ГПВЧ є:

1. Криптографія (шифрування, розшифрування, генератор ключів);
2. Імітація моделювання (економічні дослідження, математичні дослідження, фізичні дослідження, та інші);
3. Вимірювальна техніка;
4. Розробка комп’ютерних ігор.

Оскільки збільшується передача даних через загальні і приватні мережі, стає все більш важливим захист інформації яка зберігається і передається між комп'ютерами. Один із стандартних блоків безпеки є ГВЧ.

Проблема захисту інформації є багатогранна і вирішується комплексно, з використанням великої кількості способів.

Випадкові числа - фундаментальний елемент для надання обмеженого доступу до інформації. Вони являють собою основний елемент криптографії, цифрового підпису, протоколів безпеки і іншого забезпечення надійності при зв'язку.

В галузі захисту інформації існує окремий напрям, пов’язаний з генерацією випадкових (псевдовипадкових) послідовностей, йде постійна робота по удосконаленню не тільки засобів генерації, але і теорії та термінології в цьому важливому напрямі, проводиться розробка теорії і практики тестування джерел інформаційно-телекомунікаційних мереж випадкових послідовностей, оцінки і вимірювання їх показників.

ГПВЧ також часто застосовують в імітаційному моделюванні. В багатьох випадках потрібне використання різних послідовностей випадкових чисел. Наприклад для запуску однієї і тієї ж самої програми (але використовуючи різні потоки випадкових чисел) на багатьох процесорах, з метою отримання статистично незалежних результатів на кожному процесорі, а потім ці

результати можуть бути усереднити. Але використання детермінованого алгоритму при генерації чисел є також корисним в багатьох випадках. Наприклад, при моделюванні всіх видів процесів, починаючи від автоматизації телефонних ліній і закінчуючи дорожнім рухом, вимагається, щоб послідовність псевдовипадкових чисел можна було повторити для досліджень поставленої задачі при інших параметрах.

При використанні ГПВЧ необхідно враховувати те, що вони мають бути достатньо надійними. Наприклад, електронний автомат потребує таку послідовність, яку не можна було б передбачити, знаючи попереднє значення; інакше система зазнала б невдачі, якщо б гравець визначав наступні оберти на основі аналізу моделі попередніх обертів, аналогічна ситуація при кодуванні повідомлень - потрібно забезпечити таку випадкову послідовність, щоб знаючи частину розсекреченого документа неможливо було б розсекретити весь документ.

Найчастіше ГПВЧ застосовують в криптографії. Випадковість і криптографія дуже сильно взаємопов'язані. Важко знайти добре розроблене криптографічне прикладне забезпечення, яке не використовує випадкові числа.

Криптографічні ключі, їх ініціалізація, тонкощі хешування з паролями, унікальні параметри в операціях цифрового підпису системними розробниками повинні прийматися випадковими. ГПВЧ є криптографічно сильним, якщо послідовність, яку він генерує з короткого таємного вихідного ключа, є майже такою самою, як і справжня випадкова послідовність і ніяке практично легко здійснюване обчислення не може дозволити криптоаналітику отримати яку-небудь інформацію про відкритий текст при перехопленні ним шифротексту (за виключенням хіба що дуже малої ймовірності). Для застосування в криптографічних системах ГПВЧ повинні відповідати наступним вимогам:

- послідовність, яка генерується повинна мати максимально великий період;

- послідовність, яка генерується не повинна мати схованих періодичностей;

- послідовність, яка генерується повинна мати рівномірний спектр.

Найважливішою характеристикою ГПВЧ є довжина періоду повторення, після якого випадкові числа, на виході ГПВЧ почнуть повторюватися. Другою за важливістю характеристикою ГПВЧ є його продуктивність, тобто кількість чисел, які генеруються за одиницю часу. Для окремих прикладних програм (статистичне зондування, моделювання в реальному часі і т.д.) може бути потрібною продуктивністю порядку 10^{10} – 10^{12} випадкових чисел за секунду.

Швидкий і надійний ГПВЧ може легко слугувати поточним шифром. Оскільки для шифрування інформації достатньо її побітово скласти по модулю два з випадковою послідовністю бітів. Так наприклад працює поточний шифр А5 (рис. 1.3) [4].

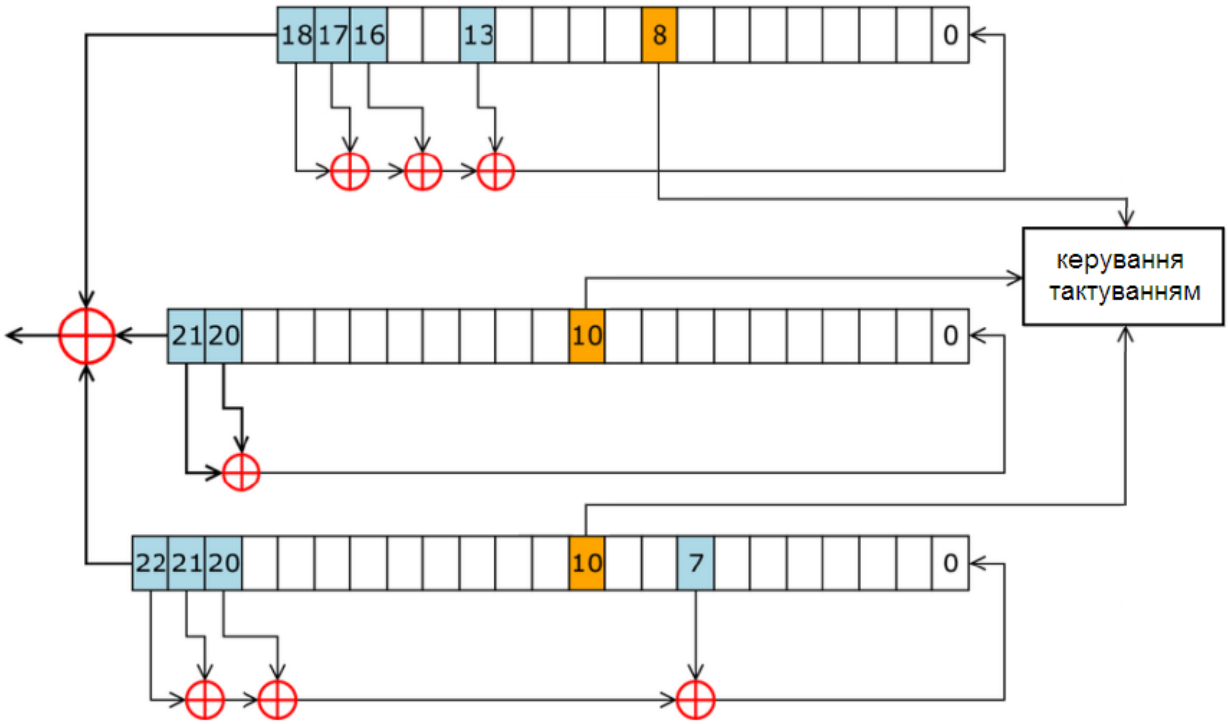


Рисунок 1.3 - Схема ГПВЧ у шифрі А5

Питанню проектування надійних і якісних ГПВЧ часто не надають належної уваги. Сама система шифрування може бути виконана на дуже висо-

кому рівні, але якщо криптографічний ГПВЧ видає ключі, які легко вгадати, то всі інші бар'єри захисту долаються без особливих зусиль. В ряді продуктів використовуються ГПВЧ, що продукують ключі, в яких відслідковується певна закономірність. В таких випадках про безпеку говорити не варто. Цікавим є те, що використання одного і того ж. генератора в деяких областях забезпечує необхідну ступінь захисту, а в інших - ні. Таким чином, необхідно підкреслити важливість криптографічного ГПВЧ – якщо він розроблений погано, то він легко може стати самим вразливим елементом системи.

Ще одна важлива галузь застосування ГВЧ - це їх застосування для контролю якості друкованих плат, окремих модулів або й цілих пристроїв [5]. Цьому питанню на сьогоднішній день приділяється не менша увага ніж застосування таких генераторів при вирішенні питань пов'язаних із захистом інформації. Наприклад в [6] автор запропонував декілька нових цікавих методик дослідження аналогових схем і електронних модулів.

Розроблена методика псевдовипадкового тестування за допомогою цифрового білого шуму з обмеженою смугою пропускання (псевдовипадкові зразки), як вхідного збуджувача. Характеристика будується, на основі обчислення взаємної кореляції між вихідною реакцією і псевдовипадковою вхідною послідовністю.

Можна зробити висновок, що, на сьогоднішній день, ГПВЧ є поширеними і мають надзвичайно важливе значення. Тому їх дослідження і удосконалення з використанням сучасних технологічних можливостей, наприклад, з використанням сучасних програмованих логічних інтегральних схем, є безумовно актуальною задачею. Також не менш важливою задачею є проведення порівняльного аналізу характеристик ГПВЧ і розроблення рекомендацій стосовно використання того чи іншого типу генераторів для конкретного використання.

Основні сфери застосування генераторів псевдовипадкових чисел приведені на рисунку 1.4 [3].

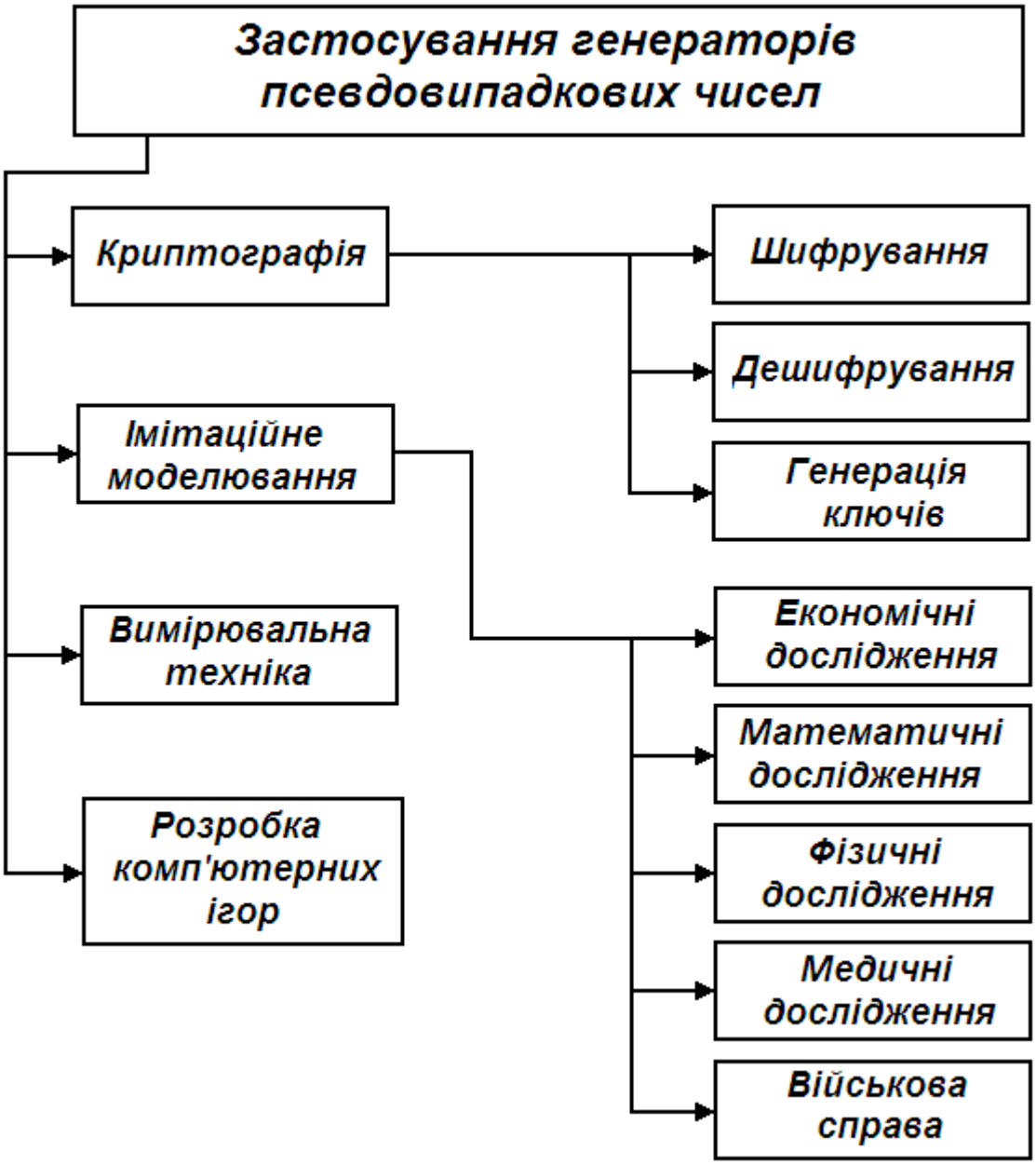


Рисунок 1.4 - Сфери застосування генераторів псевдовипадкових чисел

1.3 Схемні складові апаратних генераторів випадкових чисел

1.3.1 Вибір схеми генератора імпульсів

Генератор імпульсів призначений для формування послідовності тактових сигналів [11].

Широка зміна частоти імпульсів (близько 50 тисяч разів), що генеруються, забезпечує генератор, зібраний за схемою, що представлена на рисунку 1.5. Мінімальна частота імпульсів тут близько 0,25 Гц. Тривалість імпульсів регулюється резистором R1. Частоту дотримання можна визначити по формулі:

$$f = \frac{1}{2} R1C1,$$

Де f – частота, Гц; R1 – опір, Ом; C1 – ємність, Ф.

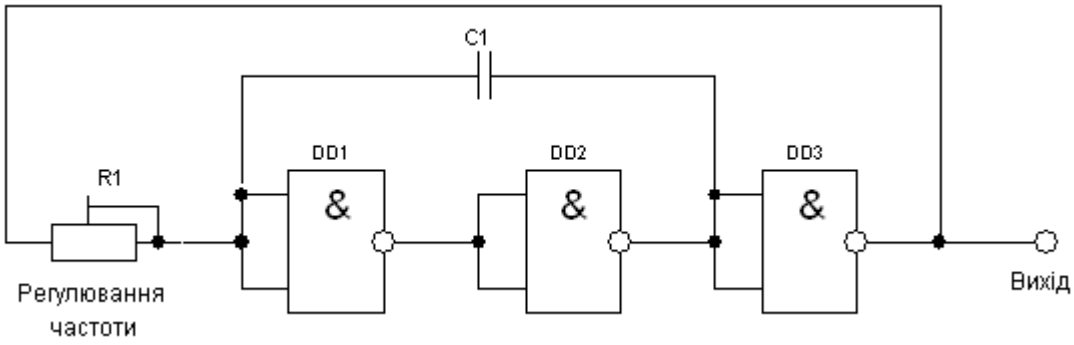


Рисунок 1.5 – Схема генератора імпульсів

1.3.2 Цифрові лічильники

Лічильником називається пристрій послідовністного типу, призначений для підрахунку числа імпульсів, що поступають на його вхід, і фіксації цього числа у вигляді коду, що зберігається в тригерах.

Лічильники - це цифрові автомати, внутрішні стани яких визначаються лише кількістю сигналів "1", що прийшли на вхід. Сигнали "0" не змінюють їх внутрішні стани [11].

Тригер Т-типу є простим лічильником, який рахує до двох. Лічильник, утворений колом з m тригерів, зможе підраховувати в двійковому коді 2^m вхідних імпульсів. Кожен з тригерів в цьому колі називають розрядом лічильника. Для установки початкового стану лічильника (скидання в нуль) зазвичай передбачається вхід скидання.

Основна характеристика лічильника – модуль рахунку, або ємність лічильника $К_{рах.}$. Це кількість вхідних сигналів, які повертають лічильник у вихідний стан. Лічильник, що не має додаткових зв'язків, має модуль рахунку $К_{рах.} = 2^n$. Лічильники, що мають модуль рахунку 2^n, називаються двійковими. Якщо $К_{рах.} \neq 2^n$, то лічильник називається недвійковим. Лічильники відрізняються один від одного кодом, в якому вони працюють. Код завжди буває двійковим, але може мати різні ваги розрядів, наприклад вага 8 – 4 – 2 – 1 або 5 – 2 – 1 – 1 і тому подібне. Одним з недвійкових є двійково-десятковий лічильник, в якому значення кожного розряду десяткового числа кодується двійковим кодом [11].

За призначенням лічильники можуть бути підсумовуючими, віднімаючими і реверсивними. Підсумовуючі лічильники виконують складання числа імпульсів, що поступають на вхід, з тим числом, яке зберігалося в ньому. Віднімаючі лічильники виконують віднімання числа імпульсу, що поступає, з початкового числа, записаного в ньому заздалегідь. Реверсивні лічильники можуть виконувати як додавання, так і віднімання імпульсів, що поступають на вхід, залежно від управляючих сигналів, що змінюють режим роботи лічильника.

За способом організації внутрішніх зв'язків лічильники можуть бути: з послідовним перенесенням, з паралельним перенесенням, з комбінованим перенесенням, кільцеві.

Лічильники бувають синхронними, тобто, коли рахункові імпульси подаються на рахункові входи всіх тригерів, і асинхронними - коли сигнал на рахунковий вхід якого-небудь тригера подається з виходу одного з тригерів молодших розрядів.

Для підвищення швидкодії лічильники виконуються синхронними з паралельним перенесенням (або паралельні). Їх особливість полягає в тому, що виходи всіх попередніх розрядів з'єднуються з входами тригера подальшого розряду, тому тривалість перехідного процесу визначається лише три-

валістю перехідного процесу одного розряду і не залежить від кількості тригерів. Звідси випливає, що паралельні лічильники – синхронні.

Структура паралельного лічильника не настільки очевидна, як структура послідовного лічильника. Для її виявлення необхідна певна процедура синтезу. Як приклад, синтезуємо двійковий паралельний лічильник з $K_{рах.} = 16$.

Процедура синтезу включає наступні операції.

1) визначається необхідна кількість розрядів m. В даному випадку:

$$m = \log_2 16 = 4.$$

2) будується таблиця станів лічильника (табл. 1.1).

Таблиця 1.1 – Таблиця функціонування двійкового підсумовуючого лічильника з паралельним перенесенням

C	$Q4^n$	$Q3^n$	$Q2^n$	$Q1^n$	$Q4^{n+1}$	$Q3^{n+1}$	$Q2^{n+1}$	$Q1^{n+1}$
1	0	0	0	0	0	0	0	1
1	0	0	0	1	0	0	1	0
1	0	0	1	0	0	0	1	1
1	0	0	1	1	0	1	0	0
1	0	1	0	0	0	1	0	1
1	0	1	0	1	0	1	1	0
1	0	1	1	0	0	1	1	1
1	0	1	1	1	1	0	0	0
1	1	0	0	0	1	0	0	1
1	1	0	0	1	1	0	1	0
1	1	0	1	0	1	0	1	1
1	1	0	1	1	1	1	0	0
1	1	1	0	0	1	1	0	1
1	1	1	0	1	1	1	1	0
1	1	1	1	0	1	1	1	1
1	1	1	1	1	0	0	0	0

3) складаються карти Карно для функцій переходів тригерів кожного розряду. Карта переходів будується по таблиці станів і відображає перехід тригера $Q_i^n \rightarrow Q_i^{n+1}$ у кожному такті, залежно від стану останніх тригерів в такті n (рис. 1.6).

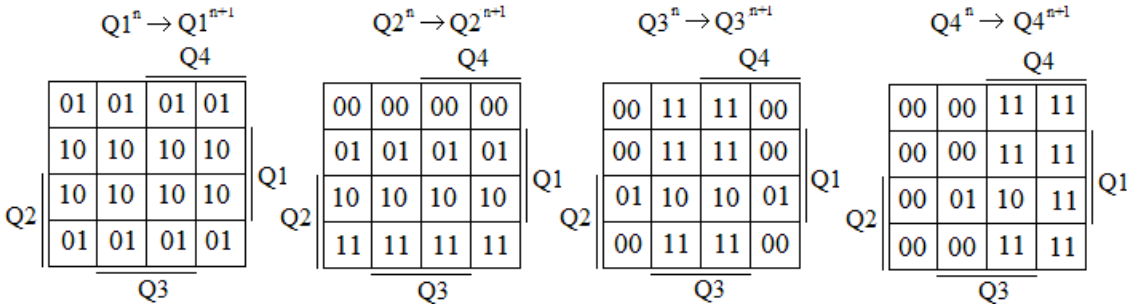


Рисунок 1.6 – Карти Карно для функцій переходів тригерів кожного розряду

Першому рядку таблиці 1.1 Q4 = Q3 = Q2 = Q1 = 0 відповідає ліва верхня клітинка карт переходів. Оскільки під час вступу першої одиниці в лічильник Q1 він повинен перейти з нульового стану в одиничний, а Q2, Q3 і Q4 повинні зберегти стан нуля, у вказану клітинку карти переходів для Q1 слід поставити «01», а в картах для Q2, Q3 і Q4 поставити «00» і так далі.

4) вибирається тип тригера, наприклад, JK – тригер, для побудови лічильника. Використовуючи словник переходів JK – тригера, для кожного входу тригера складаються карти Карно, в клітинках яких проставляються сигнали, необхідні для забезпечення переходів тригерів, вказаних в однойменних клітинках карт функцій переходів (рис. 1.7).

Наприклад, для переходів «01» JK – тригера, згідно його словнику переходів, необхідно подати сигнал J = 1, а сигнал на вході K може бути будь-яким «×», тому у верхню ліву клітинку карти Карно для J1 проставляють одиницю, а для K1 – «×» і так далі.

5) проводиться мінімізація логічних функцій входів в картах Карно з метою здобуття їх аналітичних виразів, що показують зв'язки між входами і виходами всіх тригерів, що складають лічильник. В процесі мінімізації виробляється довизначення функцій там, де це доцільно, одиницями в клітинках «×».

У результаті, отримано наступні функції входів тригерів лічильника:

$J1 = 1;\ K1 = 1;\quad J2 = Q1;\ K2 = Q1;\quad J3 = Q2 \cdot Q1;\ K3 = Q2 \cdot Q1;$

$J4 = Q3 \cdot Q2 \cdot Q1;\ K4 = Q3 \cdot Q2 \cdot Q1;$

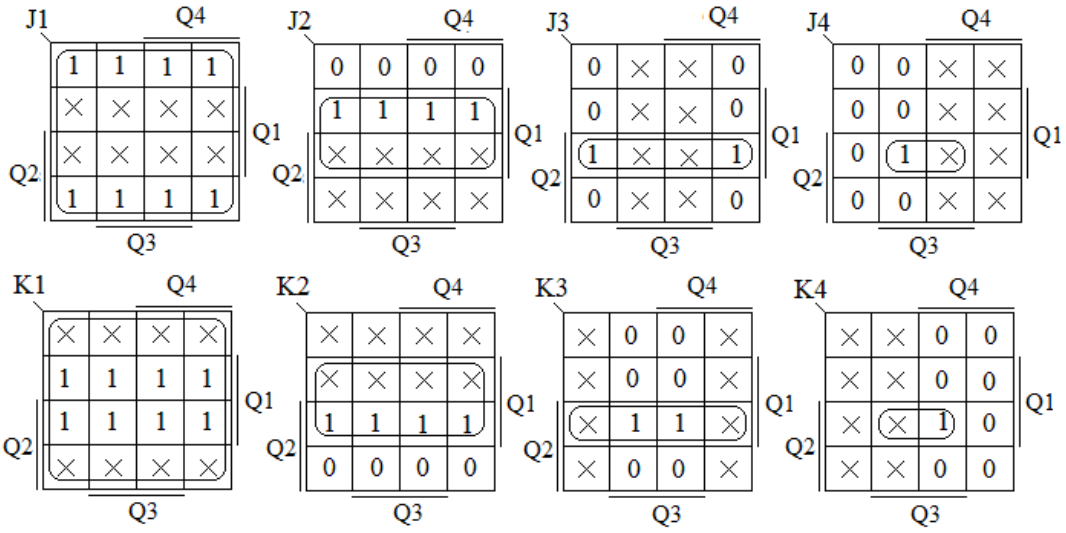


Рисунок 1.7 – Карти Карно для входів тригерів

6) будується електрична схема лічильника, відповідно до реалізації функцій входів (рис. 1.8).

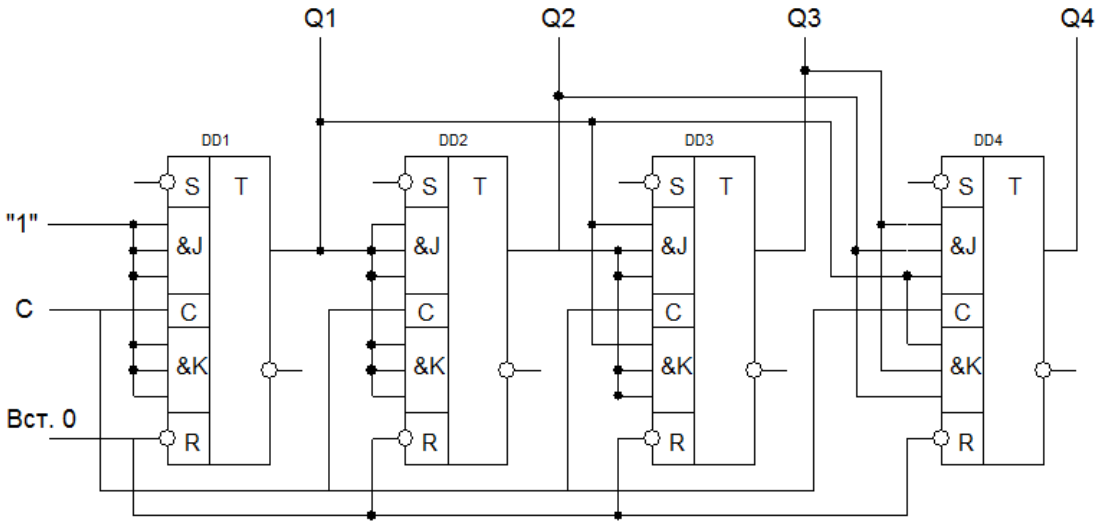


Рисунок 1.8 – Підсумовуючий двійковий лічильник з паралельним перенесенням

Метою роботи являється розрахунок схеми генератора випадкових чисел з діапазоном від 0 до 15 та фіксацією результату на індикаторах.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- розробити функціональну схему генератора;
- розробити електричну схему генератора;
- провести аналіз функціонування розробленого пристрою.

2 Розробка схеми генератора випадкових чисел

Випадкове число - число, яке представляє собою реалізацію випадкової величини.

Генератор випадкових чисел - це пристрій або алгоритм, який видає послідовність статистично незалежних і незміщених біт (тобто підкоряються закону розподілу).

Переконатися в тому, що послідовність чисел випадкова (або не випадкова) можна або за допомогою статистичних тестів, які виявлятимуть специфічні особливості випадкових послідовностей, або аналітико-обчислювальними методами.

2.1 Функціональна схема генератора випадкових чисел

Функціональну схему можна умовно поділити на чотири елементи, які послідовно виконують певні функції, а після вихід одного елемента перенаправляється на вхід наступного. Послідовність їх роботи виглядає так: генератор імпульсів → лічильник → дешифратор → семисегментний індикатор (рис. 2.1).

Генератор імпульсів виробляє послідовність цифрових імпульсів з заданою частотою і скважністю. Імпульси генератора являються тактовим сигналом для управління лічильником.

Лічильник імпульсів рахує кількість тактових послідовностей і формує на своєму виході числа у двійковому коді. Лічильник має модуль рахунку, після якого він обнуляється і рахунок починається знову.

Задача дешифратора - отримати на свої входи згенеровану попередніми двома елемента послідовність біт і поставити їй у відповідність набір сегментів на об'єкті типу «стандартний семисегментний індикатор».

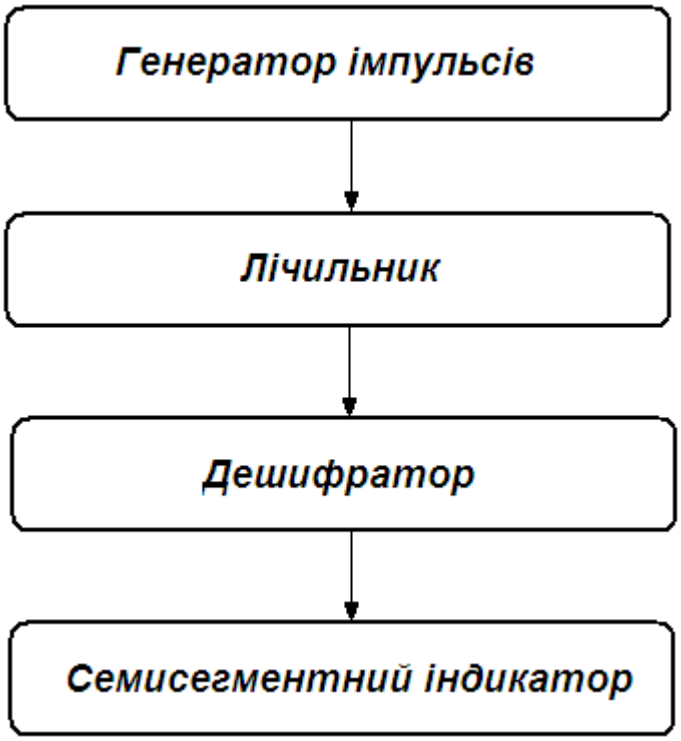


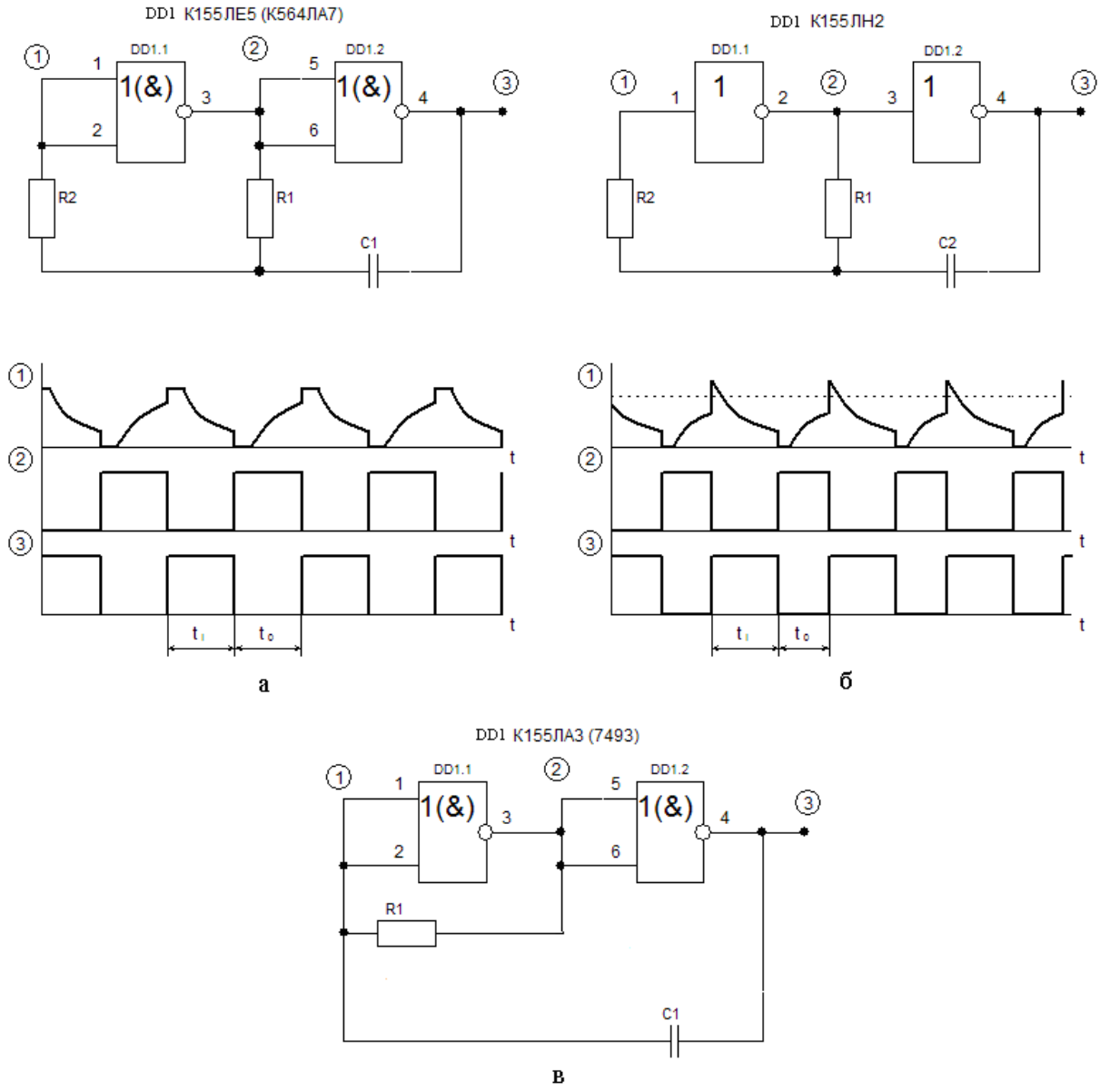
Рисунок 2.1 - Функціональна схема генератора випадкових чисел

2.2 Розробка схеми генератора цифрових імпульсів

Варіант генератора тактових імпульсів [7] на двох інверторах показаний на рисунку 2.2, а. Схема має два динамічних стана.

У першому з них, коли на виході DD1.1 стан логічної "1" (вихід DD1.2 логічний "0"), конденсатор C1 заряджається. В процесі заряду напруга на вході інвертора DD1.1 зростає, і досягши значення $U_{пор} = 0{,}5U_{жив}$ відбувається стрибкоподібний перехід в другий динамічний стан, в якому на виходах DD1.1 логічний "0", DD1.2 логічна "1". У цьому стані відбувається перезаряд ємкості (розряд) струмом зворотного напряму.

Досягши напруги на C1 $U_{пор}$ відбувається повернення схеми в перший динамічний стан. Діаграма напруги пояснює роботу генератора. Резистор R2 являється обмежувальним, і його опір не повинен бути менше 1 кОм. Аби він не впливав на розрахункову частоту, номінал резистора R1 обирається значно більше R2 (R2 < 0,01R1).



а – генератор на мікросхемі К155ЛЕ5;

б - генератор на мікросхемі К155ЛН2;

в – генератор на мікросхемі К155ЛЛА3

Рисунок 2.2 – Генератори імпульсів на двох інверторах

Обмежувальний резистор (R2) інколи встановлюють послідовно з конденсатором. При використанні неполярного конденсатора С1 тривалість імпульсів (t_i) і паузи (t_0) будуть майже однаковими: $t_i = t_0 = 0{,}7R1C1$. Повний період $T = 1{,}4R1C1$. Резистор R1 і конденсатор С1 можуть знаходитися в діапазоні 20 к0м ...10 МОм; 300 пф ...100 мкФ.

При використанні в схемі (рис. 2.2, б) двох інверторів мікросхеми К561ЛН2 (вони мають на вході лише один захисний діод) перезаряд конденсатора походитиме від рівня $U_{жив} + U_{пор}$. Внаслідок чого симетричність імпульсів порушується $t_i = 1{,}1R1C1$, $t_0 = 0{,}5R1C1$, період $T = 1{,}6R1C1$.

Оскільки поріг перемикання логічних елементів не відповідає точно половині напруги живлення, аби отримати симетричність імпульсів, в традиційну схему генератора можна додати ланцюг з R1 і C1 (рис. 2.2, в). Резистор R1 дозволяє підстроюванням отримати меандр ($t_i = t_0$) на виході генератора.

Генератор напруги прямокутної форми з високою стабільністю частоти може бути побудований за схемою, що представлена на рисунку 2.3 [8].

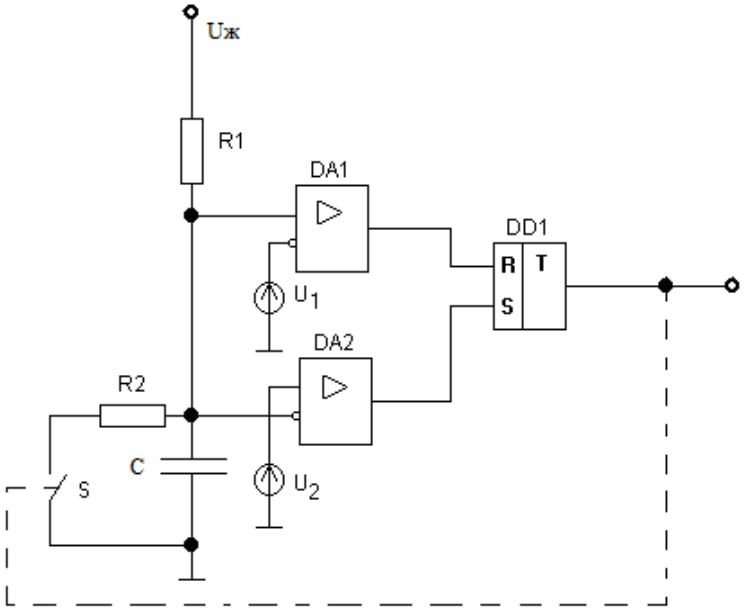


Рисунок 2.3 – Схема генератора імпульсів частотою 10 кГц

До складу її входять два диференціальні підсилювачі DA1, DA2, RS-тригер DD1 і керований їм електронний ключ S. Диференціальні підсилювачі DA1, DA2 мають великий коефіцієнт посилення по напрузі і виконують роль компараторів напруги. Компараторами називають пристрої, що використовуються для порівняння двох або декількох сигналів. Так, якщо, наприклад на неінвертуючому вході підсилювача напруга менша, ніж U_2, то на його виході буде низький рівень вихідного сигналу, відповідний коду 0 для тригера DD1. При підвищенні вхідної напруги і досягнення ним рівня, більшого U_2, на виході DA1 буде високий потенціал, відповідний коду 1. Зважаючи на ве-

ликий коефіцієнт посилення по напрузі в підсилювача зазвичай можна вважати, що зміна вихідного сигналу компараторів відбувається у момент рівності напруги на їх диференціальних входах [9].

Хай у вихідному стані конденсатор С розряджений ($U_C = 0$). Тоді на виході компаратора DA1 буде логічний 0, а на виході компаратора DA2 логічна 1. Тригер DD1 знаходиться в стані 1 і ключ S розімкнений.

Конденсатор С заряджає від джерела напруги живлення $U_ж$ через резистор R1. Напруга на ньому наростає по експоненціальному закону:

$$U_c(t) = U_ж\left(1 - e^{-\frac{t}{R1C}}\right) \qquad (2.1)$$

У момент часу t_1 напруга U_C стане рівною напрузі U1, $U_c(t) = U_1$. На виході компаратора DA2 з'явиться напруга логічного 0, яке не може змінити стан тригера DD1. Конденсатор С продовжує заряджати. У момент часу t_2 напруга U_C стане рівним U_2. При цьому на виході компаратора DA1 з'явиться логічна 1. При подачі логічної одиниці на вхід R тригер DD1 встановиться в нульовий стан і ключ S замкнеться. Паралельно конденсатору С підключиться резистор R2. Тим самим створюється коло розрядки конденсатора. Розрядка здійснюється різницею струмів резисторів R1 і R2. Проте якщо виконуються умови R1 >> R2 і U_2 близько до $U_ж$, то струмом резистора R1 можна знехтувати у зв'язку з його малим значенням. В цьому випадку зміни напруги U_C можна охарактеризувати рівнянням:

$$U_C(t) = U_2 e^{-\frac{t}{R2C}} \qquad (2.2)$$

Як тільки напруга U_C досягне напруги U_1, спрацює компаратор DA2 і переведе тригер DD1 в стан 1. Ключ S розімкнеться і процес зарядки і розрядки конденсатора повториться. Проміжки часу, в перебігу яких відбувається зарядка і розрядка конденсатора С, а вихідний сигнал тригера залишається незмінним, часто називають стадіями квазірівноваги (майже рівноваги). Тривалість їх знайдемо з рівнянь (2.1), (2.2). Підставивши в (2.1) замість $U_C(t)$ значення U_1 і U_2 знайдемо проміжки часу t_1 і t_2:

$$U_1 = U_ж\left(1 - e^{-\frac{t_1}{R1C}}\right) \quad (2.3)$$

$$U_2 = U_ж\left(1 - e^{-\frac{t_2}{R1C}}\right) \quad (2.4)$$

Перетворимо (2.3), (2.4) і прологарифмуємо:

$$e^{-\frac{t_1}{R1C}} = (U_ж - U_1) / U_ж; \quad e^{-\frac{t_2}{R1C}} = (U_ж - U_2) / U_ж; \quad (2.5)$$

$$t_1 = -R1C\ln(U_ж - U_1) / U_ж;$$

$$t_2 = -R1C\ln(U_ж - U_2) / U_ж. \quad (2.6)$$

Оскільки тривалість стадії квазірівноваги, визначувана зарядкою конденсатора С,

$$T_1 = t_2 - t_1, \quad (2.7)$$

то підставив (2.5), (2.6) в (2.7) отримаємо

$$T_1 = -R1C\ln\frac{U_ж - U_2}{U_ж - U_1} = R1C\ln\frac{U_ж - U_1}{U_ж - U_2}. \quad (2.8)$$

Тривалість проміжку часу t_2 - t_3 знайдемо з (2.2) підставивши замість $U_C(t)$ напругу U_1:

$$U_1 = U_2 e^{-\frac{t_3 - t_2}{R2C}} \quad (2.9)$$

Перетворивши (2.9) алогічно розглянутому, отримаємо

$$T_2 = R2C\ln\frac{U_2}{U_1}.$$

Період коливань

$$T_2 = T_1 + T_2,$$

а частота

$$f = 1/T$$

Тривалість фронтів прямокутної напруги визначається параметрами тригера DD1 і зазвичай оцінюється подвоєним часом затримки поширення в логічних елементах (ЛЕ), на основі яких виконаний RS-тригер [10].

Розглянутий принцип здобуття прямокутної напруги використовується в мікросхемі інтегрального таймера КР1006ВИ1 (рис. 2.4).

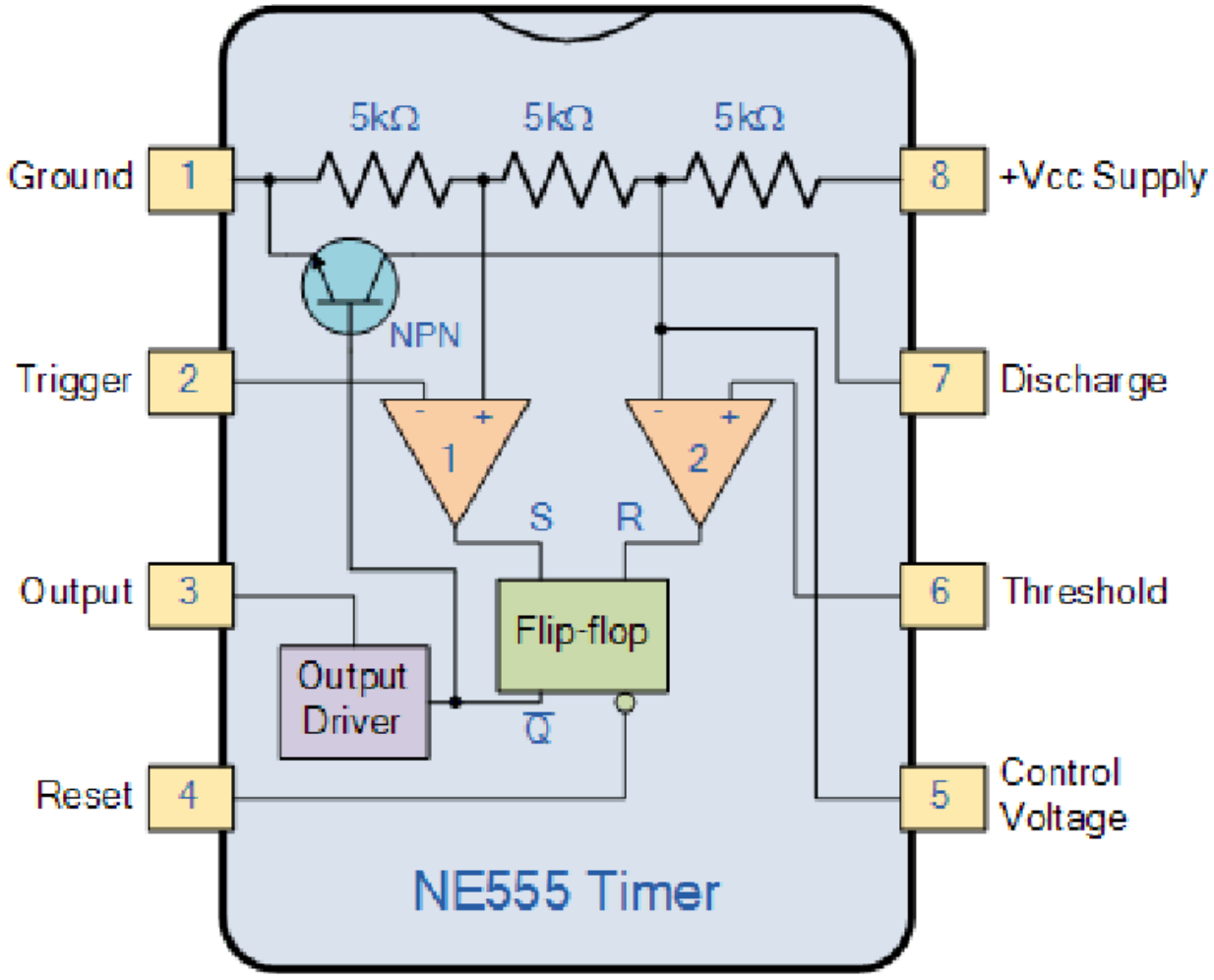


Рисунок 2.4 – Спрощена схема таймера КР1006ВИ1

Контакт 1. Заземлення, заземлюючий штифт підключає 555 таймер до негативної (0 В) подачі.

Контакт 2. Тригер, від'ємний вхід до компаратора №1. Від'ємний імпульс на цьому штифті "встановлює" внутрішній фліп-флоп, коли напруга опускається нижче 1/3 Vcc, що призводить до переходу виходу з "НИЗЬКОГО" у "ВИСОКИЙ" стан.

Контакт 3. Вихід. Вихідний штифт може керувати будь яким колом TTL і здатний подавати або пропускати до 200 мА струму при вихідній напрузі, рівній приблизно Vcc = 1,5 В, тому невеликі колонки, світлодіоди або двигуни можна підключити безпосередньо до виходу.

Контакт 4. Скидання. Цей штифт використовується для "скидання" внутрішнього фліп-флоп, керуючи станом виходу, контакт 3. Це активно-

низький вхід і зазвичай підключений до логічного рівня "1", в іншому випадку використовується для запобігання будь-якого небажаного скидання виводу.

Контакт 5. Управляюча напруга. Цей штифт регулює час 555, переосмислюючи рівень 2/3Vcc мережі дільника напруги. Застосовуючи напругу до цього контакту, ширину вихідного сигналу можна змінювати незалежно від мережі синхросигналу RC. Якщо не використовується, він підключається до землі за допомогою конденсатора 10nF для усунення будь-якого шуму.

Контакт 6. Поріг. Позитивний вхід до компаратора № 2. Цей штифт використовується для скидання фліп-флопа, коли напруга, яка подається на нього, перевищує 2/3Vcc, що призводить до переходу виходу з "ВИСОКОГО" в стан "НИЗЬКИЙ". Цей штифт підключається безпосередньо до схеми синхронізації RC.

Контакт 7. Розряд. розрядний штифт підключається безпосередньо до колектора внутрішнього транзистора n-p-n, який використовується для «розрядки» конденсатора синхронізації на землю, коли вихід на штифт 3 перемикається на «НИЗЬКИЙ».

Контакт 8. Блок живлення + Vcc. Це контакт блоку живлення таймера загального призначення TTL 555 - від постійної мережі від 4,5 до 15 В.

Таймер отримав свою назву 555 через те, що є три внутрішніх резистора 5 кОм, які він використовує для генерації опорних напруг двох компараторів. IC таймера 555 - це дуже дешевий, популярний і корисний пристрій точного хронування, який може діяти як простий таймер для генерації одиночних імпульсів або тривалих затримок, або як генератор релаксації, який генерує ланцюжок стабілізованих сигналів з різними робочими циклами від 50 до 100%.

Мікросхема таймера КР1006ВИ1 є надзвичайно надійним і стабільним пристроєм, який може працювати як дуже точний моностабільний, бістабільний або нестабільний мультивібратор для створення різних застосувань, таких як таймери одноразового спрацьовування або затримки, генерація імпу-

льсів, світлодіодні і лампові проблискові маячки, сигналізація і генерація тону, логічний годинник, частотне розділення, джерела живлення і перетворювачі тощо, фактично будь-яка схема, яка вимагає певної форми контролю часу, оскільки список нескінченний.

Мікросхема КР1006ВИ1 у своїй базовій формі являє собою біполярний 8-контактний міні-пристрій з подвійним входом у лінію (DIP), що складається з приблизно 25 транзисторів, 2 діодів і близько 16 резисторів, зкомпонованих для формування двох компараторів, тригера і вихідного каскаду високого струму.

У ньому ключ S виконаний на транзисторі VT1, на виході встановлений додатковий буферний елемент DD2, а роль джерел опорної напруги U_1, U_2 виконує дільник напруги на резисторах R1, R2, R3.

Генератор побудований на основі інтегрального таймера КР1006ВИ1, включеного як мультивібратор (рис. 2.5) [9].

При такому включенні конденсатор С заряджається через резистори R1, R2 до напруги:

$$U_2 = \frac{2}{3}U_ж,$$

а розряджається через резистор R1 до напруги:

$$U_1 = \frac{1}{3}U_ж.$$

Тривалість стадії зарядки T_1 і розрядки конденсатора С можна оцінити за допомогою рівнянь

$$T_1 \approx 0{,}693(R1 + R2)C;$$

$$T_2 \approx 0{,}693R2C.$$

Частота імпульсів, що генеруються

$$f = \frac{1}{T_1 + T_2} \approx \frac{1{,}443}{(R2 + R1)C}$$

У зв'язку із складністю підключення до мікросхеми двохполярного джерела живлення схема живиться від торби двох однополярних джерел живлення.

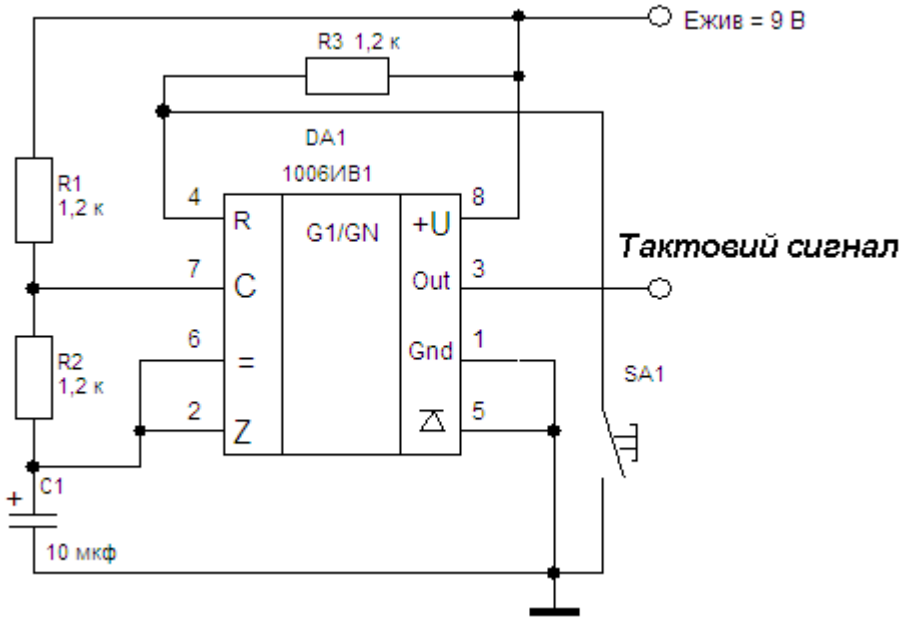


Рисунок 2.5 - Мультивібратор виконаний на інтегральному таймері КР1006ВИ1

2.3 Розробка схеми лічильника імпульсів

Лічильником називається послідовністний пристрій, призначений для підрахунку числа імпульсів, які поступають на його вхід, і фіксації цього числа у вигляді коду, що зберігається в тригерах. Лічильник відноситься до послідовних логічних пристроїв [11]. Число розрядів лічильника визначається найбільшим числом підраховуваних імпульсів. У лічильниках є один вхід і n виходів по числу розрядів. Для установки початкового стану лічильника (скидання в нуль) зазвичай передбачається вхід скидання. Лічильники будуються на Т – тригерах або на універсальних JK – тригерах.

JK – тригер – це схема з двома стійкими вихідними станами і двома входами J і K установки виходу Q тригера в стан 1 або 0. В JK – три-

гері наявність J = K = 1 наводить до переходу виходу Q тригера в протилежний стан (рис. 2.6).

J	K	Q^n	Q^{n+1}
0	0	0	0
0	1	0	0
1	0	0	1
1	1	0	1
0	0	1	1
0	1	1	0
1	0	1	1
1	1	1	0

У скороченому вигляді

J	K	Q^{n+1}
0	0	Q^n
0	1	0
1	0	1
1	1	$\overline{Q^n}$

Словник переходів

Перехід	J	K
0 → 0	0	×
0 → 1	1	×
1 → 0	×	1
1 → 1	×	0

Діаграма станів

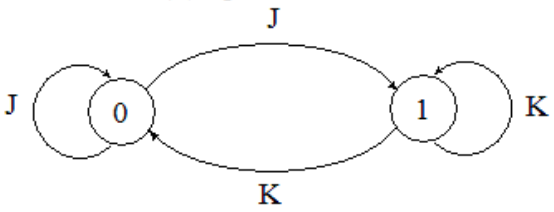
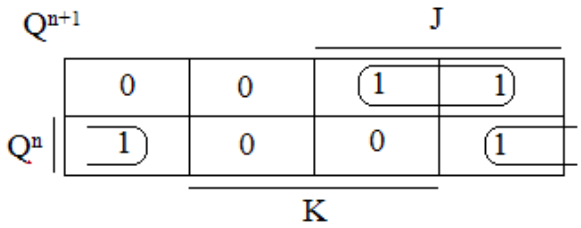


Рисунок 2.6 – Таблиця, словник і діаграма переходів JK-тригера

Відповідно до таблиці функціонування:



Рівняння функціонування:

$$Q^{n+1} = J\overline{Q^n} + \overline{K}Q^n$$

Розроблені і застосовуються в основному в інтегральному виконання JK – тригери, що тактуються фронтом тактових імпульсів, які не чутливі до тривалості тактових імпульсів. JK – тригери, що тактуються фронтом, будуються за схемою представленою на рисунку 2.7.

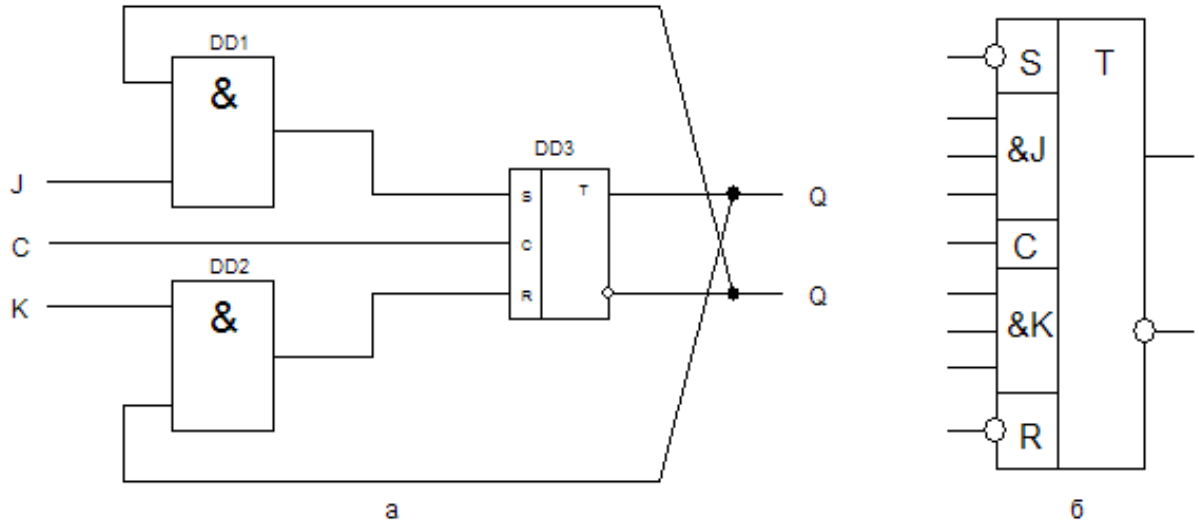


Рисунок 2.7 – JK – тригер: а) структурна схема, б) умовне графічне позначення JK – тригера

Тригер JK –типа називають універсальним тому, що на його основі за допомогою нескладних комутаційних перетворень можна отримати RS і T – тригери, а якщо між входами J і K включити інвертор, то вийде схема D – тригера (рис. 2.8).

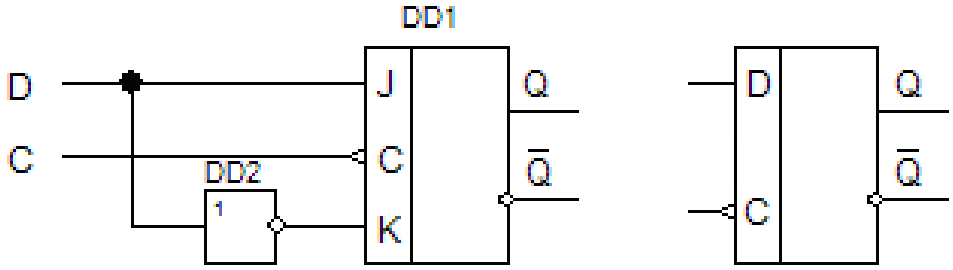


Рисунок 2.8 – D – тригер з JK – тригера

Для D-тригера скорочена таблиця істинності, словник переходів і діаграма станів приведені на рисунку 2.9.

Рівняння функціонування D-тригера:

$$Q^{n+1} = D.$$

Для функціонування логічного аналізатора необхідно розрахувати лічильник з коефіцієнтом рахунку $К_{рах} = 8$. Для його побудови необхідно $m = \log_2 8 = 3$ тригери, що відповідає трьом розрядам двійкового числа.

D	Q^n	Q^{n+1}
0	0	0
1	0	1
0	1	0
1	1	1

У скороченому вигляді

D	Q^{n+1}
0	0
1	1

Словник переходів

Переход	D
0 → 0	0
0 → 1	1
1 → 0	0
1 → 1	1

Діаграма станів

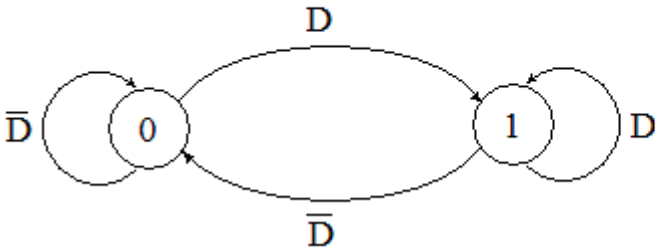


Рисунок 2.9 – Таблиця, словник і діаграма переходів D-тригера

Алгоритм станів такого лічильника представлений в таблиці 2.1. Вхідний сигнал x^n позначимо через 1, Q_3^n – старший розряд, Q_1^n – молодший розряд.

Таблиця 2.1 – Алгоритм станів лічильника

x^n	Q_3^n	Q_2^n	Q_1^n	Q_3^{n+1}	Q_2^{n+1}	Q_1^{n+1}
1	0	0	0	1	1	1
1	0	0	1	1	1	0
1	0	1	0	1	0	1
1	0	1	1	1	0	0
1	1	0	0	0	1	1
1	1	0	1	0	1	0
1	1	1	0	0	0	1
1	1	1	1	0	0	0

З аналізу таблиці видно:

- тригер молодшого розряду Q1 перемикається від кожного вхідного сигналу;

- другий розряд Q2 перемикається через два вхідні сигнали;

- третій розряд Q3 перемикається через чотири вхідні сигнали.

Таким чином, частота перемикання кожного наступного тригера зменшується удвічі. Отже, лічильник можна побудувати як коло послідовно включених рахункових тригерів.

Побудуємо такий лічильник на D-тригерах, що працюють в рахунковому режимі.

Складаємо карти функцій переходів тригерів лічильника.

$Q_1^n \to Q_1^{n+1}$

Q_1 \ Q_3				
	01	01	01	01
	10	10	10	10

Q_2

$Q_2^n \to Q_2^{n+1}$

Q_1 \ Q_3				
	01	10	10	01
	01	10	10	01

Q_2

$Q_3^n \to Q_3^{n+1}$

Q_1 \ Q_3				
	01	01	10	10
	01	01	10	10

Q_2

Використовуючи словник переходів D-тригера, для кожного входу тригера складемо карти Карно, в клітках яких проставимо сигнали, необхідні для забезпечення переходів тригерів, вказаних в однойменних клітках карт функцій переходів.

D1

Q_1 \ Q_3				
	1	1	1	1
	0	0	0	0

Q_2

D2

Q_1 \ Q_3				
	1	0	0	1
	1	0	0	1

Q_2

D3

Q_1 \ Q_3				
	1	1	0	0
	1	1	0	0

Q_2

Функції входів лічильника мають вигляд:

$$D1 = \overline{Q1};\ D2 = \overline{Q2};\ D3 = \overline{Q3}$$

Побудуємо лічильник на D-тригерах, що працюють в рахунковому режимі (рис. 2.21). Діаграма функціонування лічильника для багатоканального логічного аналізатора представлена на рисунку 2.11.

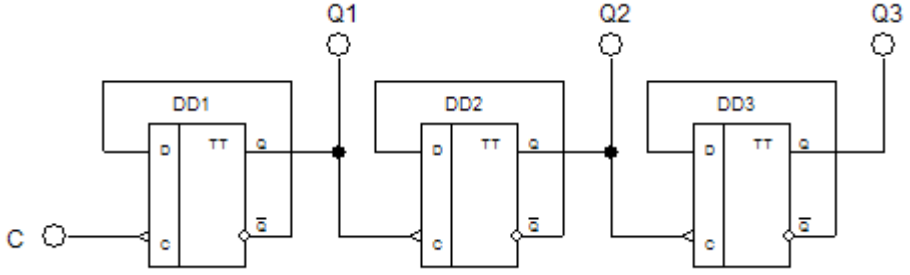


Рисунок 2.10 - Лічильник для багатоканального логічного аналізатора

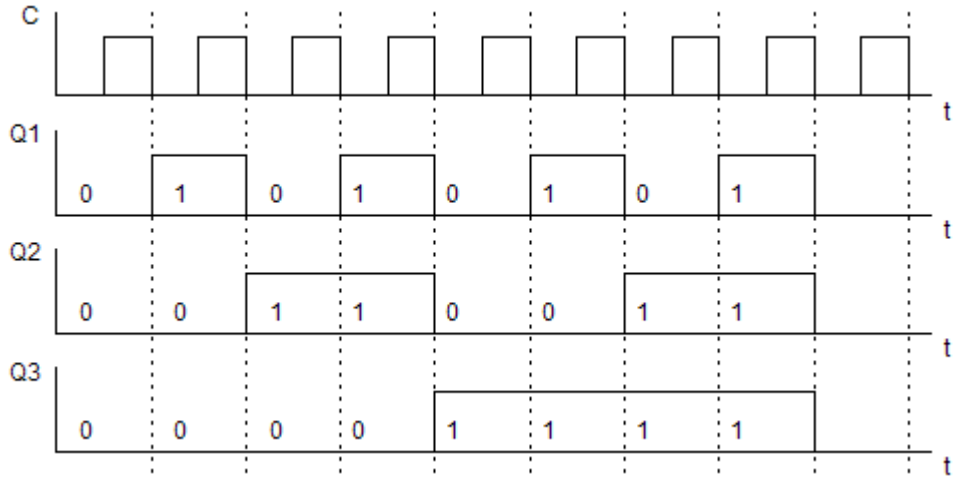


Рисунок 2.11 - Діаграма функціонування лічильника

Моделювання функціонування лічильника генератора випадкових чисел в програмному забезпеченні Electronics Workbench представлено на рисунку 2.12.

Аналіз схеми та діаграми функціонування підтверджує правильність розрахунків та вибір елементної бази.

За результатами моделювання можливо застосувати в схемі мікросхему К155ИЕ5 (рис. 2.13). Мікросхема містить рахунковий тригер (вхід С1), дільник на вісім (вхід С2), утворений сполученими послідовно тригерами. Тригери спрацьовують по зрізу вхідного імпульсу (переходу з 1 в 0). Якщо з'єднати послідовно всі 4 тригери, як показано на рисунку, вийде лічильник по модулю $2^n = 16$. Максимальне число, що зберігається в лічильнику, при повному заповненні його одиницями рівне: $N = 2^n - 1 = 15 = (1111)_2$. Такий лічильник працює з коефіцієнтом рахунку $К_{рах}$, кратним цілій мірі числа 2 і в нім здійснюється циклічний перебір $К_{рах} = 2^n$ стійких станів. Лічильник має виводи примусової установки в 0. На вхід С лічильника поступають сигнали від генератора тактових імпульсів.

Можливо розглянути питання заміни мікросхем ТТЛ логіки на КМДП, що приведе до низької споживаної потужності схеми. Але при цьому зменшиться швидкодія пристрою.

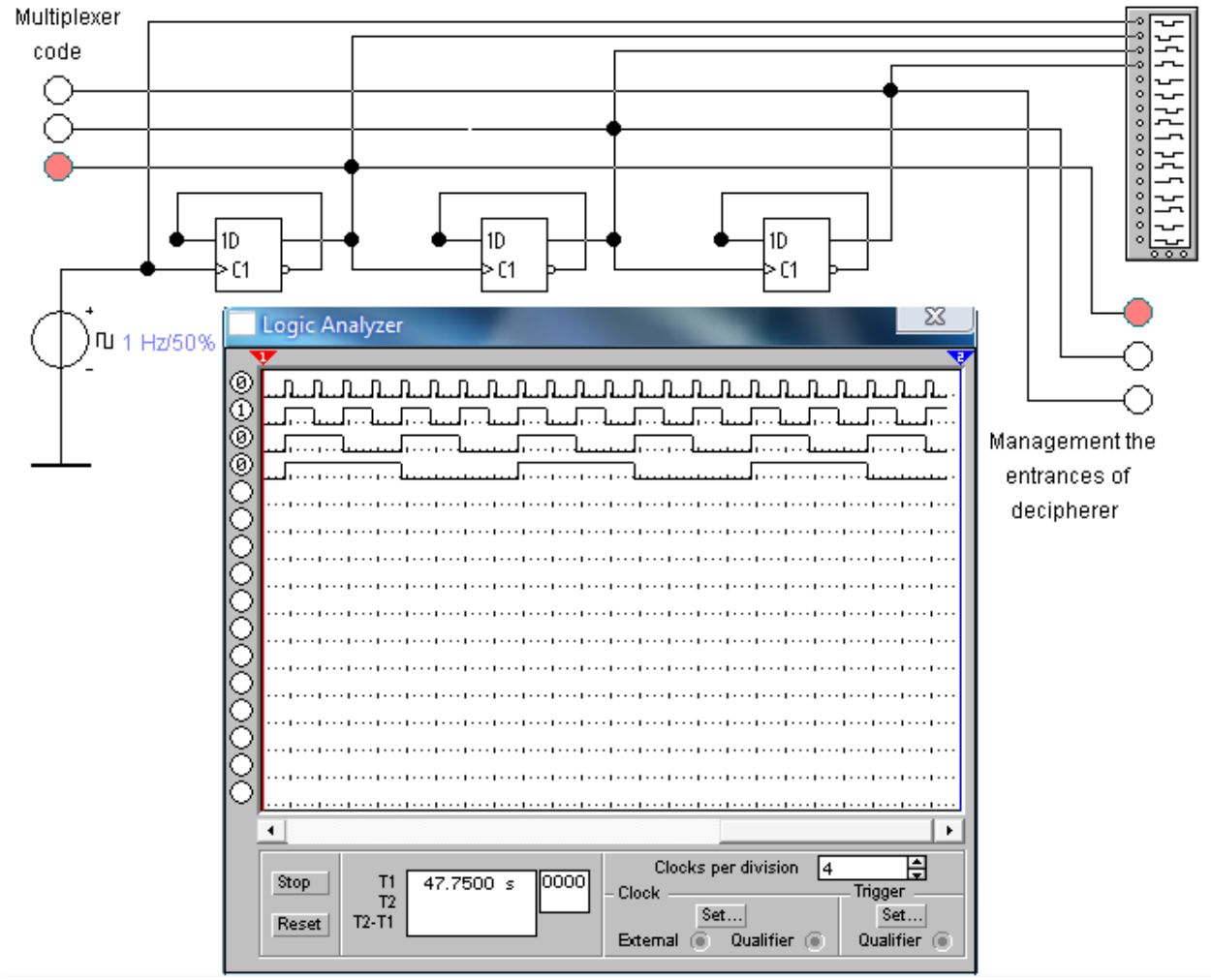


Рисунок 2.12 - Моделювання функціонування лічильника генератора випадкових чисел

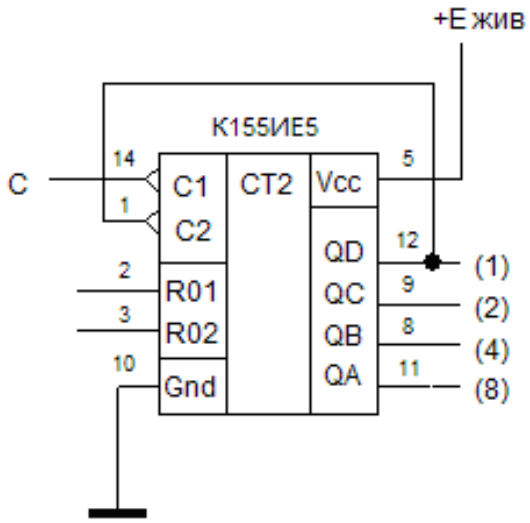


Рисунок 2.13 – Мікросхема К155ИЕ5

2.4 Розробка схеми пристрою відображення інформації

Результати випадкового обчислення необхідно представити на двох семисегментних індикаторах. Проведемо аналітичне моделювання пристрою перетворення двійкового коду чисел в код семисегментних індикаторів [11].

Максимальне число ABCD, яке поступає на схему пристрою відображення інформації у десятковому еквіваленті 15, у двійковому $(1111)_2$.

Таблиця функціонування пристрою відображення інформації (табл. 2.2) описує алгоритм функціонування перетворювача чотірьохрозрядного двійкового коду 8-4-2-1 в код семисегментних індикаторів. (рис. 2.14).

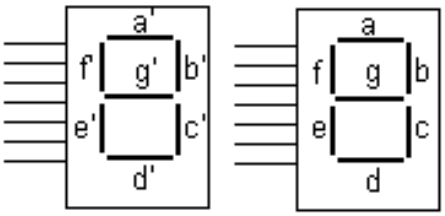


Рисунок 2.14 – Семисегментні індикатори для представлення отриманої інформації

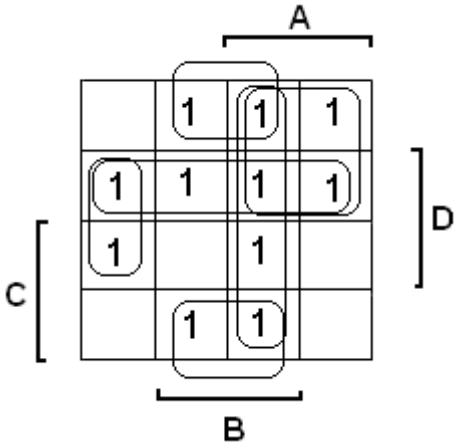
Таблиця 2.2 - Таблиця функціонування перетворювача двійкового коду чисел в код семисегментних індикаторів

№	A	B	C	D	a'	b'	c'	d'	e'	f'	g'	a	b	c	d	e	f	g
0	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0
1	0	0	0	1	1	1	1	1	1	1	0	0	1	1	0	0	0	0
2	0	0	1	0	1	1	1	1	1	1	0	1	1	0	1	1	0	1
3	0	0	1	1	1	1	1	1	1	1	0	1	1	1	1	0	0	1
4	0	1	0	0	1	1	1	1	1	1	0	0	1	1	0	0	1	1
5	0	1	0	1	1	1	1	1	1	1	0	1	0	1	1	0	1	1
6	0	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	1	1
7	0	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	0
8	1	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1
9	1	0	0	1	1	1	1	1	1	1	0	1	1	1	1	0	1	1
10	1	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1	1	0
11	1	0	1	1	0	1	1	0	0	0	0	0	1	1	0	0	0	0
12	1	1	0	0	0	1	1	0	0	0	0	1	1	0	1	1	0	1
13	1	1	0	1	0	1	1	0	0	0	0	1	1	1	1	0	0	1
14	1	1	1	0	0	1	1	0	0	0	0	0	1	1	0	0	1	1
15	1	1	1	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1

З таблиці виводимо рівняння функціонування пристрою перетворення двійкового коду чисел в код семисегментних індикаторів.

$$g = \overline{A}\overline{B}C\overline{D} + \overline{A}\overline{B}CD + \overline{A}B\overline{C}\overline{D} + \overline{A}B\overline{C}D + \overline{A}BC\overline{D} +$$
$$+ A\overline{B}\overline{C}\overline{D} + A\overline{B}\overline{C}D + AB\overline{C}\overline{D} + AB\overline{C}D + ABC\overline{D} +$$
$$+ ABCD$$

Карта Карно:

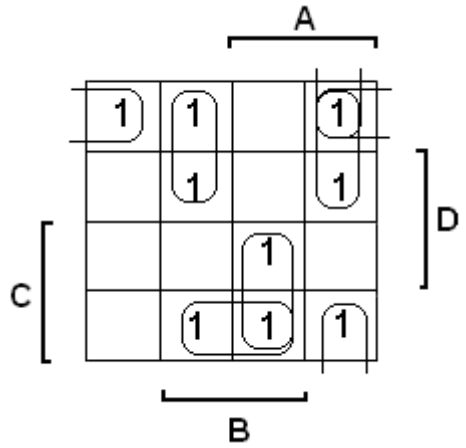


Спрощене рівняння:

$$g = \overline{C}D + A\overline{C} + AB + B\overline{D} + \overline{A}\overline{B}D$$

$$f = \overline{A}\overline{B}\overline{C}\overline{D} + \overline{A}\overline{B}\overline{C}\overline{D} + \overline{A}\overline{B}C\overline{D} + \overline{A}BC\overline{D} + A\overline{B}\overline{C}\overline{D} +$$
$$+ A\overline{B}\overline{C}D + A\overline{B}C\overline{D} + ABC\overline{D} + ABCD$$

Карта Карно:

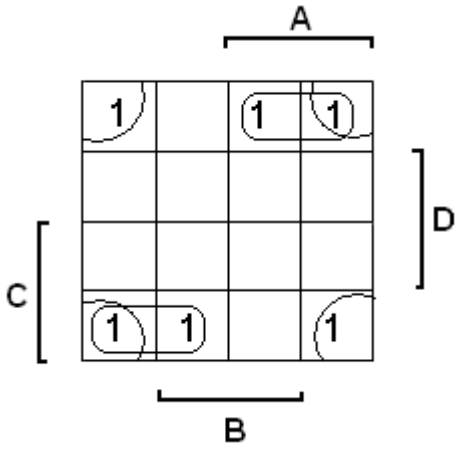


Спрощене рівняння:

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

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

Карта Карно:

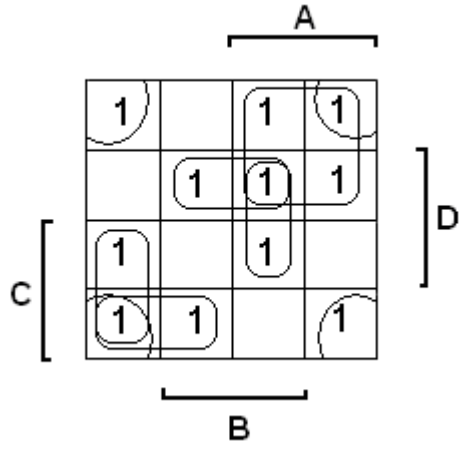


Спрощене рівняння:

$$e = \overline{B}\overline{D} + A\overline{C}\overline{D} + \overline{A}C\overline{D}$$

$$d = \overline{A}\overline{B}C\overline{D} + \overline{A}\overline{B}CD + \overline{A}B\overline{C}\overline{D} + \overline{A}B\overline{C}D + \overline{A}BC\overline{D} +$$
$$+ A\overline{B}\overline{C}\overline{D} + A\overline{B}\overline{C}D + A\overline{B}C\overline{D} + AB\overline{C}\overline{D} + AB\overline{C}D +$$
$$+ ABCD$$

Карта Карно:

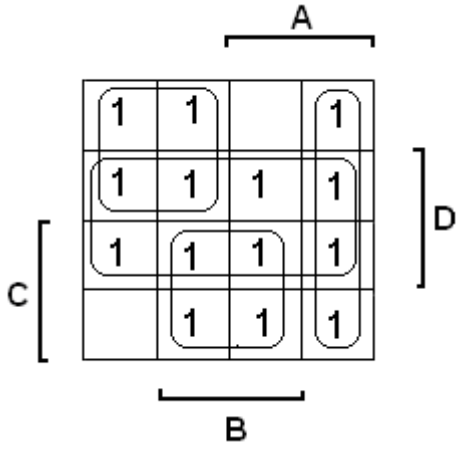


Спрощене рівняння:

$$d = A\overline{C} + \overline{B}\overline{D} + B\overline{C}D + ABD + \overline{A}\overline{B}C + \overline{A}C\overline{D}$$

$$c = \overline{A}\overline{B}C\overline{D} + \overline{A}\overline{B}CD + \overline{A}B\overline{C}\overline{D} + \overline{A}B\overline{C}D + \overline{A}BC\overline{D} +$$
$$+ \overline{A}BCD + A\overline{B}\overline{C}\overline{D} + A\overline{B}\overline{C}D +$$
$$+ A\overline{B}C\overline{D} + A\overline{B}CD + AB\overline{C}D + ABC\overline{D} + ABCD$$

Карта Карно:

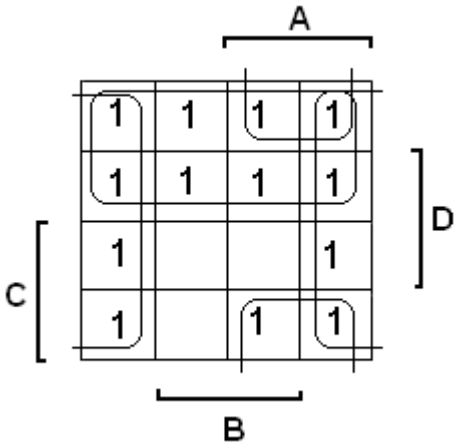


Спрощене рівняння:

$$c = D + \overline{A}\,\overline{C} + BC + A\overline{B}$$

$$b = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,\overline{B}\,\overline{C}D + \overline{A}\,\overline{B}C\,\overline{D} + \overline{A}\,\overline{B}CD + \overline{A}B\,\overline{C}\,\overline{D} +$$
$$+ \overline{A}BCD + A\,\overline{B}\,\overline{C}\,\overline{D} + A\,\overline{B}\,\overline{C}D + A\,\overline{B}C\,\overline{D} + A\,\overline{B}CD$$
$$+ AB\,\overline{C}\,\overline{D} + AB\,\overline{C}D + ABC\,\overline{D}$$

Карта Карно

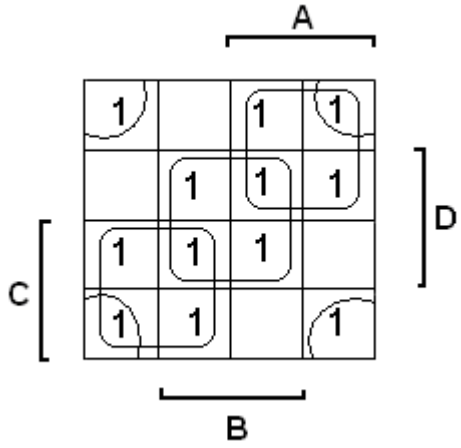


Спрощене рівняння:

$$b = \overline{C} + \overline{B} + A\overline{D}$$

$$a = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,\overline{B}\,\overline{C}D + \overline{A}\,\overline{B}C\,\overline{D} + \overline{A}\,\overline{B}CD + \overline{A}B\,\overline{C}\,\overline{D} + \overline{A}BCD$$
$$+ A\,\overline{B}\,\overline{C}\,\overline{D} + A\,\overline{B}\,\overline{C}D + A\,\overline{B}C\,\overline{D} + AB\,\overline{C}\,\overline{D} + AB\,\overline{C}D + ABCD$$

Карта Карно:



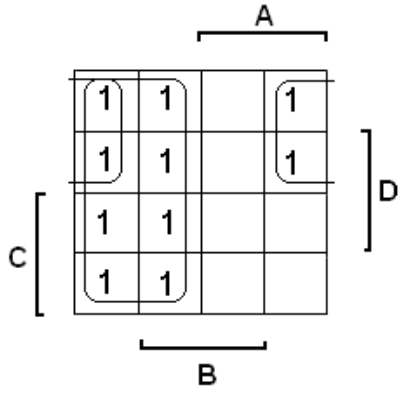
Спрощене рівняння:

$$a = A\overline{C} + BD + \overline{A}C + \overline{B}\overline{D}$$

$$g' = 0$$

$$f' = \overline{A}\overline{B}C\overline{D} + \overline{A}\overline{B}CD + \overline{A}B\overline{C}\overline{D} + \overline{A}BCD + \overline{A}BC\overline{D} +$$
$$+ \overline{A}B\overline{C}D + \overline{A}BC\overline{D} + \overline{A}BCD + A\overline{B}\overline{C}\overline{D} + A\overline{B}\overline{C}D$$

Карта Карно:



Спрощене рівняння:

$$f' = \overline{A} + \overline{B}\overline{C}$$

$$e' = \overline{A} + \overline{B}\overline{C}$$

$$d' = \overline{A} + \overline{B}\overline{C}$$

$$c' = 1$$

$$b' = 1$$

$$a' = \overline{A} + \overline{B}\overline{C}$$

Функціональна схема перетворювача двійкового коду чисел в код семи сегментного індикатора представлена на рисунку 2.15.

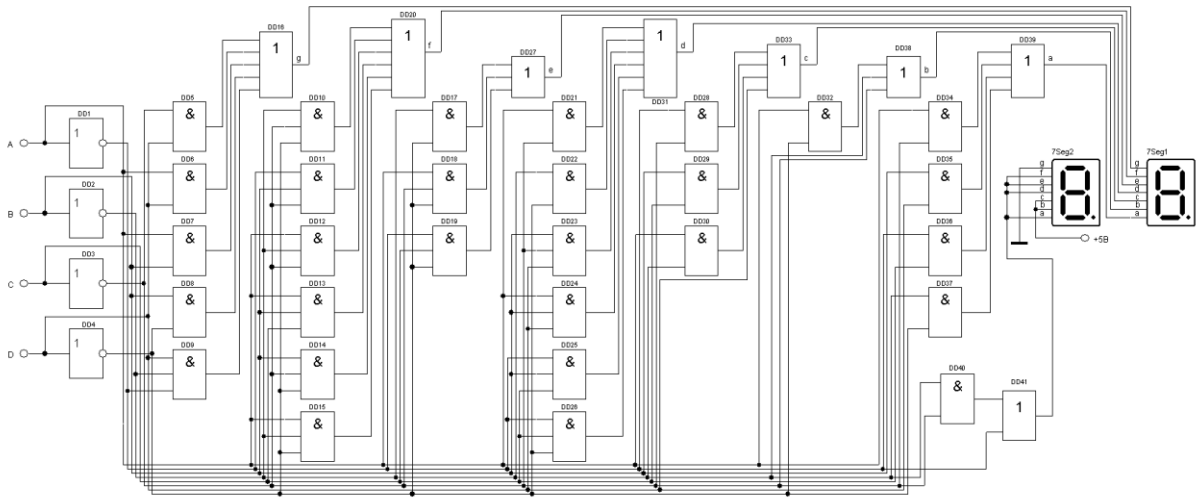


Рисунок 2.15 - Функціональна схема перетворювача двійкового коду чисел в код семи сегментних індикаторів для схеми генератора випадкових чисел

Мікросхема перетворювача двійкового коду чисел в код семи сегментного індикатора представлено на рисунку 2.16.

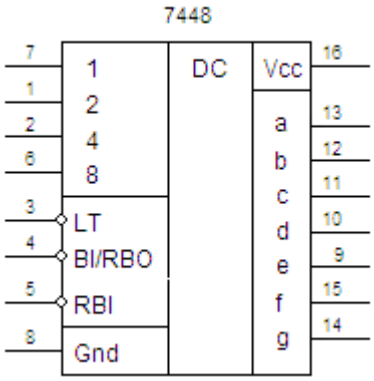


Рисунок 2.16 – Мікросхема перетворювача двійкового коду чисел в код семи сегментного індикатора

Схема відображення інформації про випадкове число складається з схеми управління індикатором розрядом одиниць і схеми управління індикатором розрядом десятків (рис. 2.17).

Виконаємо деякі перетворення:

$$a', f', e', d' = \overline{A} + \overline{B}\overline{C} = \overline{\overline{A} + \overline{B}\overline{C}} = \overline{\overline{A} \cdot \overline{\overline{B}\overline{C}}} = \overline{A \cdot \overline{B}\overline{C}}$$

Таким чином схему управління індикатором розрядом десятків можна реалізувати на одній мікросхемі 4І-НІ К155ЛА3.

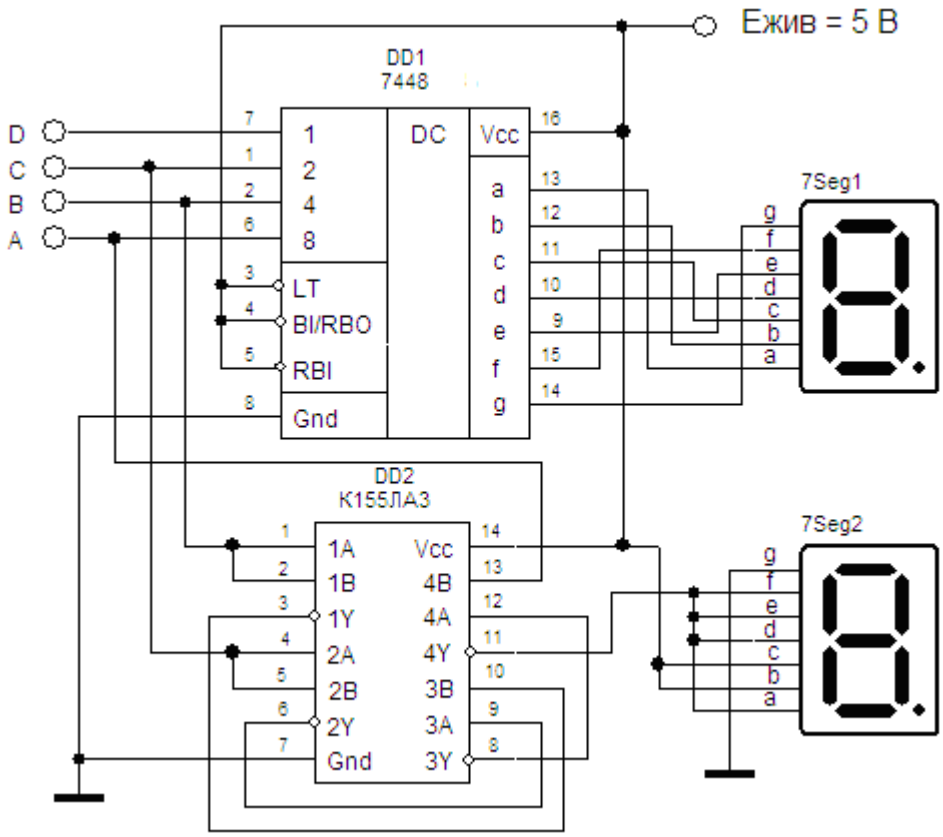


Рисунок 2.17 - Схема відображення інформації про випадкове число

Загальна розрахована схема генератора випадкових чисел від 0 до15 представлена на рисунку 2.18. Випадкова цифра виводиться як двійкове число на виходах QA, QB, QC, QD мікросхеми DD1. З мікросхеми DA1 на лічильник поступають тактові імпульси з заданою параметрами схеми частотою. Кнопкою SA1 потік імпульсі переривається і лічильник фіксує підраховану до цього моменту кількість імпульсів як випадкове число у двійковому коді. Дешифратор перетворює випадкове число у код семисегментних індикаторів. Таким чином з натисненням кнопки SA1 схемою фіксується випадкове число від 0 до 15 у десятковому представленні.

Аналіз функціонування схеми показує правильність розрахунків та вибору елементної бази генератора випадкових чисел.

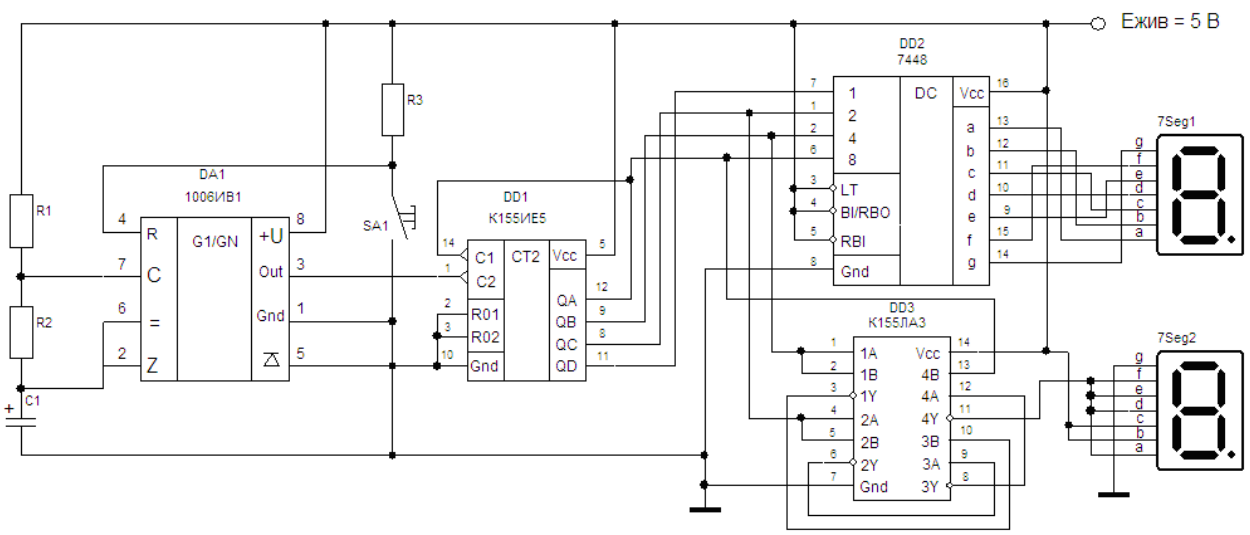


Рисунок 2.18 - Схема генератора випадкових чисел

3 Охорона праці та техногенна безпека при розробці генератора випадкових чисел

3.1 Характеристика потенційних небезпечних та шкідливих виробничих факторів

Приміщення, в якому знаходиться робоче місце інженера елекронщика, має такі характеристики: довжина приміщення 6.5 м; ширина приміщення 3.7 м; висота приміщення 3.5 м; число вікон 2; число робочих місць 3; освітлення природне (через бічні вікна) і загальне штучне. Загальна площа дорівнює 24.1 м^2. Тобто на кожне робоче місце припадає по 8 м^2, що відповідає нормам (не менше 6 м^2).

На рисунку 3.1 наведено план розташування робочих місць інженерів електронщиків. На робочому місці інженер електронщик піддається впливу наступних несприятливих факторів [12]:

- недостатнє освітлення;

- шум від працюючих машин (комп'ютерів, робочих стендів) На даному робочому місці шум непостійний. Джерелом шуму є робочі стенди. Шум діє на робітника протягом 5 годин;

- електромагнітне випромінювання. На робочому місці допустимі рівні електромагнітних випромінювань за електричної та магнітної складових в діапазоні 5…2000 Гц;

- виділення надлишків теплоти. Тепловий поріг починається з J = 10 мВт/см^2;

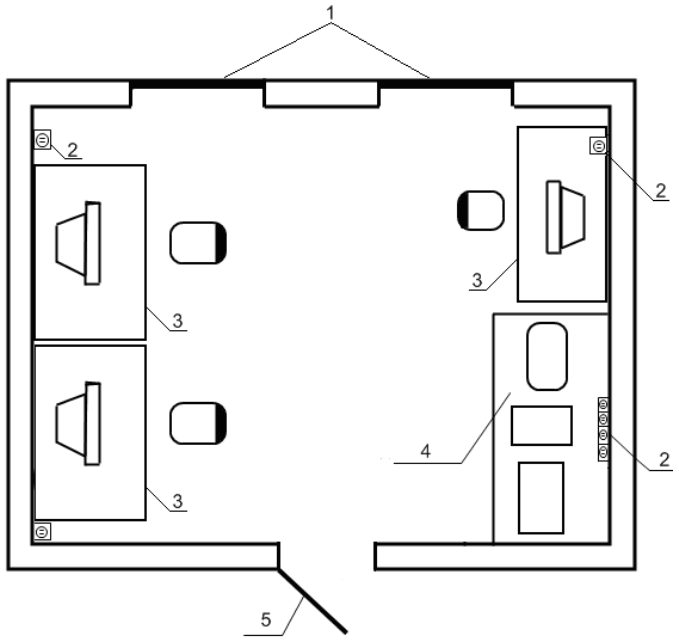
- підвищена запиленість.

Розвитку стомлюваності на робочому місці сприяють такі чинники [13]:

- неправильна ергономічна організація робочого місця, нераціональні зони розміщення обладнання по висоті від підлоги, по фронту від осі симет-

рії. Робоча поза сидячи викликає мінімальне стомлення, тому велике значення надається характеристикам робочого крісла. Велике значення також надається правильній робочій позі користувача. Істотне значення для продуктивної і якісної роботи на комп'ютері мають розміри знаків, контраст і співвідношення яскравості символів і фону екрану. Під час користування комп'ютером медики радять встановлювати монітор на відстані 50…60 см від очей.

- характер протікання праці. Трудовий процес організований таким чином, що інженер електронщик змушений з перших хвилин робочого дня вирішувати найбільш складні і трудомісткі задачі, у той час як у перші хвилини роботи функціональна рухливість нервових клітин мозку низька. Тому дотримання правильного режиму праці і відпочинку при роботі грає дуже важливу роль.



1 – вікна;

2 – розетка;

3 – робоче місце;

4 – місце для стендів;

5 – двері

Рисунок 3.1 – План розташування робочих місць інженерів-електронщиків

Важливе значення має чергування праці та відпочинку, зміна одних форм роботи іншими.

Джерела небезпечних та шкідливих чинників на інженера електронщика [13]:

- рівень шуму в приміщенні протягом робочого дня непостійний (табл. 3.1). При цьому протягом однієї години діє шум з рівнем звуку 83 дБА, протягом наступних двох годинників ¾ з рівнем звуку 86 дБА, останню годину ¾ 81 дБА при тому що норматив повинен бути не більше 70 дБА. Основними джерелами шуму є: комп'ютери, робочі стенди. Отже, робоче місце по показнику рівня шуму відноситься до класу умов праці 3.2 – шкідливий.

- основним джерелом електромагнітного випромінювання приміщення є персональні комп'ютери з системними блоками Intel Pentium і моніторами SVGA Samsung, SyncMaster 450b.

Таблиця 3.1 Оцінка чинників виробничого і трудового процесу робочого місця інженера електронщика

№	Чинники виробничого середовища і трудового процесу	Нормативне значення	Фактичне значення	III клас: шкідливі і небезпечні умови			Тривалість дії чинників за зміну %
				I ступінь	II ступінь	III ступінь	
1	Пил, переважно фіброгенної дії. мг/м^3	4	3.9				50
2	Шум, дБА	70	83		13		75
3	Мікроклімат в приміщенні:						
	- температура повітря С°	22-24	18-24				100
	- швидкість руху повітря, м/с	0,1-0,2	0,15-0,2				100
	- відносна вологість повітря %	40-60	45-60				100

3.2 Заходи зі зменшення впливу небезпечних та шкідливих виробничих

факторів

До засобів захисту відносяться: вентиляція, штучне освітлення, звукоізоляція. Існують нормативи, що визначають комфортні умови і гранично допустимі норми запиленості, температури повітря, шуму, освітленості. У системі заходів, що забезпечують сприятливі умови праці, велике місце відводиться естетичним чинникам: оформлення виробничого інтер'єру, обладнання, застосування музики та інші, які мають певний вплив на організм людини. Важливу роль відіграє забарвлення приміщень, яка повинна бути світлою. З метою запобігання або зменшення впливу на працюючих шкідливих і небезпечних виробничих чинників застосовують засоби колективного та індивідуального захисту.

Засоби колективного захисту призначені для [14]:

1) нормалізації повітряного середовища виробничих приміщень і робочих місць (вентиляція, кондиціонування, опалення, автоматичний контроль і сигналізація);

2) нормалізації освітлення виробничих приміщень і робочих місць (джерела світла, освітлювальні прилади, світлозахисне обладнання, світлофільтри). При недоліку природного освітлення необхідно буде користуватися штучним. Як джерела світла при штучному освітленні рекомендується застосовувати переважно люмінесцентні лампи типу ЛБ;

захисту від іонізуючих, інфрачервоних, ультрафіолетових, електромагнітних, лазерних, магнітних та електричних полів (огородження, герметизація, знаки безпеки, автоматичний контроль і сигналізація, дистанційне керування тощо);

3) захисту від шуму, вібрації (огородження, звукоізоляція, віброізоляція). Для зменшення рівня шуму, який перевищує норму в лабораторному приміщенні можна застосовувати оздоблювальні матеріали з шумопоглинаючим ефектом;

4) захисту від ураження електричним струмом (різні види огородження, захисне заземлення, автоматичне відключення, дистанційне керування).

5) забезпечення недоступності струмоведучих частин досягається ізолюванням струмовідних кабелів і проводів;

6) захисту від дії механічних факторів (огородження, автоматичний контроль і сигналізація, знаки безпеки);

7) захисту від хімічних факторів (огородження, герметизація, вентиляція та очищення повітря, дистанційне керування, знаки безпеки);

8) захисту від високих і низьких температур навколишнього середовища (огородження, автоматичний контроль і сигналізація, термоізоляція, дистанційне керування).

3.3 Виробнича санітарія

Оскільки у приміщенні присутнє лабораторне устаткування, комп’ютери, шафи та робоча документація, то спостерігається деяка запиленість. За нормою запиленість в приміщенні не повинна перевищувати 4 мг/м³, а в даному приміщенні вона складає 3,9 мг/м³.

Для запобігання дещо підвищеної запиленості рекомендується встановлювати витяжні пристрої, а також проводити вологе прибирання лабораторного приміщення, а перед початком і після кожної академічної години навчальних занять, до і після кожного заняття провітрювати приміщення, що забезпечить поліпшення якісного складу повітря.

Раціональне колірне оформлення приміщення направлено на поліпшення санітарно-гігієнічних умов праці, підвищення її продуктивності та безпеки. Забарвлення приміщень впливає на нервову систему людини, його настрій і в кінцевому рахунку на продуктивність праці. Основні виробничі приміщення доцільно офарблювати відповідно до кольору технічних засобів. Освітлення приміщення і устаткування має бути м'яким, без блиску.

Зниження шуму, створюваного на робочих місцях лабораторного приміщення внутрішніми джерелами, а також шуму проникаючого зовні, є дуже

важливим завданням. Зниження шуму в джерелі випромінювання можна забезпечити застосуванням пружних прокладок між підставою приладу і опорною поверхнею. Як прокладки використовуються гума, повсть, пробка, різної конструкції амортизатори. Під настільні шумливі апарати можна підкладати м'які килимки з синтетичних матеріалів, а під ніжки столів, на яких вони встановлені, - прокладки з м'якої гуми, повсті, завтовшки 6 - 8 мм. Кріплення прокладок можливе шляхом приклеювання їх до опорних частин [13].

Таким чином, для зниження шуму, створюваного на робочих місцях внутрішніми джерелами, а також шуму, що проникає з зовні необхідно:

послабити шум самих джерел (застосування екранів, звукоізолюючих кожухів);

- знизити ефект сумарної дії відбитих звукових хвиль (звукопоглинаючі поверхні конструкцій);

- застосовувати раціональне розташування обладнання;

- використовувати архітектурно-планувальні і технологічні рішення ізоляцій джерел шуму.

Температура в приміщеннях є одним з провідних чинників, що визначають метеорологічні умови виробничого середовища. Високі температури надають негативну дію на здоров'я людини. Робота в умовах високої температури супроводжується інтенсивним потовиділенням, що приводить до обезводнення організму, втрати мінеральних солей і водорозчинних вітамінів, викликає серйозні і стійкі зміни в діяльності серцево-судинної системи, збільшує частоту дихання [13].

При низькій температурі висока відносна вологість збільшує тепловтрати організму в результаті інтенсивного поглинання водяними парами енергії випромінювання людини. Це веде до переохолодження організму – гіпотермії. Низька вологість викликає пересихання слизистих оболонок дихальних шляхів.

В приміщенні нормована температура повітря повинна складати в теплий період 22-24ºС (в холодний період 21-23ºС), відносна вологість 40-60 %, швидкість руху повітря 0,1-0,2 м/с.

Фактичні параметри: температура в теплий період – 18-24 ºС, відносна вологість 45-60%, швидкість руху повітря 0,15-0,2 м/с.

У приміщеннях, обладнаних ПЕВМ, повинна проводиться щоденне, вологе прибирання і систематичне провітрювання після кожної години роботи на ПЕВМ. Рівні позитивних і негативних аероіонів в повітрі приміщень, де розташовані ПЕВМ, повинні відповідати санітарно-епідеміологічним нормативам, що діють.

Недостатнє освітлення робочого місця утрудняє тривалу роботу, викликає підвищене стомлення і сприяє розвитку короткозорості. Дуже низькі рівні освітленості викликають апатію, сонливість, а в деяких випадках сприяють розвитку відчуття тривоги. Таким чином буде доцільно зробити розрахунок фактичної освітленості приміщення [14].

3.4 Електробезпека

Електричні установки, до яких відноситься практично все обладнання ЕОМ, представляють для людини велику потенційну небезпеку, тому що в процесі експлуатації або проведенні профілактичних робіт людина може торкнутися частин, що знаходяться під напругою. Специфічна небезпека електроустановок: струмоведучі провідники, корпуси стійок ЕОМ і іншого устаткування, що опинилося під напругою в результаті пошкодження (пробою) ізоляції, не подають будь-яких сигналів, які попереджають людину про небезпеку. Реакція людини на електричний струм виникає лише при протіканні останнього через тіло людини. Виключно важливе значення для запобігання електротравматизма має правильна організація обслуговування діючих електроустановок, проведення ремонтних, монтажних і профілактичних робіт.

При цьому під правильною організацією розуміється строге виконання ряду організаційних і технічних заходів і засобів, встановлених діючими "Правилами технічної експлуатації електроустановок споживачів і правила техніки безпеки при експлуатації електроустановок споживачів" (ПТЕ і ПТБ споживачів) і "Правила установки електроустановок" (ПУЕ) Залежно від категорії приміщення необхідно вжити певних заходів, що забезпечують достатню електробезпеку при експлуатації і ремонті електроустаткування. Так, в приміщеннях з підвищеною небезпекою електроінструменти, переносні світильники повинні бути виконані з подвійною ізоляцією або напруга живлення їх не повинна перевищувати 42 В. В особливо небезпечних приміщеннях напруга живлення переносних світильників не повинна перевищувати 12 В [14]. Приміщення, в якому знаходиться робоче місце інженера електронщика, класифікується як приміщення з підвищеною небезпекою.

Щоб захистити людину від ураження електричним струмом, захисне заземлення має задовольняти ряду вимог, викладених у ПЗП. Захисне заземлення. Занулення ». Ці вимоги залежать від напруги електроустановок та потужності джерела живлення.

В електроустановках змінного струму напругою до 1000 В у мережі з ізольованою нейтраллю або ізольованим виводом джерела однофазного струму опір заземлювального пристрою не повинен перевищувати 4 Ом.

Важливо відзначити, що якщо занулений корпус одночасно заземлений, то це тільки покращує умови безпеки, тому що забезпечує додаткове заземлення нульового захисного дроту.

3.5 Пожежна та техногенна безпека

Пожежі в лабораторному приміщенні становлять особливу небезпеку, тому що пов'язані з великими матеріальними втратами. Характерна особливість лабораторних кімнат - невеликі площі приміщень. Як відомо, пожежа може виникнути при взаємодії горючих речовин, окислення і джерел запалю-

вання. У даному приміщеннях присутні всі три основні чинника, необхідні для виникнення пожежі.

Горючими компонентами в кімнаті є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, двері, підлоги, ізоляція кабелів і ін.

Джерелами запалювання в лабораторному приміщенні можуть бути електронні схеми від ЕОМ, прилади, застосовувані для технічного обслуговування, пристрої електроживлення, кондиціонування повітря, де в результаті різних порушень утворюються перегріті елементи, електричні іскри і дуги, здатні викликати загоряння горючих матеріалів.

В сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні дроти, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відводу надлишкової теплоти від ЕОМ служать системи вентиляції та кондиціонування повітря. При постійній дії ці системи представляють собою додаткову пожежну небезпеку.

Для більшості приміщень лабораторних кімнат встановлена категорія пожежної небезпеки В.

Однією з найбільш важливих завдань пожежного захисту є захист будівельних приміщень від руйнувань та забезпечення їх достатньої міцності в умовах впливу високих температур при пожежі. Враховуючи високу вартість електронного обладнання, а також категорію його пожежної небезпеки, будівлі для лабораторного приміщення і частини будівлі іншого призначення, в яких передбачено розміщення ЕОМ, повинні бути 1 та 2 ступеня вогнестійкості.

Для гасіння пожеж на початкових стадіях широко застосовуються вогнегасники. В лабораторних приміщеннях застосовуються головним чином вуглекислотні вогнегасники ВУ-5 (ВВК3,5), перевагою яких є висока ефективність гасіння пожежі, схоронність електронного устаткування, діелектри-

чні властивості вуглекислого газу, що дозволяє використовувати ці вогнегасники навіть у тому випадку, коли не вдається знеструмити електроустановку відразу. Вогнегасник ОУ5 (ВВК3,5) переносний з місткістю балона 5 літрів (3,5 кілограма), призначений для гасіння електроустановок, що знаходяться під напругою не більш 10 кВ. В даному приміщенні знаходиться один такий вогнегасник.

З приміщень, на випадок пожежі, має бути передбачена й забезпечена евакуація людей через так звані евакуаційні виходи. Найважливішою вимогою успішної евакуації людей і цінностей є улаштування внутрішніх переходів, пожежних сходів і аварійного освітлення. Виходи вважають евакуаційними, якщо вони ведуть із приміщень:

1) першого поверху назовні безпосередньо або через коридор, вестибюль, сходову клітку;

2) будь-якого поверху, крім першого, в коридор, що веде на сходову клітку, в тому числі через хол. При цьому сходові клітки повинні мати вихід назовні безпосередньо або через вестибюль, відокремлений від прилеглих коридорів перегородками з дверима;

3) у сусіднє приміщення на цьому ж поверсі, яке забезпечене виходами, зазначеними в пунктах 1 і 2.

Фактично, лабораторне приміщення має необхідні умови для евакуації людей і цінностей. В будівлі передбачені й забезпечені евакуаційні виходи з приміщення. Коридор веде на сходову клітку, яка має вихід безпосередньо назовні.

3.6 Розрахунок штучного освітлення лабораторного приміщення розробки схеми генератора випадкових чисел

Для освітленості приміщення з розмірами А = 6,5 м, В = 3,7 м та висотою Н = 3,5 м використовуються 2 світильники ОДР з двома люмінесцент-

ними лампами типа ЛБ - 40. Коефіцієнти віддзеркалення світлового потоку від стелі, стін і підлоги відповідно рівні $р_{стелі}$ = 70%, $Р_{стін}$ = 50%, $Р_{підлоги}$ = 10%. Затінювання робочих місць немає. Висота звісу світильника $h_з = 0$, висота робочої поверхні над рівнем підлоги $h_р = 0.8$ м.

Нормативна величина освітленості для відеоплейних терміналів складає $E_н = 400$ лк.

При перевірці відповідності освітленості в приміщенні нормативному рівню, коли відома кількість світильників, ламп, їх тип і потужність. фактичну освітленість в приміщенні визначаємо по формулі:

$$E_ф = \frac{N \cdot F \cdot n \cdot \eta}{S \cdot z \cdot k_{зап}}, \text{ (лк)} \qquad (3.1)$$

де N = 2 – число світильників, шт.;

F = 3120 лм – світловий потік лампи;

n = 2 – число ламп в світильнику;

S - площа освітлюваного приміщення;

z = 1,1 – коефіцієнт нерівномірності освітлення для люмінесцентних ламп (відношення $E_{сер} / E_{мін}$);

$k_{зап}$ = 1,5 – коефіцієнт запас, що враховує зниження освітленості із-за забруднення і старіння лампи ;

η – коефіцієнт використання освітлювальної установки.

Для визначення η необхідно знати тип світильника, індекс приміщення і коефіцієнт віддзеркалення світлового потоку від стелі, стін і підлоги. Оскільки тип світильника і коефіцієнти віддзеркалення світлового потоку відомі, то для знаходження η необхідно визначити значення індексу приміщення i.

$$i = \frac{A \cdot B}{h_п \cdot (A + B)} \qquad (3.2)$$

де A і B - відповідно довжина і ширина приміщення в м;

η_n - висота від робочої поверхні до світильника, визначається висотою приміщення (H, м) і висотою умовної робочої поверхні ($h_p = 0.8$ м) по формулі:

$$h_n = H - h_з - h_p = 3.5 - 0 - 0.8 = 2.7 \text{ (м)} \qquad (3.3)$$

Підставляємо набуте значення у формулу (3.2) і знаходимо індекс приміщення:

$$i = \frac{6.5 \cdot 3.7}{2.7 \cdot (65 + 3.7)} = \frac{24.05}{27.54} = 0.87$$

Підставляємо всі знайдені величини в формулу (3.1):

$$E_ф = \frac{2 \cdot 3120 \cdot 2 \cdot 0.89}{6.5 \cdot 3.7 \cdot 1.1 \cdot 1.5} = \frac{11107.2}{39.6825} = 279.9 \text{, (лк)}$$

Оскільки отримана величина $E_ф < E_н$ для досягнення нормативної освітленості необхідно або збільшити кількість світильників, або збільшити потужність ламп. Порахуємо міру збільшення W:

$$W = \frac{E_н}{E_ф} = \frac{400}{279.9} = 1.42 \text{ разів}$$

Тепер можна обчислити необхідну кількість світильників:

$$N_1 = N \cdot W = 2 \cdot 1.43 = 2.84 \text{ шт.}$$

Збільшимо кількість світильників до 3 штук. Тоді

$$E_ф = \frac{5 \cdot 3120 \cdot 2 \cdot 0.89}{6.5 \cdot 3.7 \cdot 1.1 \cdot 1.5} = \frac{27768}{39.6825} = 699.7 \text{, (лк)}$$

Таким чином, при збільшенні кількості світильників на три штуки фактична освітленість $E_ф$ практично відповідає нормативному значенню освітленості $E_н = 400$ лк.

Такий же ефект може бути отриманий при заміні лампи з великим світловим потоком. Порахуємо необхідний світловий потік лампи:

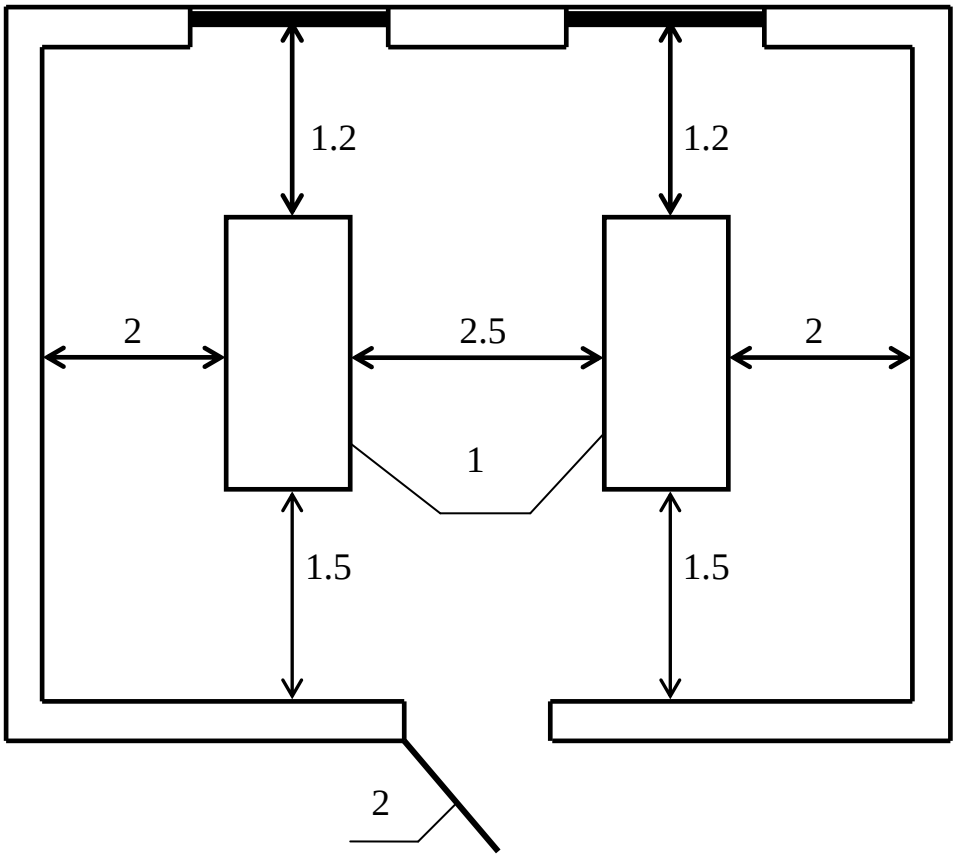
$$F_1 = F \cdot W = 3120 \cdot 1.42 = 4430.4 \text{, (лм)}$$

Так, якщо всі лампи типа ЛБ-40 в приміщенні замінити на лампи типа ЛТБ-65 з F=3980 лм $E_ф$ буде рівне:

$$E_{\phi} = \frac{2 \cdot 3980 \cdot 2 \cdot 0.89}{6.5 \cdot 3.7 \cdot 1.1 \cdot 1.5} = \frac{14168.8}{39.6825} = 357, \text{ (лк)}$$

Таким чином, в цьому випадку фактична освітленість також практично відповідатиме нормативному значенню.

На рисунку 3.2 представлена схема розташування двох світильників, в кожному з яких знаходиться по дві лампи типу ЛТБ-65.



1 – світильник;

2 – двері

Рисунок 3.2 – План розташування світильників в лабораторному приміщенні

Висновки та рекомендації

1. Проведений аналіз проблем, які виникають при рішенні задач отримання випадкової інформації, дозволив розробити оптимальну функціональну схему генератора випадкових чисел.

2. Схема генератора випадкових чисел відрізняється від існуючих апаратних аналогів компактністю та стабільністю параметрів.

3. Аналіз функціонування пристрою показує правильність функціонування згідно з поставленим завданням..

Розроблений пристрій рекомендується для впровадження в системах обробки інформації мікроелектронних інформаційних систем.

Перелік посилань

1. Горбенко І. Д., Шапочка Н. В. Аналіз генераторів випадкових бітів згідно стандарту ISO/IEC 18031 та рекомендації щодо його застосування в Україні. Міжнародний симпозіум «Вопросы оптимизации вычислений». Кацивелі, 2009. С.164-170.

2. Henk C. A., Tilborg V. A. Encyclopedia of Cryptography and Security. USA : Springer Science+Business Media, 2005. P. 509-514.

3. Потий А. В., Пестерев А. К., Олейников Р. В. Декомпозиция требований, предъявляемых к генераторам случайных и псевдослучайных чисел, на основе классификации специальных данных. Матеріали науково-практичної конференції «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». Київ : НТУУ "КПІ", 1998. С. 194.

4. Торба А. А., Елаков С. Г., Степченко А. З. Генерация равновероятных случайных последовательностей на основе физических датчиков. Всеукр. межвед. науч.-техн. сб. Радиотехника. Вып. 119, 2001. С.108-114.

5. Malgorzata Marek-Sadowska. Spherical Pseudo-Random Pattern Testing. Electrical and Computer Engineering Department University of California, Santa Barbara, CA 93106. Final Report 1997-98 for MICRO Project. P. 97-109.

6. Fritz J. Mixed-Signal Testing of Integreted Analog Circuits and Electronic Modules, College of Engineering and technology Ohio University In partial Fulfillment of the Requirement for the Degree, 1999. P. 67-84.

7. Бойко В.І., Гуржій А.М., Жуйков В.Я. Основи схемотехніки електронних систем [Підручник]. К. : Вища шк., 2004. 527 с.

8. Ненашев А. П., Коледов Л. А. Основы конструирования микроэлектронной аппаратуры. М. : Радио и связь, 1981. 315 с.

9. Николаев И.М., Филинюк Н.А. Микроэлектронные устройства и основы их проектирования. М. : Энергия, 1979. 271 с.

10. Степаненко И.П. Основы микроэлектроники. М. : Энергия, 1979. 292 с.

11. Верьовкін Л.Л., Світанько М.В., Кісельов Є.М., Хрипко С.Л. Цифрова схемотехніка: підручник. Запоріжжя : ЗДІА, 2016. 214 с.

12. 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.

13. Ткачук К. Н. Охрана труда и окружающей среды в радиоэлектронной промышленности. К. : Вища шк., 1988. 240 с.

14. Горобец А. И., Степаненко А. И. Охрана труда в радиоэлектронной промышленности. К. : Техника, 1987. 345 с.