МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра електроніки і комп'ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи
бакалавр на тему:

Комбінаторний пристрій захисту даних на основі площинних кодів

Завідуючий кафедрою А. С. Опанасюк

Керівник кваліфікаційної роботи
бакалавра М. С. Шевченко

Виконав студент С. С. Кузьменко

Суми - 2024

РЕФЕРАТ

Наведена пояснювальна записка складається з 40 сторінок, включаючи 4 таблиці, 18 джерел, 9 рисунків та супровідну графічну частину.

Обґрунтування вибору теми Комбінаторний пристрій захисту даних на основі площинних кодів є перспективним напрямком в цій сфері. Він поєднує в собі ефективність та надійність захисту інформації з можливістю швидкого та зручного доступу до неї для авторизованих користувачів.

Мета та завдання роботи Метою даної роботи є розробка та реалізація комбінаторного пристрою захисту даних на основі площинних кодів, а також вивчення його ефективності та можливостей застосування.

Основними завданнями дослідження є:

1. Проведення аналізу сучасних методів та засобів захисту інформації.
2. Розробка алгоритму комбінаторного захисту даних на основі площинних кодів.
3. Реалізація пристрою та проведення його тестування на ефективність та надійність захисту.

Структура роботи Робота складається з вступу, трьох розділів, висновків та списку використаних джерел.

У **першому розділі** проведено огляд сучасних методів та засобів захисту інформації, а також обґрунтовано необхідність розробки нових підходів.

Другий розділ присвячено розробці самого пристрою захисту даних на основі площинних кодів. Тут представлено розроблений алгоритм, архітектуру пристрою та методи його впровадження.

У **третьому розділі** наведено результати тестування розробленого пристрою, а також його порівняння з існуючими рішеннями.

Висновки містять узагальнення отриманих результатів, висновки щодо ефективності та перспектив розвитку розробленого пристрою.

Список використаних джерел містить перелік літературних джерел та інших матеріалів, використаних при підготовці роботи.

ЗМІСТ

ВСТУП

Пристрій захисту даних, який поєднує в собі безпеку та конфіденційність, має першочергове значення в сучасному суспільстві, оскільки як безпека даних, так і конфіденційність стають все більш занепокоєними. У цифровому світі, який перенаселений технологічними інноваціями та створює зростаючу загрозу кібербезпеці, як ніколи важливо розробити ефективний захист.

Ця бакалаврська робота присвячена дослідженню та створенню комбінаторного пристрою захисту даних на основі використання плоских кодів. Цей пристрій не тільки враховує сучасні технологічні досягнення, але й пропонує унікальний підхід до захисту інформації, який забезпечує високий ступінь безпеки та надійності.

У даному дослідженні виконано комплексний аналіз фахової літератури з комбінованого захисту даних і планарних кодів. Описує технічні вимоги та основні принципи роботи пристрою. Він містить огляд найновіших підходів до захисту інформації та інноваційних методів шифрування.

Основним завданням цього дослідження є дослідження та розробка ефективного комбінованого пристрою захисту інформації на основі планарних кодів, а також його експериментальна перевірка та апробація.

При цьому особлива увага приділяється створенню унікальних та інноваційних рішень, які мають потенціал для впровадження в реальні системи захисту інформації.

Тому це дослідження є актуальним і перспективним внеском у розвиток сучасних технологій захисту даних.

Впроваджуючи розроблений комбінований пристрій, можна істотно підвищити рівень інформаційної безпеки в самих різних сферах, від корпоративного до особистого використання.

1. ОГЛЯД ЛІТЕРАТУРИ ТА ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУВАННЯ

1.1Огляд літератури

У сучасному цифровому світі захист даних є однією з найактуальніших проблем. Загрози конфіденційності та цілісності інформації зростають, що змушує наше суспільство ефективно захищати конфіденційність і дані.

У цьому контексті плоскі коди відіграють ключову роль у розробці комбінованих пристроїв захисту даних. Ця інноваційна технологія поєднує математичні принципи та методи шифрування для забезпечення найвищого рівня безпеки.

Що таке плоскі коди і як вони працюють? Площинні коди — це спеціально розроблені коди, які можна представити у вигляді геометричних областей на площині. Ці області можна використовувати для зберігання та передачі інформації з високою надійністю та безпекою.

Головною перевагою використання плоских кодів у захисті даних є їх надзвичайна стійкість до хакерських атак. Інші методи шифрування можуть бути вразливими до відомих атак, але плоский код забезпечує додатковий рівень безпеки завдяки своїй композиційній природі.

Крім того, використання плоских кодів у комбінованих пристроях захисту даних відкриває нові можливості для розробки ефективних і економічних систем захисту, які можна використовувати в різних сферах, таких як фінанси, медицина та інформаційні технології.

Тому плоскі коди представляють захоплюючу область досліджень у сфері кібербезпеки та захисту даних. Вони відкривають нові перспективи для розробки ефективних і надійних систем захисту для збереження даних у цифрову епоху.

Хронологія розвитку засобів захисту інформації

Розвиток технологій захисту даних відображає важливість забезпечення конфіденційності, цілісності та доступності інформації в сучасному цифровому світі. Від перших етапів розвитку комп’ютерних технологій до сучасних інноваційних рішень хронологія розвитку обладнання для захисту даних свідчить про постійне вдосконалення та адаптацію до нових загроз і вимог.

1. Перші спроби захисту даних з’явилися з появою персональних комп’ютерів і комп’ютерних мереж. Протягом цього часу для захисту інформації використовуються основні методи шифрування та автентифікації.

2. Підвищена складність шифрування

З часом, у міру збільшення кількості та складності атак на інформаційні системи, методи шифрування стали більш досконалими та ефективними. Розвиток алгоритмів шифрування та впровадження криптографічних стандартів відкрили нові можливості захисту даних.

Сучасні системи зв’язку складаються з багатьох складних пристроїв, які перетворюють повідомлення та сигнали для найбільш ефективної передачі інформації. Дані передаються від джерела до приймача через складне обладнання, як показано на рисунку 1.1, який ілюструє структуру системи кодування цифрового зв’язку. Структура включає джерела даних, вихідні кодери, кодери, канальні кодери, модулятори, канали, демодулятори, канальні декодери, декодери, вихідні декодери та приймачі даних.

Джерело сигналу складається з джерела повідомлення та перетворювача, який перетворює повідомлення в первинний сигнал, який потім направляється на вхід кодера. Кодер виконує завдання кодування (з акцентом на ефективність і стійкість до перешкод), перетворюючи повідомлення в серію кодових символів. Ці символи утворюють цифровий сигнал, що складається з імпульсів («одиниць») і пауз («нулів»). Рухаючись далі, цей цифровий сигнал надсилається до модулятора, де прямокутні імпульси поєднуються з радіочастотним коливанням несучої, щоб сприяти ефективній передачі по лінії зв’язку. Це призводить до створення модульованого сигналу. Згодом модульований сигнал передається через канал зв’язку, де він зазнає спотворень, спричинених руйнівними флуктуаціями, відомими як інтерференція. Ці флуктуації мають випадковий характер і характеризуються білим гаусовим шумом.

Демодулятор вносить шум у сигнал на своєму виході, що призводить до рандомізованого результату. У результаті декодований сигнал може не відповідати вихідному сигналу. Основним призначенням кодера є реалізація стійкого до помилок кодування, що дозволяє ідентифікувати та виправляти помилки, що виникають під час передачі інформації.

Модулятор, який контролює параметри коливання (амплітуду, частоту, фазу), визначає тип модуляції, що впливає на конструктивне виконання модулятора.

Канал зв'язку може бути фізичним, наприклад, кабельним, або логічним, або мультиплексованим, наприклад, радіоканалом у комунікаційних і комп'ютерних технологіях. Канал передає сигнал із інформацією від відправників до одержувачів у певному діапазоні частот, який зазвичай виражається в Гц або бітах на секунду.

Теорія інформації вважає, що канал є концептуальною структурою з певним типом помилки. У зв'язку з цим запам'ятовуючий пристрій також можна вважати каналом зв'язку, цей канал дозволяє зберігати і передавати сигнал певної тривалості. Теорема про шумове кодування каналу (теорема Шеннона) стверджує, що для будь-якого рівня шуму дискретна інформація може передаватися майже без помилок до певної максимальної швидкості передачі.

Поняття канального кодування виникло через неминучу наявність помилок у будь-якому каналі зв'язку. Радіохвилі, електричні сигнали і навіть світлові хвилі в оптичних каналах зазвичай супроводжуються певним шумом і втратою сигналу на кінцевій відстані. Для вирішення цих проблем було запропоновано численні гіпотези в цих областях прикладної математики, включаючи теорію інформації та теорію кодування.

Перешкодостійке кодування досягається шляхом доповнення переданого сигналу додатковою інформацією, яка дозволяє виправляти помилки. Одним із методів є кодування FEC (кодування з упередженим виправленням помилок), яке передбачає підготовку бітів за допомогою алгоритму, який виправляє помилки на кінці прийому. Іншим підходом є кодування ARQ (автоматичний запит на повторення), коли приймач чує передачу та запитує повторну передачу, якщо її розпізнають.

Основи канального кодування були закладені математиком Річардом Хеммінгом, який популяризував код під назвою «Хеммінга». Це був перший прямий код для виправлення помилок, який використовував додаткові біти, звані бітами парності, для регулювання цілісності даних. Підрахунок цих бітів на приймальному кінці дозволяє нам розпізнавати помилки, визначати їхню позицію в бітовому рядку та пропонувати способи їх виправлення, щоб відновити вихідне повідомлення.

Код Хеммінга є частиною класу блокових кодів, який є підмножиною методів канального кодування. Блокові коди використовують блоки попередньо встановленої довжини, які називаються кодовими словами, які містять як інформаційні, так і керуючі біти. Незважаючи на те, що ці коди підвищують

точність передачі даних, вони збільшують загальний обсяг даних, що може вплинути на пропускну здатність каналу.

Інший підхід до канального кодування полягає у використанні згорткових кодів, ці коди можуть швидше обробляти будь-яку довжину потоку бітів. Одним із найвідоміших прикладів згорнутих кодів є код Вітербі, створений італійським вченим Ендрю Вітербі. Основним недоліком цього підходу є зростаюча складність декодування кодів із збільшенням їх довжини. Згорткові коди часто поєднуються з блоковими для створення складних систем виправлення помилок.

Кодування та декодування відіграють важливу роль у сфері зв’язку, включаючи цифрову електроніку, програмування, передачу даних і взаємодію з людьми. Ці процедури перетворюють вміст, щоб забезпечити оптимальну передачу або зберігання. Перетворення вважається ефективним, якщо воно досягає максимально можливої пропускної здатності каналу для даного рівня продуктивності джерела.

Процес кодування-декодування можна розділити на два етапи:

Модуляція-демодуляція: перетворення безперервного сигналу радіоканалу на дискретний.

Кодування-декодування: обробка послідовності символів.

Кодування-декодування включає два протилежні кроки:

Усунення надлишку у вихідному сигналі (економне кодування).

Додавання надлишку для підвищення надійності передачі (надмірне кодування).

При надмірному кодуванні у переданий потік додаються допоміжні символи для виправлення помилок на приймальній стороні, що збільшує швидкість передачі та ширину смуги, але може призвести до втрат енергії сигналу.

Теорема Шеннона про пропускну здатність каналу показує, що використання оптимального кодування дозволяє збільшити пропускну здатність каналу при розширенні його смуги. Надмірне кодування широко застосовується для підвищення якості передачі, особливо останніми десятиліттями, завдяки розвитку складних обчислювальних пристроїв у компактних розмірах.

Сигнали в каналах зв'язку піддаються спотворенням, шумам та перешкодам, що можуть призвести до переходу одного символу в інший. Різні типи каналів розрізняються за характером помилок:

Симетричний канал: всі помилки рівноймовірні.

Асиметричний канал: деякі помилки більш імовірні.

Канал без пам'яті: спотворення символу не залежить від інших.

Канал з пам'яттю: спотворення залежить від попередніх символів.

Канал із стиранням: разом з помилками відбувається стирання символів.

Канал зв’язку характеризується такими показниками:

Пропускна здатність: максимальна кількість бітів, переданих за одиницю часу з мінімальною ймовірністю помилок.

Швидкість передачі: кількість бітів, переданих за одиницю часу, завжди менша за пропускну здатність.

Максимальна швидкість передачі досягається за допомогою завадостійкого кодування. Якщо код виправляє найбільш ймовірні помилки, надмірність виправдана. В іншому випадку, помилки можуть бути не виправлені або навіть збільшені, що погіршить передачу.

Завадостійкі коди розрізняються за основою q, відстанню d, надмірністю, структурою, енергетичною ефективністю, кореляційними властивостями та алгоритмами. Вони класифікуються на різні типи, як показано на рис. 1.2. Введення комбінаторних пристроїв захисту даних, таких як пристрої на основі площинних кодів, відображає постійний прогрес у напрямку розробки більш надійних та ефективних методів захисту. Ці пристрої використовують складні алгоритми та математичні моделі для створення непереборних перешкод для несанкціонованого доступу до інформації.

Сучасні комбінаторні пристрої захисту даних інтегруються в різноманітні системи та пристрої, що робить їх доступними для широкого кола користувачів. Завдяки постійному вдосконаленню та оптимізації, ці пристрої стають невід'ємною частиною сучасних інформаційних технологій. В сучасному світі, де загрози кібербезпеки постійно зростають, інноваційні технології стають невід'ємною складовою сфери захисту даних. Один із передових методів захисту інформації — використання комбінаторних пристроїв на основі площинних кодів. Площинні коди виявляються не лише ефективними для збереження та передачі інформації, але й відкривають нові можливості для розробки надійних засобів кіберзахисту.

Рисунок 1.2 – Характеристика перешкодостійких кодів

Основне призначення планарних кодів у системах захисту даних полягає у розробці складних схем шифрування, які значно ускладнюють доступ до інформації для несанкціонованих осіб. Завдяки комбінації планарних кодів створюються дуже складні криптографічні системи, що вирізняються високою надійністю у порівнянні з іншими методами. Однією з ключових переваг площинних кодів є їх здатність забезпечувати високу ємність та низький рівень помилок. Це робить їх особливо привабливими для застосування у пристроях для зберігання та передачі конфіденційної інформації, де важливі не тільки високий рівень захисту, але й ефективність обробки даних.

Крім того, площинні коди ефективно використовуються у сучасних системах аутентифікації та контролю доступу. Вони дозволяють створювати унікальні ідентифікатори, які важко підробити або замінити, забезпечуючи тим самим високий рівень безпеки у системах, що потребують автентифікації користувачів.

Рисунок 1.3 – Демонстрація моделі цифрового зв’язку

Джерело інформації генерує дані у вигляді бінарних сигналів. Ймовірність виникнення нулів і одиниць може бути нерівномірною, і вони можуть з'являтися залежно один від одного [3]. Основне завдання кодера полягає в завадостійкому кодуванні сигналу, тобто в такому кодуванні, яке дозволяє виявляти та значною мірою виправляти помилки, що виникають під час проходження сигналів через канал зв'язку від передавача до приймача.

Модулятор – це пристрій, що коригує параметри переданого сигналу відповідно до змін інформаційного сигналу, забезпечуючи перетворення вихідних послідовностей кодера у задану множину сигналів.Канал зв'язку (англ. Channel, data line) - це комплекс технічних засобів і середовище, призначене для передачі сигналів в одному напрямку від джерела до приймача даних. У випадку використання провідного зв'язку, середовищем можуть служити оптичне волокно або кручені пари проводів.

Канал зв'язку є частиною системи передачі даних.

Основні характеристики каналу зв'язку включають:

1. Ширину ефективної смуги частот.
2. Динамічний діапазон.
3. Хвильовий опір.
4. Проникну здатність.
5. Завадостійкість.
6. Ємність.

Демодулятор - це пристрій, що виконує демодуляцію, тобто процес виділення інформаційного сигналу з модульованого високочастотного коливання.

Декодер виконує операцію декодування.

Для моделювання дискретного каналу необхідно визначити множину вхідних і вихідних кодових символів та множину умовних ймовірностей вихідних символів при заданих вхідних.

Коди можна поділити на дві категорії: надлишкові і ненадлишкові. Надлишкові коди дозволяють виявляти і виправляти помилки, що виникають через перешкоди і спотворення кодових комбінацій.

У надлишкових кодах є як інформаційні, так і перевірочні елементи. Вони поділяються на рівномірні (з постійною кількістю розрядів) та нерівномірні (з непостійною кількістю розрядів). Надлишкові коди також поділяються на безперервні (рекурентні), де кодування і декодування відбувається безперервно, і блокові, де кожне повідомлення відповідає окремій кодовій комбінації або блоку з фіксованою кількістю елементів. Блоки кодуються і декодуються незалежно один від одного.

Роздільні блокові коди, у свою чергу, поділяються на систематичні, де інформаційні елементи займають певні позиції в коді, і несистематичні, де інформаційні елементи не мають фіксованих позицій у кодовій комбінації.Систематичним розділеним блоковим кодом називається той код, де перші m позицій (розрядів) зайняті інформаційними елементами, а останні r = n - m позицій - перевірочними. Ці коди забезпечують можливість легкої ідентифікації і виправлення помилок.

Несистематичні блочні коди відрізняються тим, що інформаційні елементи можуть розміщуватись на довільних позиціях у кодовій комбінації, і не обов'язково займають перші k позицій.

Серед систематичних кодів особливе місце займають циклічні коди, які мають додаткові математичні властивості, що полегшують їхню реалізацію і аналіз.

При виборі кодів для передачі інформації враховують такі основні характеристики:

- кількість інформаційних елементів m;
- кількість перевірочних елементів r (для коригувальних кодів);
- довжина (розрядність) n коду, де n = m + r;
- потужність коду N,- кількість можливих кодових комбінацій, які використовуються для передачі повідомлень;
- основа (алфавіт) q коду, яка визначає число можливих символів у кодовій комбінації;

- повне число кодових комбінацій N, яке рівне q ^{n} (для двійкових кодів – N = 2 ^{n});
- надмірність коду R, яка відображає ступінь надлишковості коду і його здатність виявляти та виправляти помилки.

$$R_{и} = 1 - \frac{\log_q N_p}{\log_q N}, \qquad (1.1)$$

Чи $N_p = 2^m$ та $N = 2^n$

$$R_{и} = 1 - \frac{m}{n} = \frac{r}{n}; \qquad (1.2)$$

- відносна швидкість коду R, що характеризує ступінь використання у надмірному коді інформаційних можливостей його потужності,

$$R = \frac{\log_q N_p}{\log_q N} \text{ або } R = \frac{m}{n} = 1 - R_{и}; \qquad (1.3)$$

- вага кодової комбінації (коду) ω(в двійковому коді визначається числом одиниць у кодовій послідовності.);
- мінімальна кодова відстань коду

$$d = \min_{ij} d_{ij}, \qquad (1.4)$$

що визначається як найменша відстань серед всіх отриманих кодових відстаней між парами кодових комбінацій цього коду. Кодова відстань $d_{ij}d_{ij}$ між ii-ю та jj-ю комбінаціями цього коду визначається згідно з правилом

$$d_{ij} = \sum_{l=1}^{n} \left| a_{li} - a_{lj} \right|, \qquad (1.5)$$

де $a_{l\,i}$, a_{lj} – елементи, що стоять на l -му місці в i -й та j -й комбінаціях, тобто d_{ij} визначається числом однойменних розрядів із різними значеннями;

- Ймовірність невиявленої помилки PалеPале - ймовірність, що прийнята кодова комбінація відрізняється від переданої, але властивості коду не дозволяють визначити факт помилки.
- Ймовірність виявленої помилки PооPоо - ймовірність, що прийнята кодова комбінація відрізняється від переданої і завдяки властивостям коду встановлюється наявність помилки.

- Ймовірність помилки, що виправляється PіоPіо - ймовірність, при якій кодова комбінація відрізняється від переданої, але завдяки властивостям коду помилка виправляється.
- Ймовірність виникнення помилки PошPош - ймовірність, що прийнята кодова комбінація відрізняється від переданої ($P_{ош}=P_{але}+P_{оо}$).
- Кратність помилки v - кількість виявлених і виправлених помилок.
- Ефективність коду - загальна оцінка якості кодування і декодування за вищевказаними параметрами.

$$r_э = \frac{N_р}{N} \frac{P_{ош}}{P_{ош} - \sum_{i=1}^{v} P_i}, \quad (1.6)$$

Ступінь захисту від помилок у методі кодування визначається мінімальною кодовою відстанню d для даного коду. Виділяють три основні типи кодових відстаней: Хеммінга, Лі та матричну. Найпоширенішою в теорії кодування є кодова відстань Хеммінга, оскільки вона безпосередньо пов'язана з поняттям ваги кодової комбінації. Вона визначається як кількість позицій, у яких дві комбінації однакової довжини n відрізняються одна від одної. Для двійкових кодів, де сума однакових елементів дорівнює 0, а різних – 1, відстань Хеммінга між двома кодовими комбінаціями можна обчислити за допомогою побітового XOR їхніх бітів і підрахунку кількості ненульових бітів (це також відоме як вага такої суми). Загальна кількість комбінацій довжини n дорівнює $2n$, а кількість комбінацій, які знаходяться на відстані d від даної комбінації, визначається кількістю способів вибрати d елементів з n.

$$C_n^d = n!/d!(n-d)!. \quad (1.7)$$

Щоб знайти комбінацію, яка відрізняється від заданої на відстань d, можна додати до неї будь-яку комбінацію з вагою d (з d одиницями і n – d нулями). Додавання відбувається по mod2.

Для виявлення всіх помилок кратності v, кодова відстань має бути

$$d \geq v_{про} + 1, \quad (1.8)$$

виправлення помилок кратності v_i –

$$d \geq 2 \cdot v_{та} + 1. \quad (1.9)$$

виправлення та виявлення помилок кодова відстань

$$d \geq v_i + v_{про} + 1. \quad (1.10)$$

Приклади кодів для виявлення і коригування помилок, які широко використовуються в інформаційних системах, включають коди з перевіркою на

парність, просте повторення, коди Хеммінга, коди з постійною вагою та площинні коди.

Код з перевіркою на парність має відстань d = 2 і дозволяє виявляти всі помилки, які трапляються непарну кількість разів. Завдяки своїй простоті та низькій надмірності, цей код набув великої популярності в системах зв'язку.

Код із простим повторенням також має відстань d = 2 і дозволяє виявляти всі помилки, за винятком тих, що виникають у позиціях, які збігаються у першій і другій частині коду.

Код Хеммінга має відстань d = 4, що дозволяє виправляти всі одноразові помилки та виявляти всі помилки, які трапляються двічі.

Коди рівної ваги (збалансовані коди) мають певні переваги при застосуванні в асиметричних каналах, які часто зустрічаються на практиці. У таких каналах ці коди здатні виявляти всі непарні множинності помилок. Однак серед парних помилок залишаються невиявленими ті, де одне число перетворюється з 0 на 1, а інше - з 1 на 0. Коди постійної ваги широко застосовуються в SPD, але не забезпечують виправлення помилок. Для цього рекомендується використовувати планарний код з d = 4, який може виправити всі одиничні помилки і виявити всі подвійні помилки. Додатковою перевагою є те, що цей код є комбінаційним кодом із постійними вагами, що спрощує перетворення збалансованого коду в плоский код із мінімальними витратами на обладнання.

Таким чином, використання плоских кодів у комбінованих пристроях захисту даних впливає на різні рівні захисту - від шифрування до автентифікації користувача. Їхні унікальні функції та можливості роблять їх важливим інструментом у боротьбі з кіберзлочинністю та забезпеченні безпеки в цифровому середовищі.

1.2 Постановка завдання проектування

Метою розробки даного комбінаторного пристрою є: Розробка комбінаторного пристрою захисту даних, що базується на використанні площинних кодів. Робота має на меті створення ефективного засобу захисту конфіденційної інформації шляхом застосування новаторських технологій у сфері криптографії.

Аналіз методів захисту даних: Огляд існуючих методів захисту інформації, їх переваги та недоліки.

Створення площинних кодів: Розробка алгоритму створення площинних кодів для захисту даних. Врахування стійкості до криптоаналітичних атак.

Реалізація комбінаторного пристрою: Створення пристрою, що застосовує розроблені площинні коди для захисту даних. Врахування технічних аспектів, таких як енергоефективність та надійність роботи.

Тестування та аналіз результатів: Проведення тестування розробленого пристрою на різних тестових наборах даних. Аналіз отриманих результатів та оцінка ефективності захисту.

Виходячи з аналізу джерел та сучасних тенденцій у розвитку цифрових систем передачі даних, було сформульовано завдання для проектування комбінаторного пристрою захисту даних на основі площинних кодів з такими характеристиками:

1. Швидкість передачі даних не повинна перевищувати 120 Кбіт/сек.
2. Максимальна довжина лінії зв'язку становить 1,5 км.
3. Ймовірність спотворення одного біта у каналі зв'язку не повинна перевищувати 10^{-3}.
4. Пристрій повинен виявляти усі однократні та двократні помилки в інформаційній послідовності та виправляти усі однократні помилки.
5. Довжина інформаційних послідовностей повинна бути 8 або 27.
6. Затримка декодування не повинна перевищувати 1 мкс.
7. Кількість розрядів дискретного індикатора повинна складати 5.
8. Об'єм архіву даних має бути 1,3 Кбіт.
9. Споживана потужність пристрою не повинна перевищувати 8 Вт.
10. Надійність пристрою має бути не меншою за 3200 годин.

2. СИНТЕЗ І ОБҐРУНТУВАННЯ АЛГОРИТМУ РОБОТИ І СТРУКТУРНОЇ СХЕМИ КОМБІНАТОРНОГО ПРИСТРОЮ ЗАХИСТУ ДАНИХ НА ОСНОВІ ПЛОЩИННИХ КОДІВ

2.1Розробка алгоритму комбінаторного пристрою захисту даних на основі площинних кодів

Комбінаторний пристрій захисту даних, який базується на площинних кодах, передбачає поєднання різноманітних методів захисту для створення більш ефективної та надійної системи захисту. Основні принципи цього підходу включають мультирівневий захист, підсилення безпеки через комбінування різних методів захисту та забезпечення гнучкості та адаптивності системи до змінних потреб та загроз безпеці.

Розробка алгоритму комбінаторного пристрою захисту даних на основі площинних кодів включає такі етапи, як визначення потреб захисту даних, вибір методів захисту, реалізацію алгоритму та його налагодження. Важливим аспектом є не лише реалізація самого алгоритму, але й його відповідність вимогам ефективності та безпеки.

Комбінаторний пристрій захисту даних на основі площинних кодів відзначається кількома перевагами. Серед них варто відзначити високу стійкість до помилок, гнучкість конфігурації та ефективність. Ці переваги роблять його привабливим вибором для застосування у системах, де вимагається надійний та ефективний захист даних.

Алгоритм роботи комбінаторного пристрою захисту даних на основі площинних кодів зображено на рисунку 1.2.

З метою виконання поставленої задачі, адаптивний пристрій площинного кодування інформації повинен отримувати дискретні сигнали через канал зв'язку, проводити їх декодування, виконувати перевірку на наявність помилок та виправлення однократних помилок. Після цього пристрій має здійснити обчислення та відображення результатів на дискретному індикаторі.

У проектованому пристрої площинного кодування використовується двійковий біноміальний код з довжиною двійкового кодового слова n = 4 та числом одиниць k = 2.

Максимальне число кодових комбінацій обчислюється за наступною формулою:

Згідно (2.1) знаходимо

$$N=C^{k}_{n+1}=(n+1)!/k!(n-k+1)! \quad (2.1)$$

$$N=C^{2}_{4+1}=(4+1)!/2!(4-2+1)!=10 \quad (2.2)$$

Цей результат показує, що кожній десятковій цифрі відповідає певна бінарна комбінація за біноміальним принципом. Проектований адаптивний пристрій площинного кодування має реагувати на керуючі команди, які надходять від зовнішнього пристрою. Починаючи з початкового стану, всі вузли пристрою перебувають у нульовому стані. Код, що надходить через канал зв'язку, спочатку перетворюється з послідовного формату в паралельний. Потім проводиться перевірка на наявність помилок, які можуть бути у цій комбінації. Після визначення номера помилкового біту здійснюється його виправлення. Після виявлення та виправлення помилок числові дані зберігаються для подальшої передачі зовнішньому пристрою. Нарешті, числові дані та результати обчислень виводяться на дискретний індикатор. Формула (2.2) показує функцію кодування для двійкової біноміальної системи числення, яка використовується для отримання відповідної двійкової біноміальної комбінації.

$$A_j = a_{j-1} \cdot C_{n-1}^{k-q_j} + \cdots + a_L \cdot C_{n-j+1}^{k-q_{L+1}} + \cdots + a_0 \cdot C_{n-j}^{k-q1} \quad (2.2)$$

n-довжина двйкового кодового слова;

k – число одиниць в двійковому слові.

aL – означає цифру L-ног розряду

L=j-1,…,0 – порядковий номер розряду

qL – сума одиниць від j-1 до L

$$q_L = \sum_{\gamma=L}^{j-1} a_y \quad (2.3)$$

$$Q_j=a_j=0$$

У своєму дипломному проекті, після ретельного аналізу перешкодостійких кодів, я вирішила використати комбінаторний площинний коригуючий код.

Цей тип коду дозволяє виявити помилки у площині завдяки використанню перевірочних та інформаційних символів. Залежно від ступеня шуму на каналі,

було реалізовано режим роботи як для незашумлених, так і для сильно зашумлених каналів.

Використання площинних кодів дозволяє системі визначати будь-яку точку на площині за допомогою комбінаторних координат.

$$m = C_k^2 = \frac{1}{2} * k(k-1) \quad (2.4)$$

k – це число контрольних символів.

m – інформаційні символи.

Загальна кількість символів n – сума контрольних та перевірочний символів.

$$n = m + k = C_k^2 * k * (k+1). \quad (2.5)$$

Отже з (2.5) маємо:

$$k = \frac{1}{2} + \sqrt{\frac{1}{4} + 2 * m} \quad (2.6)$$

У проектованому пристрої площинного кодування було реалізовано два режими роботи: k = 7 (режим I для незашумленого каналу) і k = 4 (режим II для сильнозашумленого). Підставивши задані значення у формулу (2.4), отримаємо, що число інформаційних символів m = 21 і m = 6 відповідно. На рисунках 2.1 показано принцип формування площинного коригуючого коду для незашумленого каналу. Для цього режиму характерно те, що кожен перевірочний символ перевіряє більшу кількість інформаційних символів, ніж у режимі для сильнозашумленого каналу зв'язку. Цей режим дозволяє працювати з високою швидкістю передачі даних.

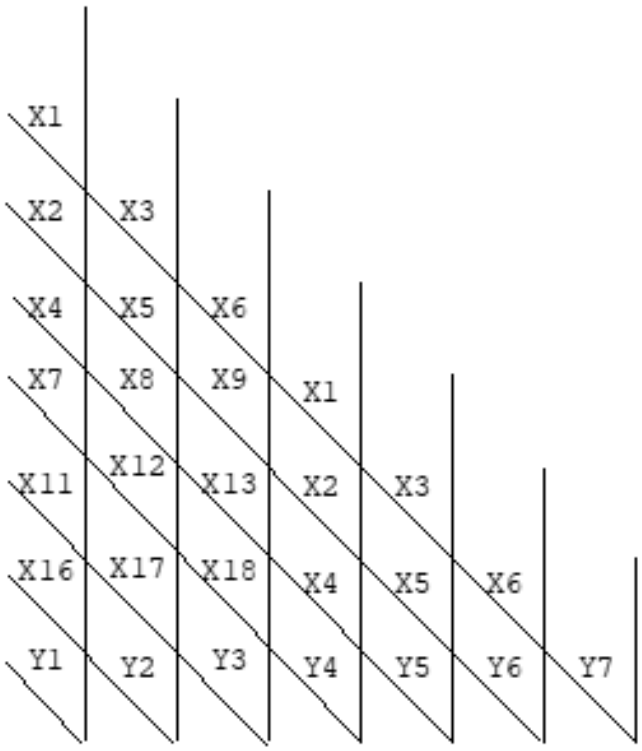

Рисунок 2.1 – Відображення роботи площинних кодів першого пристрою

На рисунку 2.2 показано принцип формування площинного коригуючого коду для сильнозашумленного каналу. Кожен перевірочний символ перевіряє меншу кількість інформаційних символів, що дозволяє ефективно виявляти однократні та двократні помилки та виправляти однократні. Режим роботи характеризується меншою швидкістю передачі даних, ніж перший режим.

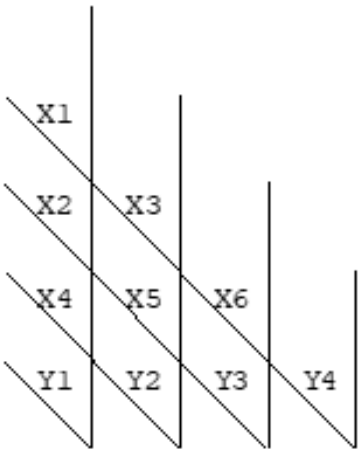

Рисунок 2.2 - Відображення роботи площинних кодів другого пристрою

Формування контролних розрядів в другому режимі:

$$y_1 = x_1 + x_2 + \mathrm{x}_4 (2.6)$$

$$\mathrm{y}_1 = \mathrm{x}_1 + \mathrm{x}_2 + \mathrm{x}_4 (2.7)$$

$$\mathrm{y}_1 = \mathrm{x}_1 + \mathrm{x}_2 + \mathrm{x}_4 (2.8)$$

$$\mathrm{y}_1 = \mathrm{x}_1 + \mathrm{x}_2 + \mathrm{x}_4 (2.9)$$

Рисунок 2.3 – Алгоритм роботи комбінаторного пристрою захисту даних на основі площинних кодів

Розробка алгоритмів для комбінаторних пристроїв захисту даних, що базуються на площинних кодах, є важливим аспектом кібербезпеки. Цей метод інтегрує переваги різних захисних технологій, дозволяючи створювати ефективні системи захисту даних, які гарантують високий рівень конфіденційності, цілісності та доступності інформації.

2.2 Розробка структурної схеми комбінаторного пристрою захисту даних на основі площинних кодів

Площинні коди є потужними засобами для зберігання і передачі інформації, оскільки вони дозволяють виявляти і виправляти помилки, що можуть виникати під час передачі. Основний принцип цих кодів полягає в організації даних у формі матриці з додаванням додаткових бітів для виявлення та корекції помилок.

Однак, використання площинних кодів само по собі не гарантує повного захисту даних. Для досягнення високого рівня безпеки необхідно створити структурну схему комбінаторного пристрою, яка забезпечуватиме не лише надійність, а й конфіденційність інформації.

Така структурна схема повинна включати не лише блоки для кодування та декодування площинних кодів, але й механізми шифрування та аутентифікації. Це дозволить захистити дані як від помилок, так і від несанкціонованого доступу.

Важливим аспектом розробки подібної схеми є оптимізація використання ресурсів, особливо в умовах обмежених обчислювальних можливостей. Застосування оптимізованих алгоритмів для кодування, декодування та шифрування сприятиме підвищенню ефективності та швидкодії пристрою.

Крім цього, структурна схема повинна бути гнучкою та легко адаптованою до різних типів даних і вимог безпеки. Це означає, що вона має бути масштабованою та здатною працювати з різними рівнями захисту відповідно до конкретних потреб користувача.

Таблиця 2.1 – Умовні позначення(Розшифрування)

ББР	блок буферного регістру
БВП1,2	перший і другий блоки виявлення помилок
БДП1,2	перший і другий блоки декодування мопилок
БВП	блок виправлення помилок
БК	блок комутації
БС	слок синхронізації
БАУ	блок адресації та управління
БПД	блок прийому даних
БПК	блок перетворення коду
БІ	блок індикації
БПІ	блок порту індикатора
ПМ	процесорний модуль
G	генератор
БВДЗП	блок видачі даних в зовнішній пристрій
БОП	блок оперативної пам'яті
БСП	блок системних програм

Вхідний буферний регістр перетворює послідовний код у паралельний формат, готуючи його для подальшої обробки. Блок виявлення помилок відзначає наявність помилок у коді. Після виявлення помилки, блок декодування точно визначає місце збою та передає цю інформацію блоку виправлення помилок. В останньому, блоку виправлення помилок доручається коригувати знайдену помилку. Після цього, інформацію можна зберігати у блоку оперативної пам'яті для подальшого використання.

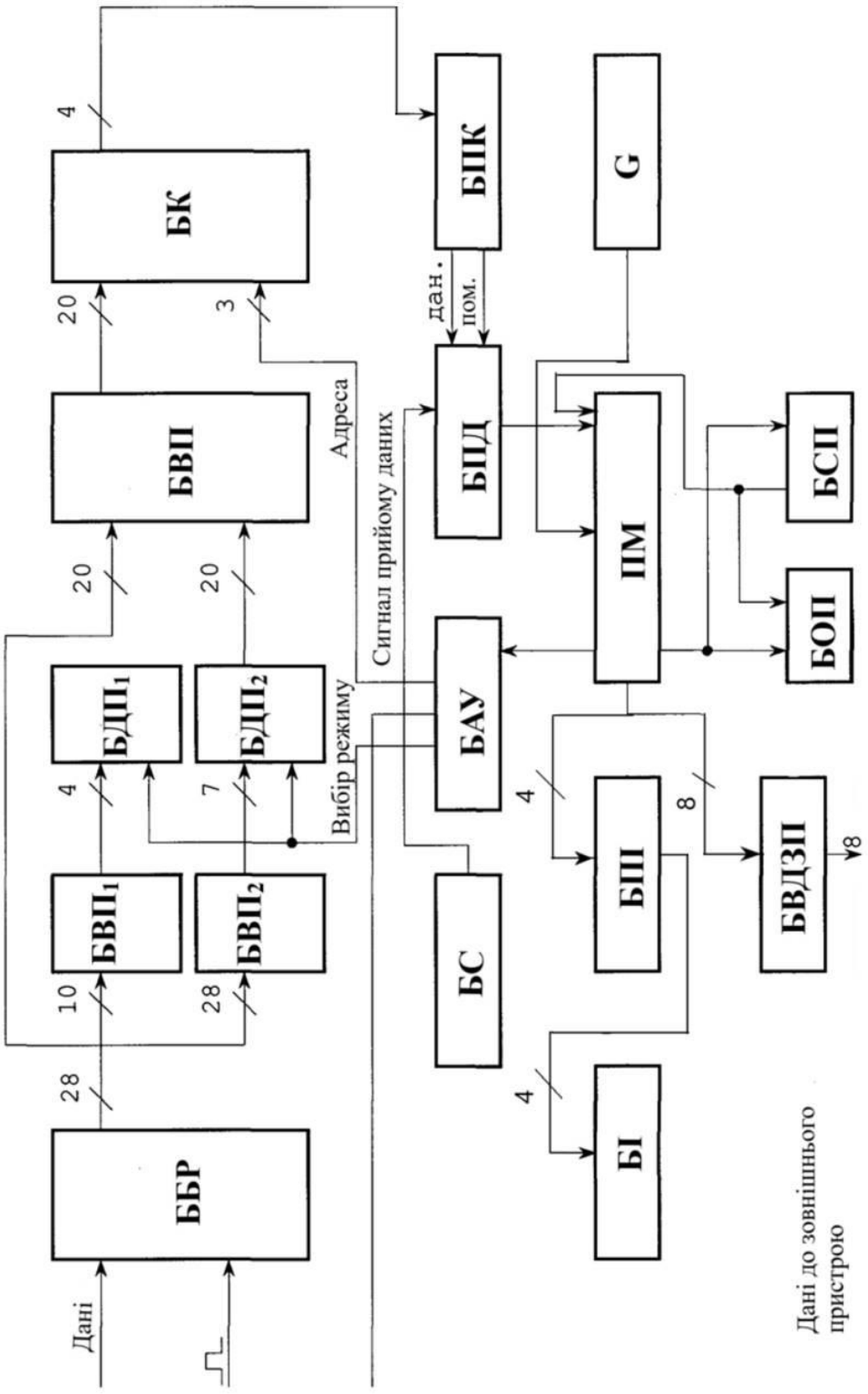

Рисунок 2.2.1 - Структурна схема комбінаторного пристрою захисту даних на основі площинних кодів

Отже, розробка структурної схеми комбінаторного пристрою захисту даних на основі площинних кодів є завданням, що вимагає глибоких знань в області теорії кодування, криптографії та алгоритміки. Це складний пазл, де кожен елемент інтегрується з іншим для створення надійного механізму захисту даних у сучасному цифровому світі.

3. РОЗРОБКА СХЕМИ ЕЛЕКТРИЧНОЇ ФУНКЦІОНАЛЬНОЇ КОМБІНАТОРНОГО ПРИСТРОЮ ЗАХИСТУ ДАНИХ НА ОСНОВІ ПЛОЩИННИХ КОДІВ

Таблиця 3.1 - Демонстрація відповідності біноміального та двійково-десяткових кодів.

Десятковий код	Біноміальний код	Двійково-десятковий код
0	0000	0000
1	0010	0001
2	0011	0010
3	0100	0011
4	0101	0100
5	0110	0101
6	1000	0110
7	1001	0111
8	1010	1000
9	1100	1001

Благодаря разработанному алгоритму работы устройства и его структурной схеме, я создал следующие функциональные модули. Комбинаторный регистр предназначен для временного хранения (буферизации) информации и используется для организации буферных запоминающих элементов, портов ввода-вывода, мультиплексоров и т. д. Комбинаторный регистр синхронизируется с тактовой частотой, переданной кодером, и преобразует последовательный код в параллельный. Он реализуется в электрической функциональной схеме с использованием сдвигового регистра, количество выходов которого соответствует длине передаваемого слова в режиме I.

Блоки обнаружения ошибок отвечают за выявление и коррекцию ошибок. Для данного устройства характерно обнаружение однократных и двукратных ошибок. На функциональной электрической схеме блоки обнаружения ошибок 1 и 2 реализуются на четырёхвходовых и семивходовых элементах сложения по модулю два, обнаруживая ошибку, если ai = 1 или bi = 1.

Для першого режиму:

$$y_1 + x_1 + x_2 + x_4 + x_7 + x_{11} + x_{16} = b_1 \quad (3.1)$$

$$y_2 + x_3 + x_5 + x_8 + x_{12} + x_{16} + x_{17} = b_2 \quad (3.2)$$

$$y_3 + x_6 + x_9 + x_{11} + x_{13} + x_{17} + x_{18} = b_3 \quad (3.3)$$

$$y_4 + x_7 + x_{10} + x_{12} + x_{14} + x_{18} + x_{19} = b_4 \quad (3.4)$$

$$y_5 + x_4 + x_8 + x_{13} + x_{15} + x_{19} + x_{20} = b_5 \quad (3.5)$$

$$y_6 + x_2 + x_5 + x_9 + x_{14} + x_{20} + x_{21} = b_6 \quad (3.6)$$

$$y_7 + x_1 + x_3 + x_6 + x_{10} + x_{15} + x_{21} = b_7 \quad (3.7)$$

Для другого режиму:

$$y_1 + x_1 + x_2 + x_4 = a_1 \quad (3.8)$$

$$y_2 + x_3 + x_4 + x_5 = a_2 \quad (3.9)$$

$$y_3 + x_2 + x_5 + x_6 = a_3 \quad (3.10)$$

$$y_4 + x_1 + x_3 + x_6 = a_4 \quad (3.11)$$

Блоки декодування помилок 1 і 2 визначають біт, у якому сталася помилка, і передають його номер у блок корекції помилок. Для комбінаторного пристрою на основі площинного кодування властиве виправлення лише одиночних помилок. Якщо дві з перевірок a1, a2, a3, a4 або b1, b2, b3, b4, b5, b6, b7 дорівнюють 1, блоки ідентифікують помилковий біт. Це реалізується за допомогою дешифратора, на адресні входи якого подаються сигнали a1, a2, a3, a4 і b1, b2, b3, b4, b5, b6, b7.

Блок комутації реалізовано на мультиплексорі, на адресні входи якого подається адреса, обрана мікропроцесором.

Блок корекції помилок виправляє одиночну помилку в отриманих даних шляхом додавання за модулем два з відповідним помилковим бітом. Це реалізується за допомогою двовходового елемента "дорівнює 1".

Блок перетворення коду перетворює отримані дані з біноміального коду в двійково-десятковий код. Це реалізується за допомогою дешифратора, виходи якого підключені до входів шифратора.

Блок синхронізації узгоджує роботу мікропроцесора та апаратної частини. В залежності від рівня зашумленості каналу, він підраховує синхроімпульси до 27 сигналів для I режиму (до 8 сигналів для II режиму) і подає процесору сигнал про готовність до зчитування даних. Це реалізується за допомогою двох лічильників з коефіцієнтами k1 = 27 і k2 = 8.

Блок порту індикатора, блок адресації і управління, блок прийому даних та блок передачі даних у зовнішній пристрій виконані у вигляді восьмирозрядних регістрів і забезпечують зв'язок апаратної частини системи з шиною даних мікропроцесора.

Генератор формує синхроімпульси для мікропроцесора з частотою f = 2 МГц і складається з логічних елементів.

Блок оперативної пам'яті є ОЗП, де зберігаються початкові дані, проміжні обчислення та результати.

Блок системних програм реалізований на основі ПЗП, де зберігається код програми для мікропроцесора, обсягом приблизно 1 Кбайт. Відповідно, шина адреси мікропроцесора повинна бути 10-розрядною.

4. РОЗРОБКА І РОЗРАХУНОК ПРИНЦИПОВОЇ ЕЛЕКТРИЧНИЇ СХЕМИ КОМБІНАТОРНОГО ПРИСТРОЮ ЗАХИСТУ ДАНИХ НА ОСНОВІ ПЛОЩИННИХ КОДІВ

4.1Вибір елементної бази

Вибір елементної бази – дуже важливий процес і для цього нам знадобиться порівняльна таблися 4.1.

Таблиця 4.1 – Параметри різних серій мікросхем.

Параметр	Серія					
	155	530	531	533	555	1533
Час затримки розповсюдження	10	3	3	9,5	9,5	4
Питома споживана потужність, *мВт / ле*	10	19	19	2	2	1
Коефіцієнт розгалуження по входу	10	10	10	20	20	40
Відхилення напруги живлення,%	+-5	+-5	+-5	+-5	+-5	+-10
Максимальный вихідний струм: "0"	16		20		8	4
Максимальний виходный струм: "1"	-0,4		(-1)		(-0,8)	(-0,4)

Логічні елементи складають основу комбінаторних схем. Для реалізації пристрою на основі площинних кодів необхідні наступні елементи:

Логічні вентилі (AND, OR, NOT, XOR): ці елементи забезпечують виконання основних логічних операцій, необхідних для формування та обробки кодових комбінацій.

Мультиплексори (MUX): ці пристрої дозволяють вибирати один з кількох вхідних сигналів для передачі на вихід, що корисно для маршрутизації даних та виконання умовних операцій.

Демультиплексори (DEMUX): вони використовуються для розподілу одного входу на кілька виходів, що дозволяє ефективно керувати розподілом даних.

Пам'ять для зберігання кодових слів та проміжних результатів обробки використовуються елементи пам'яті:

Регістри: регістри потрібні для тимчасового зберігання даних під час обробки, забезпечуючи швидкий доступ до них.

Постійна запам'ятовуюча пам'ять (ПЗП): ПЗП використовується для зберігання незмінних даних, таких як таблиці кодування та декодування.

Оперативна запам'ятовуюча пам'ять (ОЗП): ОЗП необхідна для динамічного зберігання даних, що змінюються під час роботи пристрою.

Процесори та контролери для виконання складних обчислень та керування процесом обробки даних можуть бути використані спеціалізовані процесори та контролери:

Цифрові сигнальні процесори (DSP): DSP оптимізовані для обробки великих обсягів даних у реальному часі, завдяки їх здатності виконувати математичні операції.

Програмовані логічні матриці (FPGA): FPGA дозволяють створювати високопродуктивні спеціалізовані обчислювальні схеми, які можна налаштувати для виконання конкретних завдань, пов'язаних із площинними кодами.

Логічні елементи

Для забезпечення високої продуктивності та надійності комбінаторного пристрою варто використовувати сучасні логічні елементи з низьким рівнем споживання енергії та високою швидкістю. Наприклад, елементи серії 74HC або 74HCT забезпечують високу швидкодію та сумісність з іншими компонентами.

Пам'ять

Для регістрів та ОЗП слід обирати компоненти з достатньою ємністю та швидким доступом до даних. Наприклад, регістри серії 74LS забезпечують необхідну швидкодію. Для ПЗП варто використовувати сучасні флеш-пам'яті або EEPROM з достатньою ємністю для зберігання таблиць кодів.

Процесори та контролери

Вибір між DSP та FPGA залежить від вимог до продуктивності та гнучкості системи. Якщо потрібна висока швидкодія та можливість паралельної обробки даних, краще обрати FPGA. Наприклад, FPGA від Xilinx або Altera забезпечують високий рівень інтеграції та гнучкості для налаштування під конкретні завдання.

4.2 Розрахунок і синтез принципової схеми блоків виявлення помилки пристрою захисту даних на основі площинних кодів

Комбінаторний пристрій захисту даних на основі площинних кодів є важливим елементом сучасних систем передачі та зберігання інформації, де забезпечення цілісності даних є критичною задачею. Площинні коди (також відомі як коди Пітерсона) використовуються для виявлення і виправлення помилок, які можуть виникнути під час передачі або зберігання інформації. Основною перевагою площинних кодів є їх здатність виявляти та виправляти помилки з високою ефективністю та мінімальними втратами продуктивності.

Для розрахунку і синтезу принципової схеми блоків виявлення помилки пристрою площинного кодування даних необхідно визначити ключові параметри коду, такі як довжина кодових слів, кількість контрольних символів та ступінь корекції помилок. Першим кроком є вибір поля Галуа, в якому будуть виконуватися всі операції кодування та декодування. Найчастіше використовуються поля Галуа GF(2^m), де m — це число, що визначає розмірність поля.

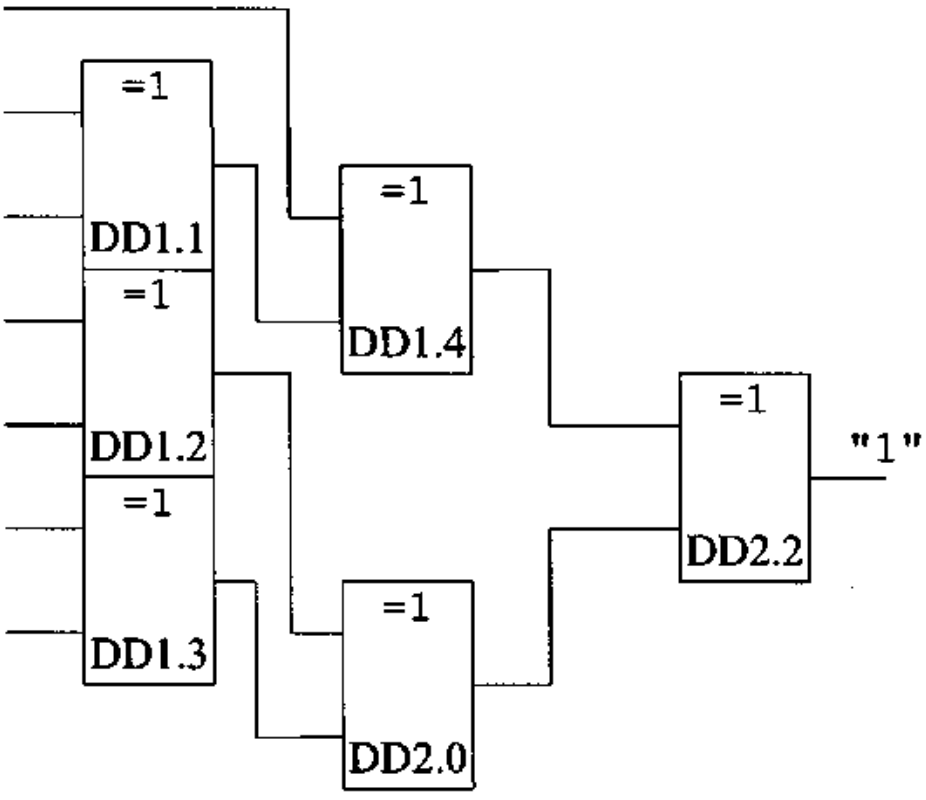

Рисунок 4.2 – Схема блоку виправлення помилок 1

Наступним етапом є побудова матриці перевірки коду (Н-матриці), яка використовується для генерації синдромів помилок. Кожне кодове слово можна подати у вигляді матриці, що складається з інформаційних та контрольних символів. Під час передачі даних за допомогою площинного коду, кожне прийняте слово підлягає перевірці на наявність помилок за допомогою множення прийнятого вектора на транспоновану матрицю перевірки. Якщо результатом цього множення є ненульовий вектор (синдром), це свідчить про наявність помилки.

Процес синтезу схем виявлення помилки включає розробку комбінаційних логічних схем, що реалізують множення та додавання в полі Галуа. Для цього використовуються спеціальні логічні елементи, які забезпечують виконання арифметичних операцій над полями GF(2^m). В результаті, схема виявлення помилок складається з багатьох паралельних блоків, кожен з яких відповідає за обробку певної частини кодового слова.

У підсумку, правильно розрахована та синтезована принципова схема блоків виявлення помилки забезпечує високу надійність передачі даних та мінімізує вплив помилок, що виникають під час передачі або зберігання. Це дозволяє використовувати комбінаторний пристрій захисту даних на основі площинних кодів у різноманітних застосуваннях, від телекомунікаційних систем до систем зберігання даних, забезпечуючи цілісність і достовірність інформації.

Для DD1-DD2 –в даній роботі використовується мікросхема серії К1533ЛП5.

На входи вузлів DD1-DD2 подаються разряди даних, описані формулами (3.1)-(3.7).

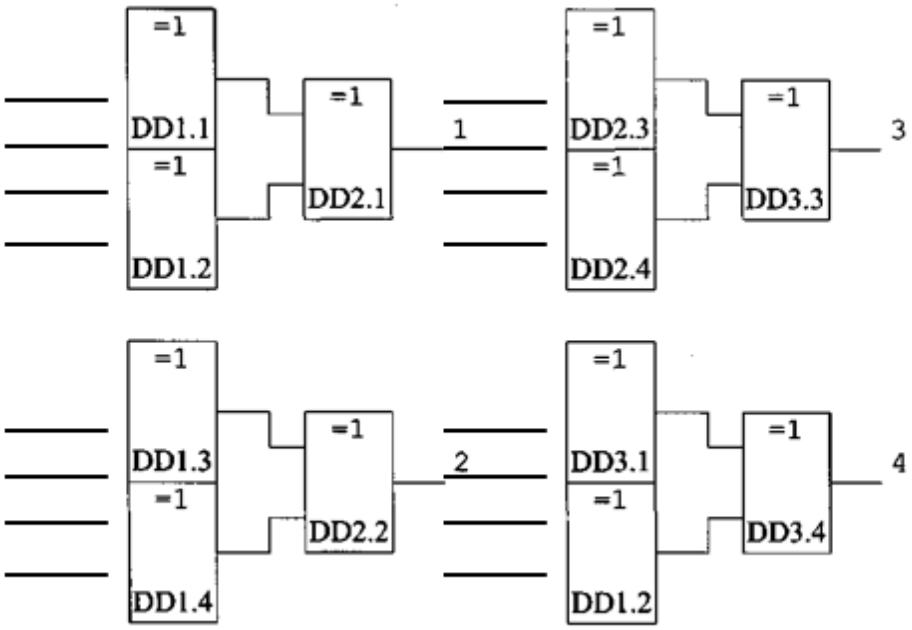

Рисунок 4.3– Схема блоку виправлення помилки 2

Для DD1-DD3 в роботі було використано мікросхему серії К1533ЛП5.

На входи елемнтів подаються розряди прийнятих даних, що описані формулами (3.8)-(3.11).

Розрахуємо споживану потужність (2), підставивши значення в формулу (4.3)

$$P_{сум.} = 14 \cdot 5 \cdot 5{,}9 = 413\ мВт.$$

$$T_з = 3 \cdot 17 = 51\ нс.$$

4.3 Розрахунок і синтез принципової схеми блоків декодування помилок пристрою захисту даних на основі площинних кодів

Блоки декодування помилок 1 та 2 визначають, в якому біті сталася помилка, і передають номер цього помилкового біта до блоку виправлення помилки. Для цього пристрою площинного кодування характерна здатність виправляти лише однократні помилки. Якщо дві з перевірок a1, a2, a3, a4 або дві з b1, b2, b3, b4, b5, b6, b7 мають значення 1, блоки визначають помилковий біт. Вони реалізуються за допомогою дешифраторів, на адресні входи яких подаються сигнали a1, a2, a3, a4 та b1, b2, b3, b4, b5, b6, b7.

Блок декодування помилок 1 складається з двох декодерів К1533ИД3 та К1533ИД7, на входи яких подаються вихідні сигнали від блоку виявлення помилки 1. Блок декодування помилок 2 зібраний на декодері К1533ИД3, на входи якого подаються сигнали 1-4 від блоку виявлення помилок 2. Робота блоку декодування

помилок 2 реалізується в режимі II і запускається мікропроцесором шляхом подачі логічного "0" на вхід ОЕ.

В даній роботі використовуються логічні мікросхеми серії: К1533ЛИ1; К1533ЛЕ1 (3 шт.); К1533ЛН1 (2 шт.).

$$P_{сум.2} = U\cdot(I_{ИД3}+I_{ИД7}+3\cdot I_{ЛЕ1} + I_{ЛИ1}+I_{ЛН1}), \quad (4.4)$$

$$P_{сум.2} = 5\cdot(15 + 10 + 3\cdot4 + 4 + 4{,}2) = 236\ мВт.$$

$$P_{сум.} = 236 + 5\cdot15 = 311\ мВт.$$

$$T_з = T_{зИД3}+T_{зЛИ1} \quad (4.5)$$

$$T_з = 36 + 14 = 50\ нс.$$

4.4 Розрахунок і синтез принципової схеми блоку виправлення помилок пристрою захисту даних на основі площинних кодів

Цей блок побудований на 20 двовходових елементах складання по модулю два типу К1533ЛП5. На один вхід подається біт отриманих даних, а на інший — біт, що сигналізує про наявність помилки в цьому розряді.

Рсум. = 5·5·5,9 = 147,5 мВт, Тз = 17 нс.

Блок виправлення помилок призначений для корекції тільки однократних помилок в отриманих даних. Корекція здійснюється додаванням по модулю два з відповідним помилковим бітом. Реалізується за допомогою двовходового елемента "дорівнює 1". У сучасних цифрових системах захист даних є критично важливим аспектом забезпечення надійності та безпеки інформації. Одним із ефективних методів забезпечення захисту даних є використання кодів виправлення помилок. В цій розповіді розглянемо розробку та синтез принципової схеми блоку виправлення помилок, який використовує площинні коди.

Площинні коди (або Product Codes) є різновидом блокових кодів, які складаються з двох або більше простих кодів, що накладаються один на одного, формуючи двовимірну структуру. Такий підхід дозволяє виправляти множинні помилки в кодових словах. Площинний код формується шляхом організації даних у двовимірну матрицю, де кожен рядок і кожен стовпчик кодується окремим кодом. Наприклад, використовуючи код Хемінга для рядків і стовпчиків, можна отримати потужний захист від помилок. Якщо розглянути матрицю даних розміром $n\times mn\times m$, де nn — кількість рядків, а mm — кількість стовпчиків, то кодування виконується наступним чином: спочатку кожен рядок матриці кодується кодом Хемінга, додаючи до кожного рядка перевірочні біти. Потім, після додавання перевірочних

бітів до кожного рядка, кожен стовпчик отриманої матриці знову кодується кодом Хемінга.

Для синтезу блоку виправлення помилок на основі площинних кодів необхідно розробити комбінаційний пристрій, що складається з двох основних частин: кодувального блоку, який здійснює кодування даних, та декодувального блоку, який здійснює виявлення та виправлення помилок. Кодувальний блок складається з двох підблоків: рядкового кодувальника, де кожен рядок вхідної матриці кодується за допомогою коду Хемінга, та стовпчикового кодувальника, де після кодування рядків кожен стовпчик нової матриці кодується знову. Принципова схема кодувального блоку може бути представлена у вигляді набору паралельних кодерів Хемінга, що працюють незалежно над рядками і стовпчиками.

Декодувальний блок складається з таких підблоків: рядковий декодувальник, що виявляє і виправляє помилки в кожному рядку, та стовпчиковий декодувальник, що після виправлення рядків здійснює виявлення та виправлення помилок у кожному стовпчику. Принципова схема декодувального блоку складається з детекторів помилок та коректорів для кожного рядка і стовпчика. Декодування відбувається у два етапи: спочатку по рядках, потім по стовпчиках.

Алгоритм роботи включає три основні етапи: кодування, передачу даних та декодування. На етапі кодування вхідні дані організовуються у матрицю, кожен рядок якої кодується кодом Хемінга. Після цього отримана матриця з перевірочними бітами по рядках кодується по стовпчиках кодом Хемінга. На етапі передачі дані передаються через канал зв’язку. На етапі декодування прийняті дані організовуються у матрицю, кожен рядок якої перевіряється на помилки та коригується, а після виправлення рядків кожен стовпчик перевіряється на помилки та коригується.

Використання площинних кодів у комбінаційних пристроях захисту даних дозволяє ефективно виявляти та виправляти помилки в цифрових системах. Розрахунок та синтез принципової схеми такого блоку виправлення помилок включає розробку кодувальних та декодувальних підблоків, які працюють з двовимірними структурами даних. Це забезпечує високу надійність та стійкість до помилок, що є критично важливим для сучасних інформаційних технологій.

4.5 Розрахунок і синтез принципової схеми блоку перетворення коду пристрою захисту даних на основі площинних кодів

Блок перетворення коду здійснює перетворення біноміального коду в двійково-десятковий формат та виявляє однократні і двократні помилки.

Таблиця 4.2 – Відповідність біноміального коду двійково-десятковому.

Десятковий код	Біноміальний код	Двійково-десятковий код
0	0000	0000
1	0010	0001
2	0011	0010
3	0100	0011
4	0101	0100
5	0110	0101
6	1000	0110
7	1001	0111
8	1010	1000
9	1100	1001

Щоб реалізувати блок перетворення ми використали мікросхеми з такими серіями:

DD1 – К1533ИД3;
DD2.1-DD2.2 – К1533ЛИ1;
DD2.3 – К1533ЛП5;
DD2.4 – К1533ЛА3;
DD4 – К1533ЛН1;
DD3 – К555ИВ1.

4.6 Висновки

На основі досліджених джерел літератури були проаналізовані методи створення комбінованого пристрою для захисту даних із використанням площинних кодів, а також визначені технічні вимоги до його проектування.

У цій бакалаврській кваліфікаційній роботі було розроблено алгоритм роботи комбінованого пристрою захисту даних, створено його структурну схему та розроблено і розраховано функціональні та принципові схеми всіх компонентів пристрою. Крім того, була представлена програма для мікропроцесора.

Робота досліджує режими функціонування комбінованого пристрою захисту даних у залежності від рівня шуму в каналі зв’язку, а також описує основні блоки, з яких складається пристрій. Мікропроцесорний модуль базується на процесорі Zilog Z80 та програмованому контролері паралельного введення-виведення Intel 8255.

НАУКОВІ ПРАЦІ СТУДЕНТА

Програма перетворення десяткових цілих чисел в двійкові

Борисенко О.А., професор; Кузьменко С.С., студент

Сумський державний університет, м. Суми, Україна

Пропонується програма перетворення десяткових чисел в двійкові написана на мові С++, яка використовує швидкодіючий алгоритм, в якому використовується діапазон значень чисел, що зберігається у вигляді масиву з 2N елементами де N = {1, 2, 3 ...R}.На вхід програми подається ціле невід'ємне значення числа, яке не більше за подвоєне останнє значення з діапазону чисел, що перетворюються. Потім запускається цикл який починає перевірку з кінця. Якщо вхідне число більше ніж 2N то у N-му розряді в двійковому числі буде представлена одиниця (1), в іншому випадку нуль (0). На кожній ітерації N буде зменшуватися на 1. В результаті після проходження всього циклу ми отримуємо двійкове число. Діапазон значень може змінюватися, від 0 до 4294967295,. Щоб його збільшити можна створити спеціальний клас чисел, який буде записувати великі числа в масив рядків. Нижче на рис.1 наведений програмний код алгоритму.

```
#include <iostream>

using namespace std;


int main()
{                       //   2^0   2^1   2^2   2^3   2^4   2^5   2^6   2^7   2^8   2^9   2^10
    unsigned int diapazon[] = {1,    2,    4,    8,    16,   32,   64,   128,  256,  512,  1024};
    const int amount = 11;

    unsigned int *result = new unsigned int[amount];
    int decNum;
    cout << "Enter decNimber < "<<diapazon[amount-1]*2 << endl;
    cin >> decNum;

    int poz = amount-1;

    for (int i = amount-1; i >=0;i--) {
        if (decNum >= diapazon[i]) {
            decNum -= diapazon[i];
            result[poz] = 1;
            poz--;
        }else {
            result[poz] = 0;
            poz--;
        }
    }

    for (int i = amount-1; i >=0;i--) {
        cout << result[i];
    }
}
```

Рисунок 1 – Програмний код

Structural characteristics of films MnTe and Cd1–xMnxTe for radiation detectors

Oleg Pysany PhD student; Kuzmenko Sergey student; Anatoliy Opanasyuk Professor

Sumy State University, Sumy, Ukraine

The MnTe compound and the Cd1–xMnxTe solid solution attract the increased attention of researchers due to the possibility of creating a number of electronic, magneto- and optoelectronic devices based on them. At the same time, recently, Cd1–xMnxTe is considered as an alternative to the compound Cd1 – xZnxTe for use in X-ray and gamma radiation detectors. Importantly, the band gap (Eg) and lattice constant (a) of the ternary semiconductor can be effectively controlled by varying the Mn concentration. This makes this material promising for creating heterojunctions with properties close to ideal. However, nowadays, the films of MnTe, Cd1–xMnxTe compounds have not been sufficiently studied due to the complexity of their production since the vapor pressure of the material components differs significantly. This determined the purpose of the work - to study the effect of substrate temperature on the composition and structural characteristics of films of solid solutions. Cd1–xMnxTe films were obtained on cleaned glass substrates in a VUP- 5M vacuum unit. Evaporation of the mixture of CdTe and MnTe charge was carried out by the quasi-closed volume method. The temperature of the substrate when applying the films varied in the interval Ts = (573-823) K. The temperature of the evaporator was Te = 1123 K. The condensation time of the films was t = (8-10) min. Structural studies of chalcogenide layers were performed on a DRON 4-07 X-ray diffractometer in Ni-filtered K□ radiation of a copper anode. Shooting was carried out in the range of 2θ angles from 200 to 800, where 2θ is the Bragg angle. It was established that the films obtained at substrate temperatures Ts < 773 K corresponded to a Cd1–xMnxTe solid solution with a cubic structure and different Mn content. The layers obtained at the substrate temperature Ts = 823 K consisted of hexagonal MnTe. At intermediate Ts, the condensates contained a mixture of two phases, MnTe and Cd1–xMnxTe. The conducted studies show that by changing the temperature of the substrate, it is possible to obtain both MnTe films and their solid solution.

ВИСНОВОК

Під час виконання бакалаврської кваліфікаційної роботи був створений комбінаторний пристрій захисту даних на основі площинних кодів, який відповідає вимогам проекту. Пристрій обробляє дані, закодовані завадостійким площинним кодом, що дозволяє виявляти та виправляти однократні помилки, а також виявляти помилки іншої кратності.

Для оптимізації роботи пристрою та його адаптації до умов передачі інформації були впроваджені два режими роботи: Режим I і Режим II. Вибір режиму залежить від рівня шуму в каналі зв'язку. Адаптивний пристрій аналізує рівень зашумленості та обирає відповідний режим роботи.

Пристрій призначений для передачі числових даних і забезпечує ефективний прийом і відображення інформації. Основні технічні характеристики системи такі:

1. Довжина лінії зв’язку не перевищує 1,3 км.
2. Швидкість передачі даних перевищує 32 Кбіт/сек.
3. Здатність виявляти всі одноразові та дворазові помилки в інформаційній послідовності.
4. Можливість виправляти всі одноразові помилки в інформаційній послідовності.
5. Довжина інформаційної послідовності в режимі I складає 40 біт (з них 20 контрольних).
6. Довжина інформаційної послідовності в режимі II складає 27 біт (з них 7 контрольних).
7. Час затримки декодування становить 791 наносекунду.
8. Кількість розрядів у дискретному напівпровідниковому семисегментному індикаторі – 5.
9. Обсяг архіву даних – 1 Кбіт.
10. Споживана потужність дорівнює 5 Вт.
11. Надійність не менше 4500 годин.

СПИСОК ЛІТЕРАТУРИ

1 Золотарьов В.В. Перешкодостійке кодування. Методи і алгоритми / В.В. Золотарьов, Г.В. Овечкін – Довідникове видання, 2021.- 25 с.

2 Винберг Е.Б. Дивовижні арифметичні властивості біноміальних коефіцієнтів. Математичне просвітництво / Е.Б. Винберг — Вид. 12, 2020. — 33–42 с.

3 Гадзиковський В.І. Цифрова обробка сигналів. – М.:Солон, 2019.

4 Пат. 31749 МПК (2006) G01S 13/00. Спосіб ідентифікації об’єктів. / Обод І. І., Ключкевич Є. О., Ярова А. В. – № u200712210; заявл. 05.11.2019; опубл. 25.04.2020, Бюл. № 8, 2008 р. – 4 с.

5 Анісімов А.В. Інформаційні системи та бази даних: Навчальний посібник для студентів факультету комп’ютерних наук та кібернетики / А.В. Анісімов, П.П. Кулябко − Київ. – 2019. – 110 с.

6 Вишенський В.А. Комбінаторика: перші кроки / В.А Вишенський, М.О. Перестюк —Кам'янець-Подільський: Аксіома, 2020. — 324 с.

7 Грахольська, А.В. Пристрій площинного кодування даних [Текст]: робота на здобуття кваліфікаційного рівня бакалавра; спец.: 171 – електроніка / А.В. Грахольська; наук. керівник І.А. Кулик. – Суми: СумДУ, 2020.– 56 с.

8 Жураковський, Б.Ю., Довженко, Н.М. (2020). Сфери застосування двовимірних штрихових кодів. Системи управління, навігації та зв’язку, (32 (2)), 83-88.

9 Ako, M. A., Hikmat, R. A. (2019). Evaluating the Use of Quick Response (QR) Code at Sulaimani University Libraries. ISSN: 2277 128X.

10 Chelabi M. A., Basova Y., Hamidou M. K., Dobrotvorskiy S. (2021). Analysis of the three-dimensional accelerating flow in a mixed turbine rotor. Journal of Engineering Sciences, Vol. 8(2), pp. D1-D7, doi: 10.21272/jes.2021.8(2).d2

11 Les entrepeises francaises [Текст] = Підприємства Франції : навч. посіб. / уклад. Ю. А. Скарлупіна. - Суми : ДВНЗ "УАБС НБУ", 2019. - 111 с.