**ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ**

**Актуальність.** Зі зростанням використання електроніки і комп'ютерів, зростає потреба у швидкій і надійної передачі інформації по каналах зв'язку. У будь-якому каналі зв'язку присутні шуми - сигнали, які можуть спотворювати інформацію, що передається. З цими спотвореннями можна боротися, перетворюючи інформацію, що передається за допомогою коду, який буде виявляти, і виправляти помилки. В основі роботи всіх кодів лежить модифікування вихідних даних шляхом додавання деякої надлишкової інформації, яка дозволяє виявляти і виправляти помилки, які могли виникнути при передачі кодованої інформації по зашумленими каналу зв'язку.

У 1969 році, за допомогою штучних супутників Mariner 6 і Mariner 7, було отримано близько двохсот фотографій Марса. Кожна фотографія складалася з 658240 восьми бітних пікселів. Таким чином, для кожної фотографії було потрібно близько 5-ти мільйонів біт інформації. Ці біти були кодовані кодом, що виправляють помилки, і передані зі швидкістю 16200 біт в секунду на Землю, де вони були успішно декодувати.

Історія кодування, що контролює помилки, почалася в 1948р. публікацією знаменитої статті Клода Шенона. Шенон показав, що з кожним каналом пов'язано вимірюється в бітах в секунду і зване пропускною спроможністю каналу число C, що має таке значення. Якщо необхідна від системи зв'язку швидкість передачі інформації R (яка вимірюється в бітах секунду) менше C, то, використовуючи коди, які контролюють помилки, для даного каналу можна побудувати таку систему зв'язку, що ймовірність помилки на виході буде як завгодно мала.

У п'ятдесяті роки багато зусиль було витрачено на спроби побудови в явному вигляді класів кодів, що дозволяють отримати обіцяну як завгодно малу ймовірність помилки, але результати були мізерними. У наступному десятилітті цій захоплюючій завдання приділялося менше уваги, замість цього дослідники кодів зробили атаку за кількома основними напрямками.

Один з напрямків носило чисто алгебраїчний характер і переважно розглядало блокові коди. Перші блокові коди були введені в 1950 р., коли Хеммінга описав клас блокових кодів, що виправляють поодинокі помилки. Незважаючи на посилені дослідження, до кінця п'ятдесятих років не було побудовано кращого класу кодів. Основний зсув стався, коли Боуз і Рой-Чоудхурі в 1960 р. і Хоквінгем в 1959 р. знайшли великий клас кодів, що виправляють кратні помилки (коди БЧХ).

Але клас кодів що виправляють кратні помилки не є досить потужним для виправлення пакетних помилок, що часто виникають у каналах зв’язку, тому є виправданим рішення розглядати код Ріда-Соломона для проектування програмного комплексу, а методом проектування обрати розробку програми що працюватиме по алгоритму Ріда-Соломона.

**Зв'язок роботи з науковими програмами, планами, темами.**

Кваліфікаційна робота виконана в рамках держбюджетних НДР: 388-ДБ07 «Розробка та впровадження новітніх технологій стиску та захисту сигналів та зображень в радіоелектронних системах і комплексах» (№0107U002666), 669-ДБ10 «Розроблення та впровадження програмних засобів захисту інформації від несанкціонованого доступу в електронних системах документообігу у вищих навальних закладах України» (№0110U000222).

**Мета і задачі дослідження.** Метою роботи є розробка програмної частини для цифрового апаратно-програмного комплексу завадостійкої системи прийомо-передачі криптографічних даних що дасть змогу, при впровадженні даної системи, отримати досить стійку систему захищену як від завад та помилок у обмінюваній інформації але й забезпечити конфіденційність цієї інформації.

**Завдання роботи.** Завданням даної роботи є розробка цифрового програмно-апаратного комплексу завадостійкої системи прийомо-передачі криптографічних даних а саме алгоритм завадостійкого кодування-декодування.

**Об’єкт дослідження.** Об'єктом роботи є процес побудови завадостійкого кодування по алгоритму Ріда-Соломона з елементами RAID системи та криптографічною складовою.

**Предмет дослідження.** Предметом дослідження є різні методи завадостійкого кодування інформації з єлементами криптографічного захисту. Під час дослідження методів завадостійкого кодування використовувалися методи кодування за допомогою алгоритму Ріда-Соломона, RAID метод кодування та метод CRC кодів. Було досліджено методики блокового, циклічного кодування, кодів Хеммінга та БЧХ коди.

**Методи дослідження.** Для вирішення даного завдання було використано наступні методи:

1. Метод матричних обчислень в RAID-подібних системах.
2. Метод розрахунку матриці Вандермонда.
3. Пошуку оберненої матриці методом Жорданових винятків.
4. Метод оптимізації матричних обчислень.
5. У елементах криптографічного захисту використовувалися методи стохастичної кругової прокрутки блоку, ковзного кодування, нелінійної заміни байтів та стохастичної перестановки.

**Наукова новизна.** Наукова новизна полягає в способі захисту інформації від помилок та завад, полягає у поєднанні досить потужних методик (RAID системи, алгоритм Ріда-Соломона) боротьби з цими проблемами, що є до речі досить новим підходом до вирішення цих проблем.

**Практичне значення отриманих результатів.** Практичне значення отриманих результатів можна виразити через визначення: комп'ютерний захист - це постійна боротьба з «дурістю» користувачів й інтелектом хакерів. Навіть хакери найчастіше використають саме некомпетентність і недбалість обслуговуючого персоналу й саме останнім можна вважати головною загрозою безпеки. Одна із проблем подібного роду - так звані слабкі паролі. Користувачі для кращого запам'ятовування вибирають паролі, що легко вгадати. Причому проконтролювати складність пароля неможливо. Інша проблема - зневага вимогами безпеки. Наприклад, небезпечно використати неперевірене програмне забезпечення. Звичайно користувач сам "запрошує" у систему віруси й "троянських коней". Крім того, багато неприємностей може принести неправильно набрана команда.

Кращий захист від нападу - не допускати його. Навчання користувачів правилам безпеки мережі може запобігти нападам. Захист інформації містить у собі крім технічних мір ще й навчання або правильний підбор обслуговуючого персоналу.

Захист інформації не обмежується технічними методами. Проблема є значно ширшою. Основний недолік захисту - люди, і тому надійність системи безпеки залежить в основному від відношення до неї. Крім цього, захист повинен постійно вдосконалюватися разом з розвитком комп'ютерної мережі.

У цей час узагальнена теорія безпеки інформації поки не створена. Застосовувані на практиці підходи й засоби нерідко страждають істотними недоліками й не мають оголошену надійність. Тому необхідно володіти достатньою підготовкою й кваліфіковано орієнтуватися у всьому спектрі питань забезпечення інформаційної безпеки, розуміючи їх комплексний і взаємообумовлений характер

А захист від помилок – це боротьба з природними впливами, що загрожують інформації у будь-яких методах її зберігання та обміну оскільки «ідеального» пристрою не існує, а тому потрібно розробляти системи та алгоритми які будуть виправляти цей недолік апаратних комплексів.

**Особистий внесок здобувача.**

В роботі [1] удосконалено алгоритм установки ключів, що дозволяє використовувати даний алгоритм у незахищених комп’ютерних мережах оскільки забезпечує захист від завад при передачі ключа по каналах зв’язку. В роботі [3] розроблено алгоритм синтезу утворюючих та перевірочних матриць для (*n, k*) – кодів Хемінга, а також вирішена задача локалізації та усунення одиничної помилки у любому розряді коду, причому розроблені алгоритми допускають досить просту як програмну так і апаратну реалізацію.

**Апробація результатів роботи.** Апробація отриманих результатів була проведена під час багатьох виставок та конференцій, а саме конференції «Політ» за 2007, 2008 роки та в цих же роках у виставках студентських талантів інституту ІЕСУ НАУ. Також основні положення роботи доповідались на науково-практичній конференції «Захист в інформаційно-комунікаційних системах» (НАУ, травень 2009) та студентській науково-технічній конференції ІНТ (НАУ, листопад 2009).

**Публікації.** За темою кваліфікаційної роботи опубліковано 3 друковані праці (дві статті та одні тези доповідей на конференціях).

**Структура кваліфікаційної роботи.** Робота складається із вступу, списку скорочень, трьох розділів, висновків. Обсяг роботи складає 104 сторінок, робота містить 22 рисунки, 19 таблиць, 52 використаних джерел, 6 додатків.

**ОСНОВНИЙ ЗМІСТ РОБОТИ**

Увступірозкриті сутність і стан наукової проблеми, обґрунтована актуальність, сформульовані мета й завдання досліджень, а також визначена новизна й практична цінність отриманих результатів. Вказані результати апробації й публікації.

У першому розділі розглянуті основи теорії секретних систем та основні поняття цієї теорії. Проаналізовані сучасні методи криптографічного захисту інформації, описані загальні відомості, проведений аналіз цих методів та методів завадостійкого кодування та алгоритмів, що виявляють та виправляють помилки.

Серед яких такі типи кодів:

* Блокові коди
* Лінійні коди загального вигляду (Коди Хеммінга)
* Лінійні циклічні коди
* Коди CRC
* Коди БЧХ
* Коди корекції помилок Ріда - Соломона
* Сверточні коди

Розглянута класифікація та основні вимоги, які пред’являються до сучасних криптосистем.

Також був проведений аналіз існуючих методів завадостійкого кодування та алгоритмів, що виявляють та виправляють помилки. Виходячи з того що алгоритм Ріда-Соломона якнайкраще підходить для виправлення пакетних помилок у каналах зв’язку тому саме його покладено у основу роботи. Окрім того для підвищення завадостійких властивостей проектуємої системи було вирішено покласти в основу алгоритму кодування RAID принцип кодування.

У другому розділі наведені та розглянуті математичні основи застосованих алгоритмів завадостійкого кодування та елементів криптографічного захисту. Наведено процеси матричних обчислень, як елементу RAID-подібного кодування, суть коду Ріда-Соломона та схема застосованого RSB алгоритму. А саме перш ніж описувати процес обчислення томів для відновлення на основі даних основних томів, розглядається матриця Вандермонда. Кожен елемент такої матриці може бути обчислений за такою формулою:

F(i, j) = i j-1;

де i - номер рядка, в якій знаходиться обчислюваний елемент; j - номер стовпця, в якому знаходиться обчислюваний елемент.

Головною властивістю матриці, що заповнюється таким чином, є те, що вона ніколи не є виродження, тобто завжди має зворотну матрицю. Якщо матрицю Вандермонда помножити на вектор-стовпець зрізу даних основних томів, то результатом операції стане вектор-стовпець зрізу даних томів для відновлення.

Далі усі матричні операції RAID-систем можуть бути застосовні як для звичайної арифметики і при необхідності, кількість рядків в матриці Вандермонда може перевищувати кількість стовпців, що буде означати кодування з збитковістю більше 100%. Але якщо всі обчислення проводити у звичайних числах, то ніяких проблем з матричної арифметикою не виникає. Однак, в реальних системах, зважаючи на величезних чисел, що виникають у процесі роботи з матрицями, використовується спеціальна арифметика полів Галуа. По-суті вона працює не з самими числами, а з їх залишками (в рамках поля заданого розміру).

Матричні обчислення - основна складова завантаження центрального процесора при кодуванні або декодування. При збільшенні матриці на вектор з використанням арифметики поля Галуа досить розумно не обчислювати дискретний логарифм елементів матриці кожного разу, коли він потрібен, а використовувати заздалегідь про логарифмовану матрицю (втім, як і вхідний вектор). Операція XOR (додавання або віднімання в полях Галуа) використовується в оптимізованому варіанті безпосередньо, а не через клас GF16 з метою збільшення швидкості. Для того, щоб уникнути використання логічних умов в операції множення (адже логарифм нуля не існує, і потрібні перевірки) можна надійти в такий спосіб - використовувати таблицю експонент учетверенного розміру. При цьому перша її половина - це сама таблиця експонент з копією (щоб не приводити результат суми до розміру поля), а решта заповнена нулями. При цьому логарифм нуля покладається таким, щоб сума логарифмів завжди вказувала у частину таблиці експонент, заповнену нулями, якщо хоча б один з співмножників дорівнює нулю.

Існує ще один досить важливий момент в оптимізації: тип масиву матриці кодування. Будь-який двовимірний масив може бути легко і просто замінено на одновимірний, з використанням складного індексу за схемою:

array[i][j] → array[(i \* кількість стовпців) + j];

Це дає приблизно 1,5 .. 2 - разовий виграш у швидкодії.

Також у цьому розділі подано опис нового криптографічного алгоритму RSB. Абревіатура RSB походить від ключових слів Rоund, Step, Blok, підкреслюючи тим самим, що основними для крипто-алгоритму є раундові перетворення, розбиті на певну кількість кроків, а дія алгоритму здійснюється над блоками відкритого або закритого текстів. Це ітераційний блочний шифр, який дає унікальну можливість по зміні як розмірів секретних ключів, так і числа кроків (раундів) шифрування [14-15]. Відмінна особливість алгоритму полягає у використанні функції шифрування типу ковзного кодування, яка забезпечує не лише глибоке перемішування відкритого тексту, але і бере участь у формуванні блокового раундового ключа (визначення дається нижче) для чергового блоку, що шифрується. Тим самим всі перетворення, що виконуються крипто-алгоритмом, стають залежними не тільки від секретного ключа, а й від даних, що шифруються, тобто відносяться до класу «керованих операцій крипто-перетворень», або «керованих крипто-примітивів».

Алгоритм передбачає три варіанти довжини блоку (для застосування в різних класах безпеки) і змінну довжину ключа шифрування для кожного варіанта довжини блоку. Структура RSB алгоритму ідентична для різних розмірів блоку, що дорівнює 128 *n* , де *n* коефіцієнт кратності довжини блоку, який може приймати значення 1, 2 або 3, тобто алгоритм підтримує блоки довжиною 128, 256 і 512 біт.

Узагальнена структурна схема RSB алгоритму наведена на рис. 1.

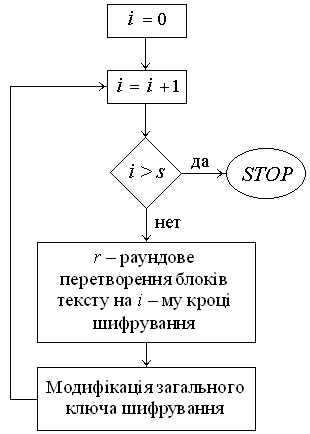


Рис. 1. Узагальнена структурна схема RSB алгоритму

Структурна схема раундового перетворення блоку, що шифрується, в загальному вигляді представлена на рис. 2.

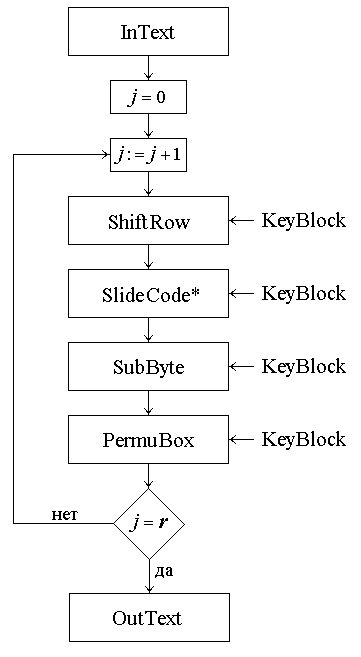


Рис. 2. Структурна схема раундового перетворення

Опис алгоритму наводиться в основному для довжини блоку 256 біт і відзначаються особливості реалізації шифру для інших розмірів блоку.

* Основні параметри RSB алгоритму:
* Размір блоку: *N* = 128, 256 або 512 біт.
* Довжина раундового ключа - 32 біта.
* Довжина загального (крокового) ключа: *r\*32*, *r=1,2,..*
* Число кроків шифрування: *s=1,2,..*
* Загальне число раундів шифрування: *r\*s*.
* Розмір елементів ковзного кодування - 32 біта.
* Розмір елементів нелінійної заміни: 8 біт.

Схеми базових раундовий ключів на етапі за шифрування та розшифрування показані на рис. 3 та 4.

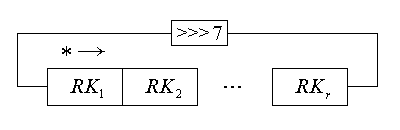


Рис. 3. Схема модифікації базових раундовий ключів на етапі за шифрування

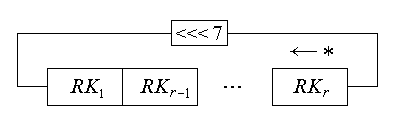


Рис. 4. Схема модифікації базових раундовий ключів на етапі розшифрування

У третьому розділі проведено проектування програмного комплексу завадостійкої та криптографічно захищеної системи для роботи в каналах прийомо-передачі даних. Було зроблено дві програми: «RS кодер-декодер» (рис. 5) та «RSB32 2.0» (рис. 6).

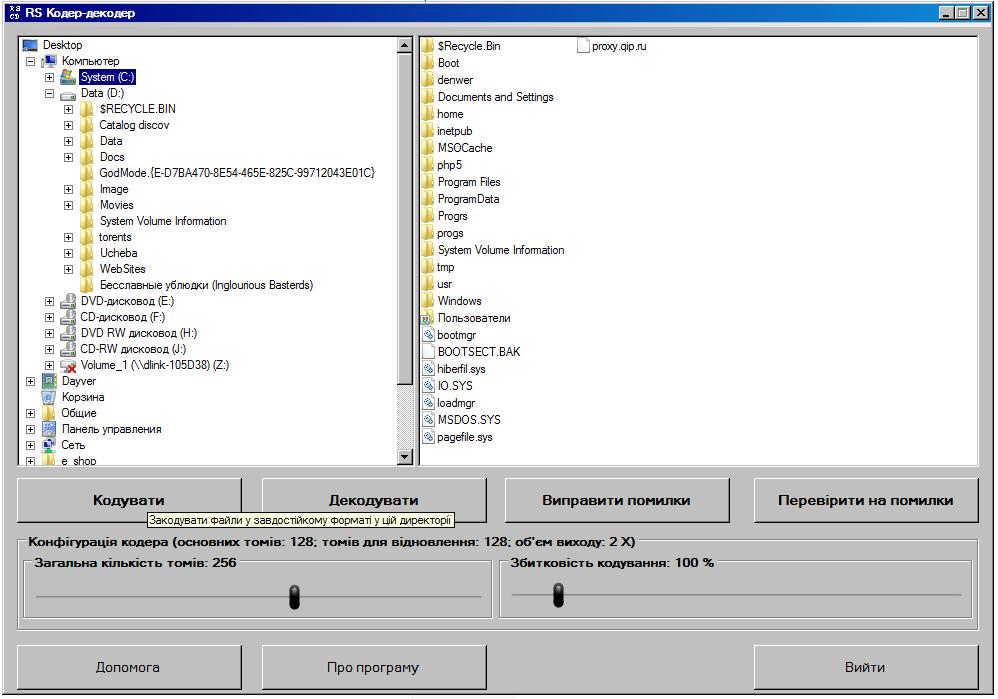


Рис. 5. Зовнішній вигляд головного вікна програми «RS Кодер-декодер»

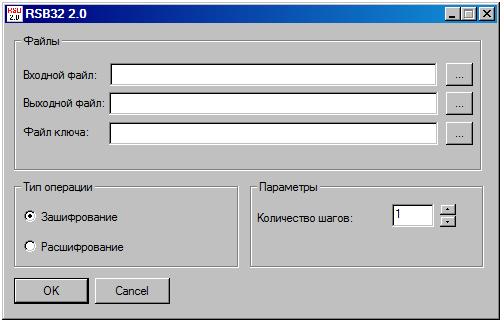
****

Рис. 6. Інтерфейс головного вікна програми «RSB32 2.0»

У загальному вигляді структурна схема програми «RS кодер-декодер» показана на рис. 7., а пояснення до неї у табл. 1.

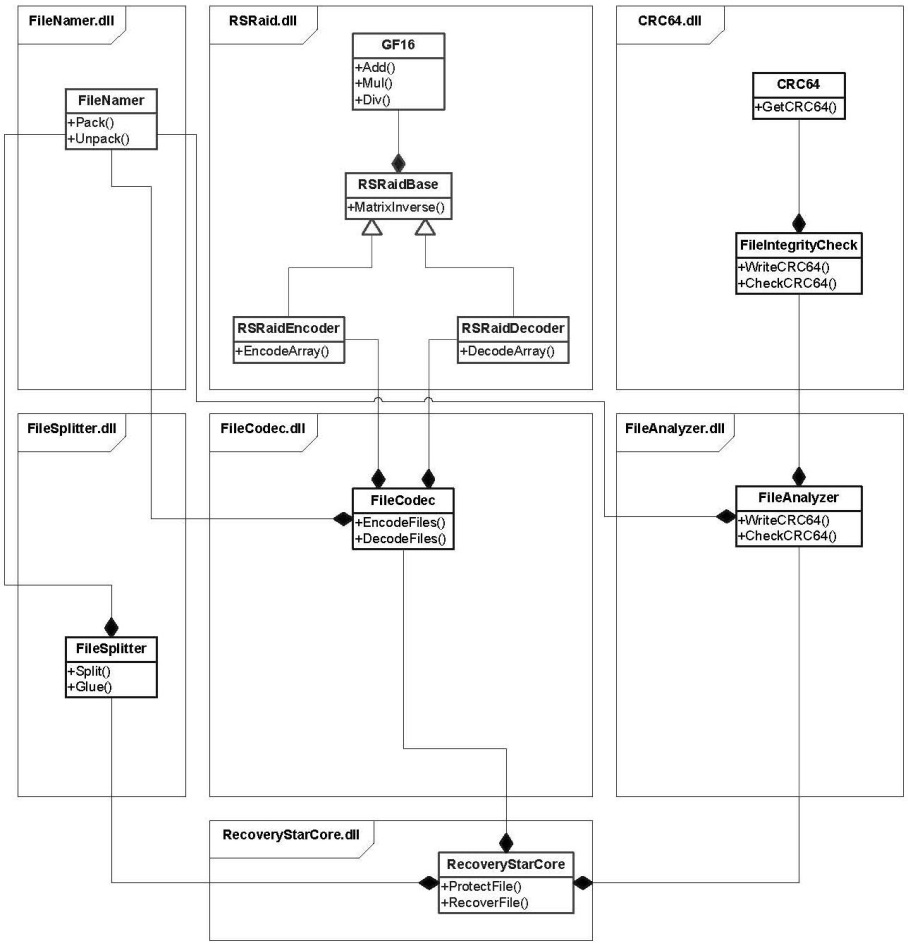
****

Рис. 7. Діаграма класів ядра системи з розділенням на інкапсулюючі модулі

Таблиця 1.

Призначення класів, відображених на рис. 7

|  |  |
| --- | --- |
| Найменування класу | Призначення класу |
| CRC64 | Розрахунок і перевірка сигнатури цілісності CRC-64, записуваної в кінець файлу. |
| FileIntegrityCheck | Розрахунок і перевірка сигнатур цілісності набору файлів, що породжується розбиванням вихідного на фрагменти-томи. |
| GF16 | Реалізація арифметики поля Галуа GF (2 ^ 16). |
| RSRaidBase | Базовий клас RAID-подібного кодера Ріда-Соломона. |
| RSRaidEncoder | RAID-подібний кодер Ріда-Соломона. |
| RSRaidDecoder | RAID-подібний декодер Ріда-Соломона. |
| FileCodec | Кодер набору файлів (використовує RSRaidEncoder / RSRaidDecoder). |
| FileNamer | Пакувальник / розпакувальник імені файлу в префіксний формат. |
| FileSplitter | Розбиття / склеювання файлу на фрагменти. |
| RecoveryStarCore | Ядро системи, що управляє перерахованими вище модулями. |

Програма «RS кодер-декодер» (завадостійка компонента розроблюваної системи) може використовуватися як окремо від програми «RSB32 2.0» так і разом та забезпечувати завадостійке кодування інформації для подальшої передачі її в по канал зв’язку. Програма «RSB32 2.0» (криптографічна складова системи передачі інформації) також в свою чергу може використовуватися як окремо так а разом з програмою «RS кодер-декодер» та забезпечувати шифрування\розшифруваня конфіденційної інформації для подальшої передачі по незахищеним каналам зв’язку. А також слід зазначити що, спроектована програма «RSB32 2.0» може виконувати окремо дві дії, а саме - процес кодування та процес декодування. Інтерфейс програм «RSB32 2.0» та «RS кодер-декодер» досить простий та має лише найголовніші органи управління тому це дозволяє охопити досить широкий круг користувачів серед яких можуть буті як досвідчені спеціалісти так і користувачі з малим рівнем володіння комп’ютерною технікою.

**ВИСНОВКИ**

Захист від помилок – це боротьба з природними впливами, що загрожують інформації у будь-яких методах її зберігання та обміну оскільки «ідеального» пристрою не існує, а тому потрібно розробляти системи та алгоритми які будуть виправляти цей недолік апаратних комплексів.

В даній роботі освітлена тема завадостійкого кодування, проаналізовані алгоритми існуючих завадостійких кодів, а також розроблені програми «RS кодер-декодер» та «RSB32 2.0», чим вирішено такі цілі:

* Запропоновано більш потужний алгоритм виправлення помилок у блоках даних в основі якого лежить сучасний код Ріда-Соломона
* Розроблено комплекс алгоритмів, що дозволяє не лише передавати конфіденційну інформацію по каналах передачі даних в яких можливість пошкодження переданих пакетів досить велика але разом з тим отримувати її без помилковою, а й не хвилюватися про її криптографічну незахищеність.
* Проведені оцінка криптостійкості даного алгоритму за допомогою методів статистичного крипто аналізу;
* Розроблена програмна реалізація модифікованого алгоритму кодування для виправлення помилок у інформації що підлягає передачі по зашумленим каналам передачі даних.
* Розроблена програмна реалізація криптографічного RSB алгоритму захисту інформації від несанкціонованого доступу.

Розглядаючи роботу в цілому, можна зробити такий висновок, що були розглянуті та висвітлені у повному обсязі всі поставлені задачі. Розроблені, спроектовані та протестовані програми для завадостійкого та криптографічно захищеного апаратно-програмного комплексу прийомо-передачі даних який функціонально вирішуватиме задачі захисту від завад та несанкціонованого доступу інформації, що передаватиметься цим комплексом.

**СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ**

* 1. Білецький А.Я., Стеценко Д.А., Ткаченко П.Л., Бабич В.В. MARK алгоритм установки ключів шифрування. Защита информации: сборник научных трудов НАУ. – Киев: НАУ, 2009. – с. 43-46.
  2. Білецький А.Я., Стеценко Д.А., Ткаченко П.Л., Бабич В.В. Система розповсюдження ключів шифрування. Захист в інформаційно-комунікаційних системах: тези науково-практичної конференції. – Київ: НАУ, 2009 – с.39-40.
  3. Білецький А.Я., Ткаченко П.Л. Неформальний синтез кодів Хемінга. Електроніка та системи управління – Київ: НАУ, 1(23)-2010, с. 12-19.

**АНОТАЦІЯ**

**Ткаченко П.Л. Синтез і аналіз ефективності модифікованого алгоритму завадостійкого коду Ріда-Соломона. – Рукопис.**

Кваліфікаційна робота на здобуття наукового ступеня кандидата технічних наук НАУ за спеціальністю 05.13.21 – Системи захисту інформації. – Національний авіаційний університет, м. Київ, 2010 р.

Дана робота включає опис сучасних методів завадостійкого кодування та криптографічного захисту інформації. В цій роботі запропонований та розроблений модифікований алгоритм Ріда-

Соломона завадостійкого кодування даних, який використовує принцип RAID-подібних систем та CRC кодів, та поєднанні з RSB алгоритмом криптографічного захисту. Запропоновано модифікацію алгоритму Ріда-Соломона з матричною оптимізацією та захистом на основі криптографічних примітивів, для шифрування даних та подальшим безпечним розповсюдження по незахищеним каналам зв’язку. Проведений статистичний криптоаналіз запропонованого алгоритму. Висновки сформульовані за результатами дослідів та практичних рекомендацій.

Ключові слова: Алгоритм Ріда-Соломона, RAID системи, CRC код, RSB алгоритм, матрична оптимізація, криптографічні примітиви.

**АННОТАЦИЯ**

**Ткаченко П.Л. Синтез и анализ эффективности модифицированного алгоритма помехоустойчивого кода Рида-Соломона. - Рукопись.**

Квалификационная работа на соискание ученой степени кандидата технических наук НАУ по специальности 05.13.21 - Системы защиты информации. - Национальный авиационный университет, г. Киев, 2010 г.

Данная работа включает описание современных методов помехоустойчивого кодирования и криптографической защиты информации. В этой работе предложен и разработан модифицированный алгоритм Рида-Соломона помехоустойчивого кодирования данных, который использует принцип RAID-подобных систем и CRC кодов и сочетается с RSB алгоритмом криптографической защиты. Предложена модификация алгоритма Рида-Соломона с матричной оптимизацией и защитой на основе криптографических примитивов, для шифрования данных и последующим безопасным распространения по незащищенным каналам связи. Проведенный статистический криптоанализ предложенного алгоритма. Выводы сформулированы по результатам исследований и практических рекомендаций.

Ключевые слова: Алгоритм Рида-Соломона, RAID системы, CRC код, RSB алгоритм, матричная оптимизация, криптографические примитива.

**ANNOTATION**

**Tkachenko PL Synthesis and analysis of the effectiveness of the modified algorithm for error-correcting Reed-Solomon. - Manuscript.**

Thesis for candidate’s degree in technical sciences NAU in specialty 05.13.21 - Information security systems. - National Aviation University, Kiev, 2010.

This work includes a description of modern methods of error-correcting coding and cryptographic protection of information. In this paper we proposed and developed a modified algorithm for Reed-Solomon error-correcting coding of data, which uses the principle of RAID-like systems and CRC codes and combined with the RSB algorithm for cryptographic protection. A modified algorithm for Reed-Solomon with matrix optimization and protection based on the cryptographic primitive for data encryption and subsequent safe distribution over unsecured communication channels. There was made statistical cryptanalysis of the proposed algorithm. The conclusions are formulated based on research findings and practical recommendations.

Keywords: Reed-Solomon algorithm, RAID Systems, CRC code, RSB algorithm, matrix optimization, cryptographic primitives.