МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КРИЛОВА Вікторія Анатоліївна

УДК 004.056.5

РОЗРОБКА УНІФІКОВАНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРИЗОВАНИХ ІНТЕГРОВАНИХ СИСТЕМАХ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2014

Дисертацією є рукопис.

Робота виконана на кафедрі автоматики та управління в технічних системах Національного технічного університету «Харківський політехнічний інститут» Міністерства освіти і науки України.

Науковий керівник кандидат технічних наук, доцент
Горбачов Віктор Васильович,
Національний технічний університет «Харківський політехнічний інститут»,
доцент кафедри автоматики та управління в технічних системах

Офіційні опоненти: доктор технічних наук, професор
Фурман Ілля Олександрович,
Харківський національний технічний університет сільського господарства ім. Петра Василенка,
завідувач кафедри автоматизації та комп'ютерно-інтегрованих технологій

доктор технічних наук, доцент
Мірошник Марина Анатоліївна,
Українська державна академія залізничного транспорту,
доцент кафедри спеціалізованих комп'ютерних систем

Захист відбудеться "27" січня 2014 р. о 15^{30} годині на засіданні спеціалізованої вченої ради Д 64.050.14 в Національному технічному університеті «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Фрунзе, 21.

З дисертацією можна ознайомитися у бібліотеці Національного технічного університету «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Фрунзе, 21.

Автореферат розісланий "24" грудня 2013 року.

Вчений секретар
спеціалізованої вченої ради І. Г. Ліберг

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Розвиток і впровадження автоматизованих систем управління є необхідною умовою науково-технічного прогресу суспільства. Стрімке зростання інформаційних технологій, широке розповсюдження комп'ютеризованих систем та мереж обумовили необхідність створення засобів комунікації, здатних забезпечити швидку та достовірну передачу інформації. Питання обробки, захисту і передачі інформації є важливим як для бізнесу, медицини, приватних осіб, так й для військового сектору. Зростаючи вимоги до оперативності та своєчасності передачі повідомлень в спеціалізованих комп'ютеризованих системах і мережах управління, у поєднанні з жорсткими вимогами до ймовірнісних характеристик доведення інформації, роблять проблему вдосконалення та розробки апаратно-програмних засобів обробки, захисту і передачі інформації особливо актуальною. Одним із шляхів вирішення проблеми підвищення ефективності захисту і передачі даних є розробка і застосування уніфікованих адаптивних методів кодування.

За останні десятиріччя з'явилось багато робіт, присвячених побудові алгоритмів і протоколів передачі інформації в комп'ютеризованих інтегрованих системах, а також апаратної та програмної реалізації адаптивних методів захисту інформації. В цьому напрямі особливої уваги заслуговують монографії та праці наукових шкіл У. Петерсона, Е.Р. Берлекемпа, Р. Блейхута, В.В. Зяблова, В.Б. Афанасьєва, В.В. Квашеникова, M. Bossert, R. Jordan, R. Johannesson і багатьох інших вчених.

Процедура вибору завадостійкого коду, а також параметрів кодера для відповідного інформаційного каналу здійснюється на етапі розробки і проектування комп'ютерних компонентів системи, виходячи з передбачуваних характеристик каналу. Доцільним є перехід до адаптивних систем захисту інформації, у яких коди здатні змінювати свої параметри на стадії експлуатації комп'ютеризованої системи, забезпечуючи при цьому задану ймовірність доведення повідомлення за мінімальної надмірності завадостійкого коду. При використанні адаптивних методів захисту інформації в цифрових інформаційних мережах важливим є питання вибору сигнально-кодової конструкції, що має розширений енергетичний спектр, для підвищення завадостійкості за умов завад, зосереджених за спектром.

У зв'язку з цим розробка та вдосконалення апаратно-програмного забезпечення обробки, захисту і передачі даних в комп'ютеризованих системах та мережах з уніфікованими методами захисту інформації, які виконують процедуру адаптації та відповідають вимогам мінімальних апаратних та енергетичних затрат, є актуальною науково-технічною проблемою, яка визначила напрямок дисертаційної роботи.

Зв'язок роботи з науковими планами, програмами, темами. Розробка основних положень роботи здійснювалася на кафедрі автоматики та управління в технічних системах НТУ «ХПІ» відповідно до держбюджетної науково-

дослідної роботи МОН України «Розробка програмних та апаратних засобів моделювання та відображення динамічних об’єктів» (Д.Р. № 0113U000436), в яких здобувач була виконавцем окремих етапів.

Мета і задачі дослідження. Метою дисертаційної роботи є розробка та вдосконалення уніфікованих методів і алгоритмів захисту інформації від помилок в комп’ютеризованих інтегрованих системах, які забезпечують високу достовірність та швидкість передачі.

Для досягнення зазначеної мети поставлені наступні задачі:

− провести аналіз стану, тенденцій розвитку методів захисту інформації у комп'ютеризованих інтегрованих мережах й обґрунтування доцільності розробки методів адаптивної корекції параметрів системи захисту, які забезпечують високу достовірність і швидкість передачі даних за рахунок перерозподілу надмірності коду;

− удосконалити методи захисту інформації в комп’ютеризованих системах на основі побудови адаптивних процедур кодування й декодування з різними ймовірнісними характеристиками при єдиній макроструктурі кодера;

− розробити методи контролю якості каналу зв’язку на основі визначення статистичних характеристик каналу, які дозволяють встановити параметри адаптивної системи захисту;

− удосконалити методи синтезу сигнально-кодових конструкцій для адаптивних систем захисту і передачі інформації в комп’ютеризованих інтегрованих системах;

− розробити технічні рішення щодо реалізації уніфікованих систем захисту та передачі інформації в комп’ютеризованих та інформаційно-керувальних системах.

Об'єкт дослідження – процеси обробки, захисту та передачі інформації в спеціалізованих комп’ютеризованих системах та мережах управління об’єктами.

Предмет дослідження – методи і спеціалізовані програмно-апаратні засоби з адаптивними алгоритмами захисту інформації для комп’ютеризованих інтегрованих систем.

Методи дослідження. Основні положення дисертації базуються на фундаментальних основах теорії обробки й передачі інформації , а також теорії завадостійкого кодування інформації у цифрових системах. Дослідження та розробки виконано на основі використання математичного апарату теорії інформації й випадкових процесів. Для розрахунку оцінки статистичних характеристик каналу зв’язку використовувалися методи лінійної алгебри, теорії імовірності. Для синтезу системи сигналів використовувалися методи Фур’є аналізу й синтезу лінійної алгебри, математичної статистики. Оцінку ефективності розроблених методів і результатів досліджень здійснено на основі комп’ютерних експериментів і математичного моделювання отриманих у лабораторних і виробничих умовах при розробці програмно-апаратного модуля.

Наукова новизна отриманих результатів полягає в наступному:

вперше:

− запропоновано і розроблено метод адаптивної корекції параметрів коду, що базується на генерації множини гніздових згортальних кодів з різними значеннями енергетичного виграшу за рахунок кодування, що дозволяє синтезувати уніфіковані алгоритми захисту інформації в комп'ютеризованих системах;

− розроблено метод визначення якості інформаційного каналу на основі оцінки статистичних характеристик потоку помилок, що дозволяє із зміною поточного стану інформаційного каналу оптимізувати параметрами коду з метою максимізації швидкості передачі при мінімальній надлишковості коду;

− запропоновано і розроблено метод формування і об'єднання широкосмугових сигналів для забезпечення достовірної та своєчасної передачі інформації в комп'ютеризованих мережах та підвищення їх енергетичної ефективності та перешкодостійкості;

отримали подальший розвиток:

− метод декодування згортальних кодів с гнучким алгоритмом Вітербі, який дозволяє декодувати множину синтезованих гніздових кодів, забезпечивши високу достовірність та швидкість передачі інформації за рахунок перерозподілу надлишковості коду системи захисту в інтегрованих системах управління;

− метод для розрахунку параметрів системи об'єднання сигналів, реалізованої на базі цифрових гребінчастих фільтрів, що дозволяє оптимізувати характеристики системи захисту і передачі інформації;

− синтез сигнально-кодових конструкцій для адаптивних систем передачі інформації в комп'ютеризованих системах і мережах, що дозволяє підвищити ефективне використання частотного ресурсу інформаційного каналу.

Практичне значення отриманих результатів для комп'ютеризованих інтегрованих систем полягає у розробці та проектуванні універсальних приладів захисту і передачі інформації, реалізованих на сучасних ПЛІС, які забезпечують функціонування автоматизованої системи управління, як єдиної комп'ютеризованої структури. Розроблені й вдосконалені в роботі методи й алгоритми доведено до практичного втілення, що дозволяє підвищити достовірність і швидкість передачі інформації в інформаційних системах управління.

Практична цінність дисертаційної роботи полягає в наступному:

− уніфіковані методи захисту інформації, що орієнтовані на застосування програмованих засобів обчислювальної техніки, реалізовані у складі комп'ютерних компонентів інформаційних системах управління, дозволяють підвищити достовірність та швидкість передачі інформації.

− метод синтезу сигнально-кодових конструкцій на базі широкосмугових сигналів склав основу розробки функціональних модулів обробки і передачі інформації в комп'ютеризованих системах управління тренажерними комплексами, який забезпечує ефективне використання частотного ресурсу;

− результати роботи використовувались при проектуванні приладів захисту і передачі даних в автоматизованих інформаційних системах для застосу-

вання в комп'ютеризованих мережах управління тренажерними комплексами танків «Оплот», бронемашини БТР-4 (м. Харків КБ ХКБМ), які успішно пройшли державні випробування та впровадження.

Основні положення дисертаційної роботи використовуються в навчальному процесі на кафедрі автоматики та управління в технічних системах НТУ «ХПІ» при дипломному проектуванні й викладанні дисциплін «Теорія інформації», «Комп'ютеризовані системи управління», «Основи збору, обробки і передачі інформації».

Особистий внесок здобувача. Основні результати, що виносяться на захист дисертаційної роботи, отримані здобувачем самостійно. Серед них: методи встановлення якості інформаційного каналу передачі на основі оцінки статистичних характеристик потоку помилок; методи синтезу множини гніздових згортальних кодів зі змінними параметрами для адаптивної системи кодування; удосконалений гнучкий алгоритм Вітербі для декодування набору гніздових згортальних кодів з різними значеннями виграшу/швидкості; методи формування системи сигналів із штучно створеним гребінчастим спектром, які належать до класу широкосмугових сигналів; технологія побудови сигнально-кодових конструкцій на базі системи об'єднання сигналів із гребінчастим спектром і адаптивними загортальними кодами.

Апробація результатів. Основні наукові положення і результати роботи доповідалися й обговорювалися на: XVI, XVII, XIX, XX, XXII Міжнародних науково-практичних конференціях «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, НТУ «ХПІ» 2008, 2009, 2011, 2012, 2014), 26-ій Міжнародній науково-практичній конференції «Впровадження мікропроцесорних систем залізничної автоматики й засобів телекомунікації на базі цифровізації» (м. Алушта, Крим, 2013), 1-ой Науково-технічної конференції «Актуальні проблеми автоматики та приладобудування України» (м. Харків, 2013), 27-ій Міжнародній науково-практичній конференції «Інформаційно-керувальні системи на залізничному транспорті» (м. Харків, 2014), на науково-технічних семінарах кафедри автоматики та управління в технічних системах НТУ «ХПІ».

Публікації. Основний зміст дисертації відображено у 18 наукових публікаціях, з них: 10 статей у наукових фахових виданнях України, 1 – у закордонному періодичному фаховому виданні, 7 – у матеріалах конференцій.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 188 сторінок; з них 50 рисунків по тексту, 2 рисунка на 2 окремих сторінках; 16 таблиць по тексту, список використаних джерел з 135 найменувань на 13 сторінках, 3 додатки на 20 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано її мету й задачі, визначено об'єкт, предмет і методи дослідження, наукову новизну і практичну цінність отриманих результатів, а також відомості про публікації, впровадження, апробацію і структуру роботи.

Перший розділ присвячено проблемному аналізу науково-технічної інформації щодо стану технічних рішень підвищення ефективності обробки, захисту та передачі інформації у комп'ютерних інформаційних системах та мережах для побудови єдиної автоматизованої системи управління тактичними тренажерними комплексами. Проаналізовано сучасний стан питання створення уніфікованих систем захисту від помилок на сучасній елементній базі за допомогою програмних засобів обчислювальної техніки.

Дослідження показали, що в системах передачі інформації в комп'ютеризованих системах та мережах кожний пристрій захисту розробляється під кожний тип каналу зв'язку, що породжує велику кількість різноманітних модулів, які реалізують одну функцію – захист інформації від помилок. Показана доцільність розробки уніфікованих методів і засобів захисту інформації, які враховують поточний стан інформаційного каналу в комп'ютеризованих інтегрованих системах. Проведений аналіз існуючих методів обробки, захисту інформації на основі адаптивного кодування та модуляції з контролем якості показав основні недоліки й обмеження відомих технологій адаптації за швидкістю і енергетичним виграшем. Для ефективного здійснення передачі даних доцільна адаптація за двома критеріями – отримання потрібної величини енергетичного виграшу за рахунок кодування та забезпечення різної швидкості за мінімальної надлишковості коду. Практична реалізація адаптивного кодування в комп'ютерних системах приводить до необхідності використання сумісних за швидкістю перфорованих згортальних кодів і гніздових згортальних кодів з технологією розкладання на підмножину підкодів. Показано, що існуючі інформаційні канали при тій самій ймовірності елементарної помилки або ймовірності створення кодової послідовності можуть суттєво відрізнятися топологією помилок на кодовій послідовності, яка має вирішальне значення при виборі способів підвищення достовірності. Тому оперативний контроль якості каналу необхідно здійснювати з урахуванням оцінки статистичних характеристик потоку помилок в інформаційних комп'ютеризованих системах. Для оптимізації параметрів передачі інформації з адаптивними методами захисту технологія синтезу сигнально-кодових конструкцій повинна забезпечувати високошвидкісну передачу з ефективним використанням частотного та енергетичного ресурсів каналу в комп'ютеризованих інформаційних системах та мережах.

На підставі дослідження й аналізу стану вирішення задачі розробки уніфікованих методів адаптивної корекції параметрів системи захисту інформації, а також способів оперативного контролю якості каналу, обґрунтовані перспективні можливості удосконалення обробки, передачі і захисту інформації в комп'ютеризованих системах та мережах.

Другий розділ присвячений розробці методів адаптивного кодування, процедур синтезу множини згортальних кодів, алгоритмам декодування адаптивних кодів, а також визначенню якості інформаційного каналу, що почало основні теоретичні аспекти побудови уніфікованої системи захисту в комп'ютеризованих інтегрованих системах.

Для побудови адаптивних систем кодування серед завадостійких кодів найбільший інтерес мають згортальні коди, а також клас кодів, сумісних за

швидкістю (перфоровані коди). Аналіз ймовірнісних характеристик згорткальних кодів показав, що із зростанням m (довжина кодового обмеження) енергетичний виграш від кодування (ЕВК) збільшується приблизно на 0,3 … 0,4 дБ, що дозволяє оцінити можливості побудови універсальних кодерів швидкістю $R = 1/n$ з різними значеннями m. Множина підкодів, синтезованих з базового згортального кодера зі швидкістю R за допомогою зміни довжини кодового обмеження і породжувальних поліномів, зберігши макроструктуру кодера і декодера, отримало назву гніздові згортальні коди (Nested Convolution Codes − NCC).

Згортальний код зі швидкістю R і числом розрядів пам'яті m складається з m-розрядного зсувного регістру та n суматорів за модулем два. Коефіцієнти сполучення G_i^j $j = 1, \ldots n$, $0 \le i \le m$ належать скінченному полю $GF(2)$ елементів відводу. Згортальний код з числом розрядів пам'яті m задається поліномами своїх генераторів

$$G_m^j(x) = g_0^j + g_1^j(x) + g_2^j(x^2) + ... + g_{l+1}^j(x^{l+1}) + ... + g_m^j(x^m), \qquad (1)$$

де $g_0^j = g_m^j = 1$ і $j = 1, \ldots n$.

Множина гніздових згортальних кодів з числом розрядів пам'яті $m-l$ визначено $G_{m-l}^j(x)$ для $1 \le l \le m-2$ і отримано з базового коду швидкості $R = 1/n$ с генераторними послідовностями $G_m^j(x)$ визначаються як

$$G_{m-l}^j(x) = g_0^j + g_{l+1}^j(x) + g_{l+2}^j(x^2) + ... + g_{m-1}^j(x^{m-l-1}) + g_m^j(x^{m-l}), \qquad (2)$$

де $g_0^j = g_m^j = 1$ і $j = 1, \ldots n$.

Синтез множини гніздових згортальних кодів базується на 2-х методах: метод уперед і метод назад. Метод назад використовується для отримання кодів з меншим числом розрядів пам'яті і передбачає, що для даного згортального коду з довжиною кодового обмеження m є можливим синтез гніздового коду з довжиною кодового обмеження $m-l$ та з оптимальною вільною відстанню. У таблиці 1 наведено синтезовані генераторні послідовності множини гніздових згортальних кодів, які отримані з базових генераторних послідовностей $G_6(171, 133)$ за методом назад. Вільна відстань генеруємих гніздових кодів має теж значення, що й у відомих оптимальних згортальних кодів.

Метод вперед будується зі стандартного базового загортального коду ($R = 1/n$) з довжиною кодового обмеження $m = 2$ і генераторними послідовностями

$$G_1^j(x) = g_0^j + g_2^j(x^2),\ G_2^j(x) = g_0^j + g_1^j(x) + g_2^j(x^2), \qquad (3)$$

де $j = 1, \ldots n$.

Основою даного методу є отримання коду з довжиною кодового обмеження $m+1$. У таблиці 2 наведено генераторні послідовності множини гніздових згортальних кодів з довжиною кодового обмеження m від 2 до 6, син-

тезовані за методом уперед. Для порівняння наведено також вільну відстань і загальне число ненульових інформаційних бітів. На довжині вільної відстані для оптимальних згортальних кодів. Можна зазначити, що всі коди, які генеруються за методом уперед досягають вільної відстані такої ж величини, як d_f у оптимальних кодів.

Таблиця 1 − Гніздові згортальні коди, побудовані за методом назад

m	Кодові генератори		Гніздові згортальні коди		Оптімальні згортальні коди	
			d_f	N	d_f	N
6	1011011 1111001	171, 133	10	36	10	36
5	111011 111001	73, 71	8	10	8	2
4	11011 11001	33, 31	7	4	7	4
3	1011 1001	13, 11	5	1	6	2
2	101 111	7, 5	5	1	5	1

Таблиця 2 − Гніздові згортальні коди, побудовані за методом уперед

m	Кодові генератори		Гніздові згортальні коди		Оптімальні згортальні коди	
			d_f	N	d_f	N
2	101 111	7, 5	5	1	5	1
3	1101 1011	15, 13	6	4	6	2
4	11101 10011	35, 23	7	4	7	4
5	111101 110011	75, 63	8	6	8	2
6	1011101 1110011	163, 135	10	46	10	36

Показано, що для декодування множини гніздових згортальних кодів використовується гнучкий алгоритм Вітербі з архітектурою, яка має лише два працюючих паралельно блоки скласти-порівняти-вибрати (СПВ). Цей алгоритм передбачає послідовну обробку станів $0 + j$ и $2^{m-1} + j$, де $j = 0, \ldots, 2^{m-2} - 1$ першим процесором, у той час коли другий процесор виконує послідовну обробку станів від $2^{m-2} + j$ и $2^{m-1} + 2^{m-2} + j$, де $j = 0, \ldots, 2^{m-2} - 1$. Таким чином, процесор Вітербі, розрахований на декодування згортального коду зі швидкістю $R=1/n$ з 2^m станів, запрограмований так, щоб декодувати згортальний код зі швидкістю $R=1/n$ с 2^{m-l} станами при $0 \le l \le m-2$. У цьому випадку перший блок СПВ обробляє стани: $0 + j$ и $2^{m-l-1} + j$, де $j = 0, \ldots, 2^{m-l-2} - 1$, а другий блок СПВ обробляє стани $2^{m-l-2} + j$ і $2^{m-l-1} + 2^{m-l-2} + j$, де $j = 0,\ldots,2^{m-l-2} - 1$.

Обидва процесори поновлюють старі значення станів метрик з метричних таблиць від комірки 0 до $2^{m-l}-1$, тоді як оновленні значення метрик записуються в комірки від 0 до $2^{m-l-1}-1$ першим процесором і в комірки від 2^{m-l-1} до $2^{m-l}-1$ другим процесором.

Надані методи визначення інформаційного стану каналу на основі оцінки статистичних характеристик потоку помилок на виході інформаційного каналу. Оцінка основана на топологічному представлені процесу формування помилок на довжині кодових блоків, яка дозволяє оптимізувати вагову функцію помилок *n*-послідовностей на множинні (*n*, *m*) – розбиттів. Показано, що при заданому значенні довжини кодової послідовності одному і тому самому значенню ймовірності помилок на біт на виході інформаційного каналу відповідають різні розподіли помилок на множені n – послідовностей. Дослідження виконані в роботі, показали, що потенційна ймовірність помилки декодування $Ð^{*}_{ïîì\ \ .äåê}$ визначається подвійною нерівністю $0 \le P^{*}_{ïîì\ \ .äåê} \le \overline{p}_{\sigma}$ ($\overline{p}_{\sigma}$ − ймовірність помилки біта) в залежності від розподілу помилок в інформаційному каналі. Рівність нулю досягається при виконанні умови

$$\sum_{d=1}^{m} d \cdot V_d^{[m]} = \sum_{d=1}^{m} d \cdot V_d^{[n]} \ , \tag{4}$$

коли вагова функція *n*−послідовності $V_d^{[n]}$ дорівнює ваговій функції *m* −послідовності $V_d^{[m]}$, тобто на довжині *n*-послідовності не виникають помилки ваги більше *m*.

Для аналізу залежності $Ð^{*}_{ïîì\ \ .äåê}$ від статистики помилок, виражену через функцію кратності $P(d, n)$, та параметрів (*n*, *m*) розбиття послідовності помилок на виході каналу, знайдено співвідношення

$$P^{*}_{ïîì\ \ .äåê} = \overline{p}_{\sigma} - \sum_{d=1}^{m} \frac{d}{n} \cdot P(d,n) \ . \tag{5}$$

Ймовірність помилки біту для *j*-го стану каналу визначається як

$$\overline{p}_{\sigma} = \frac{1}{m}\sum_{d=1}^{m} d \cdot P(d,m) = \frac{1}{n}\sum_{d=1}^{n} d \cdot P(d,n), \tag{6}$$

де $P(d, n)$, $P(d,m)$ − функція кратності помилок, а значення *n* та *m* в знаку доданку визначає верхню межу кратності помилок на *n* і *m* послідовностях. Якщо *n*>*m*, то вираз (6) має вигляд

$$\frac{1}{m}\sum_{d=1}^{m} d \cdot P(d,m) - \frac{1}{n}\sum_{d=1}^{n} d \cdot P(d,n) = \sum_{d=m+1}^{n} \frac{d}{n} \cdot P(d,n). \tag{7}$$

Вираз (7) базується на твердженні, що ймовірність помилки біта (6) в каналі є постійною для даної реалізації процесу формування помилок та не зале-

жить від способу розбиття інформації на кодові блоки. З цього випливає, що при зміні довжини ділянки розбиття від m до n ($n > m$) маючи на увазі при цьому під m − довжина інформаційної частини , а під n – довжина кодового блоку, необхідно досягти мінімального значення правої частини приведеного виразу.

Третій розділ присвячений розробці процедур синтезу сигнально-кодових конструкцій для адаптивних систем кодування на базі сигналів з розширеним спектром, як основні теоретичні аспекти для проектування приладів обробки і передачі інформації в комп'ютеризованих системах і мережах.

Показано, що при формуванні широкосмугових сигналів з гребінчастим спектром проблема набуття необхідної ширини спектра F_c' первинного сигналу вирішується шляхом компресії його часових відрізків у N разів так, що $F_c' = NF_c$, де F_c' − значення ширини спектра групового сигналу, або в більш загальному випадку, відповідає ширині спектра системи сигналів з гребінчастими спектрами. Використання штучно розширеної бази для кожного з сигналів дає стійкість до зосереджених за спектром завад. Об'єднання сигналів з гребінчастим спектром передбачає «стиск» за часом i-го індивідуального сигналу тривалістю T_c^i з ефективною шириною спектра $\Delta\omega_i$ у n разів ($i = \overline{1, n}$), внаслідок чого його спектр розширюється до смуги групового каналу $\Delta\omega_k = \omega_в - \omega_н$, тобто всі сигнали мають спектри, які повністю перекриваються. При цьому тривалість «стислого» за часом відрізка сигналу стає рівною

$$T_k = \frac{\Delta\omega_i}{\Delta\omega_k} T_c^{\,i}, \qquad (8)$$

але однаковою для усіх сигналів, які об'єднуються. Для кожного з індивідуальних сигналів формується канальна форма $S'_i(\omega)$, ($i = \overline{1, n}$), яка виходить шляхом «вирізання» не перехресних ділянок спектра. Тобто канальна форма кожного з індивідуальних сигналів має гребінчасту структуру, яка формується за допомогою гребінчастих фільтрів (ГФ). Груповий сигнал $S_г(\omega)$ формується шляхом підсумування індивідуальних сигналів з неперервними гребінчастими спектрами (рис. 1).

Показано, що сигнали з гребінчастим спектром використовують весь частотний діапазон групового каналу, який надає їм можливість виявити позитивні якості широкосмугових сигналів, стійких до впливу зосереджених за спектром завад. Канальна форма перетвореного сигналу являє собою n-кратно повторюваний із відповідним масштабуванням a_k первинний інформаційний сигнал

$$x_k^i = \sum_{k=0}^{p} a_k^i x(t - k\tau), \qquad (9)$$

де $x_i(t)$ − i-й індивідуальний сигнал, який подається на вхід ГФ; a_k^i − коефіцієнти i-го ГФ; τ − період ГФ

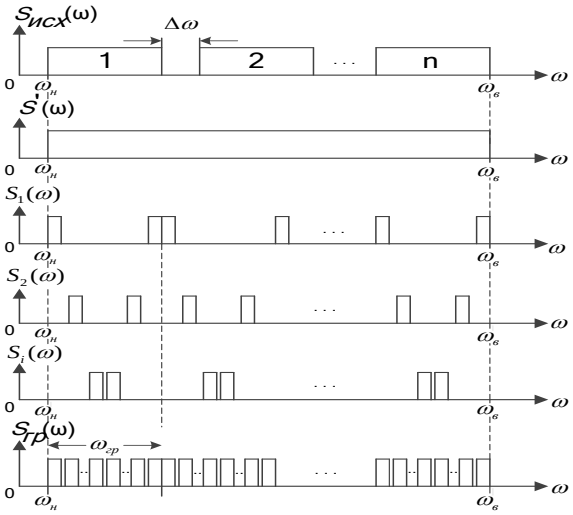

Рисунок 1 − Порядок формування групового сигналу

Для виділення початкового індивідуального сигналу з групового достатньо обробити останній гребінчастим фільтром тотожним за структурою і параметрам формуючому. На *p*–м такті роботи фільтра після початку приймання групового сигналу, на його виході з'явиться відлік

$$x_{âèõ}^{\ i}(t)=\sum_{k=0}^{p} a_k^{\ i} x_i'(t). \tag{10}$$

При цьому однакові перетворення сигналів на передавальній і приймальній сторонах системи дозволяють отримати достатньо просту схему системи об'єднання.

Розглянуто і наведено алгоритм розрахунку коефіцієнтів гребінчастих фільтрів при проектуванні сигнально-кодових конструкцій на основі системи об'єднання і виділення сигналів з урахуванням умовної мінімізації перехідних завад між сигналами, які об'єднуються. На основі використання метода найменших квадратів виконано розрахунок коефіцієнтів цифрового фільтра шляхом мінімізації відстані між еталонною характеристикою $f(\omega)$ і передаточною функцією $K(j\omega)$

$$\pi a_k^i = \frac{sin(T-k\tau)\omega_â^i - sin(T-k\tau)\omega_1^i}{(T-k\tau)}\ . \tag{11}$$

Виключення перехідних завад досягається шляхом забезпечення ортогональності векторів коефіцієнтів індивідуальних формуючих фільтрів

$$\sum_{k=0}^{p} a_k^i a_k^j = 0, \tag{12}$$

де $i = 1, \ldots, n$; $j = 1, \ldots, n$; $i \neq j$.

Урахування розмірності векторів коефіцієнтів фільтрів потребує для існування n ортогональних векторів розмірності простору не менш n. Звідси вихо-

дить висновок,що при об'єднанні n сигналів порядок фільтрів має бути не менше ($n-1$). Тоді задача знаходження коефіцієнтів гребінчастих фільтрів має вигляд задачі на умовний екстремум

$$min\left\{ C_i + \sum_{j=1}^{n} \lambda_j \sum_{k=0}^{p} a_k^i a_k^j \right\}, \qquad (13)$$

де λ_i – множителі Лагранжа; C_i – цільова функція мінімізації відстані між еталонною передаточною функцією аналогового прототипу і поточною передаточною функцією; $i = 1, \ldots, n$; $j \neq i$.

Запропоновано схему побудови адаптивної сигнально-кодової конструкції на основі згортальних кодів зі змінними параметрами і з процедурою об'єднання сигналів з гребінчастим спектром (рис. 2). Довільний i-й індивідуальний сигнал $x_i(t)$ с ефективною шириною спектра $\Delta\omega_i$, проходячи крізь часовий компресор (ЧК), підлягає перетворенню шляхом «ділення» на відрізки T_c^i і видавання зі швидкістю у $\Delta\omega_k/\Delta\omega_i$ разів вищою у порівнянні с первинною. Виділення індивідуальних сигналів виконується набором гребінчастих фільтрів, тотожних формуючим, які у даному випадку реалізують як частотну, так і узгоджену фільтрацію шляхом згортання відліків формуючих гребінчастих фільтрів в один часовий відрізок T_k з максимальною амплітудою. Для встановлення первинної форми сигналів $x_i(t)$ використовується часова декомпресія, яка виконується набором часовий декомпресор (ЧД). На наступному етапі кодова комбінація $\{x_i'(t)\}$ декодується гнучким алгоритмом Вітербі та формується інформаційна послідовність $\{a_i'(t)\}$.

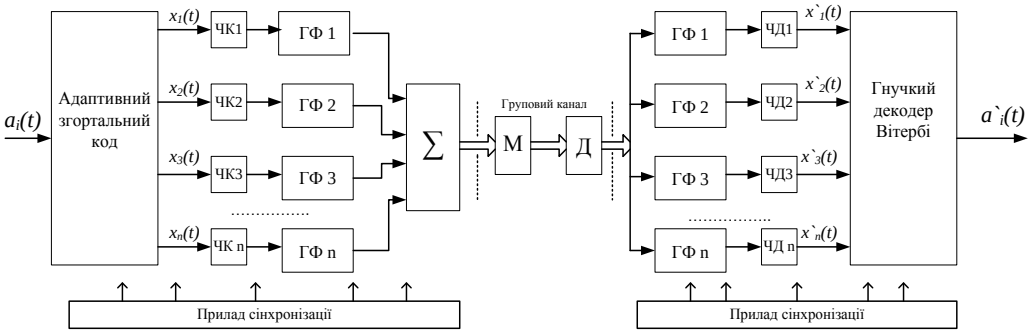

Рисунок 2 − Структурна схема сигнально-кодової конструкції

Запропонована технологія синтезу сигнально-кодових конструкцій на основі системи сигналів с гребінчастим спектром (ССГС) дозволяє виключати не ефективні затрати смуги частот високошвидкісних трактів шляхом усунення захисних інтервалів між індивідуальними каналами, та таким чином підвищити функціональність комп'ютеризованої інтегрованої системи.

Четвертий розділ присвячений розробці імітаційної моделі адаптивної системи передачі даних для оцінки імовірнісних характеристик синтезованих гніздових згортальних кодів зі змінними параметрами, а також дослідженню практичної реалізації цифрової системи об'єднання сигналів з гребінчастим

спектром. Запропоновано технічне рішення реалізації адаптивного пристрою захисту і передачі інформації на ПЛІС типа FPGA фірми Altera, з використанням вбудованих IP core блоків для побудови систем на кристалі, як комп'ютерного компоненту.

Проведено експериментальні дослідження визначення якості інформаційного каналу зв'язку на основі оцінки топологічних характеристик потоку помилок в каналі комп'ютеризованої інтегрованої системи. Наведено результати дослідження, які підтверджують розроблену теорію, що зі зростанням довжини кодового слова також зростає максимальна вага помилок при фіксованій корегувальній здатності, яка зумовлює зростання ймовірності помилки декодування (рис. 3).

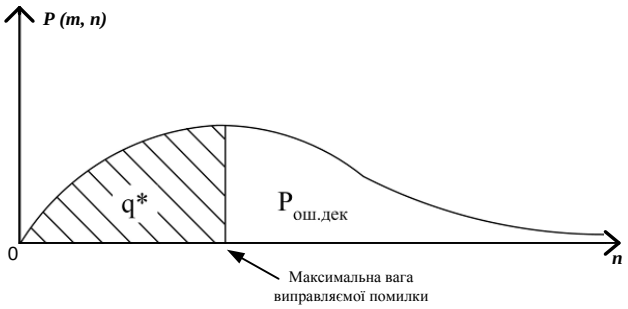

Рисунок 3 − Ймовірностний вектор топології помилок

Для оцінки ймовірних характеристик бітових помилок перфорованих згортальних кодів, синтезованих з множини гніздових, розроблено імітаційну модель адаптивної системи передачі у середовищі Matlab+Simulink (пакеті Communications Blocked). Отримано результати досяжних значень енергетичного виграшу за рахунок кодування у залежності від швидкості та довжини кодового обмеження коду (m) при $P_\sigma=10^{-5}$ (частота бітових помилок) для адаптивної системи кодування зі змінними значеннями виграш/швидкість і з гнучким декодером Вітербі (табл. 3).

Аналіз ймовірнісних характеристик частоти бітових помилок множини гніздових згортальних кодів, які декодуються гнучким алгоритмом Вітербі, показує, що достатньо великі значення ЕВК (більш 2,2 дБ) можуть досягатися навіть при високих швидкостях кодування.

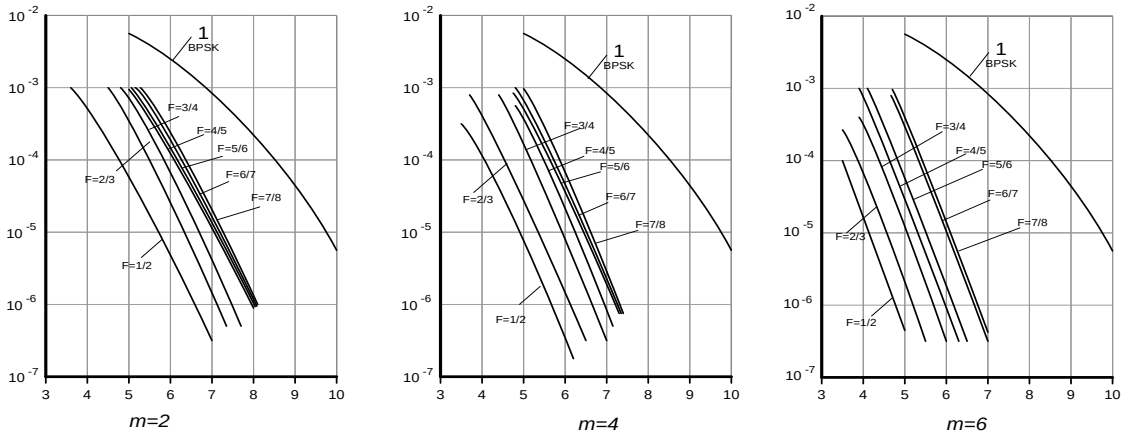

Рисунок 4 − Характеристики частоти бітових помилок для адаптивних кодів

Таблиця 3 − Значення ЕВК для адаптивної системи кодування

R	*m*=2	*m*=4	*m*=6
7/8	2,2	3,0	3,4
6/7	2,3	3,1	3,5
5/6	2,4	3,2	3,9
4/5	2,5	3,4	4,2
3/4	2,0	3,7	4,5
2/3	3,1	4,0	5,0
1/2	3,7	4,6	5,4

Надано порівняльну оцінку частотної ефективності запропонованого методу формування системи сигналів з гребінчастим спектром і частотно-модульованих сигналів (ЧМ-2). Дослідження показало, що перехід до методу формування групового сигналу за технологією ССГС приводить до звуження енергетичного спектра й концентрації енергій поряд з несучою частотою. Таким чином, у задану смугу, обмежену фільтром на вході частот корисного сигналу, що приводить до зростання відношення сигнал/шум на вході дискримінатора, і як наслідок, до зменшення ймовірності помилки на біт повідомлень, які передаються. У табл. 4 наведено частку енергії сигналу, яка потрапляє в смугу пропускання фільтра приймача при різних значеннях швидкості модуляції для ЧМ-2, а також для ССГС-2, ССГС-4 і ССГС -10. Дані таблиці показують, що при однакових енергетичних умовах ССГС-10 виграють у порівнянні з ЧМ-2 за допустимою швидкістю більш ніж у 2 рази (10800 проти 4800).

Таблиця 4 − Частка енергії сигналу, яка потрапляє в смугу пропускання фільтра

Режим	Швидкість модуляції, бит/с						
	200	1200	2400	4800	5600	9600	10800
ЧМ-2	0,997	0,978	0,954	0,910	0,890	0,767	0,710
ССГС-2	0,998	0,981	0,967	0,943	0,922	0,850	0,816
ССГС-4	0,999	0,987	0,972	0,965	0,941	0,894	0,870
ССГС-10	1	0,999	0,984	0,980	0,960	0,910	0,900

Експериментальні дослідження підтвердили високу ефективність запропонованої технології побудови ССГС, яка використовує увесь частотний діапазон групового каналу, що обумовлюється їх властивостями широкосмугових сигналів, стійких до впливу зосереджених за спектром завад.

Запропоновано технічне рішення апаратної реалізації адаптивного пристрою захисту і передачі інформації на ПЛІС типу FPGA фірми Altera з використанням вбудованих IP core блоків для побудови систем на кристалі. Синтезований пристрій дозволяє без додаткових енергетичних затрат підвищити завадостійкість сигналів, у тому числі до впливу зосереджених за спектром імпульсних завад і переривів зв’язку, а також підвищити на 25-50% коефіцієнт використовування смуги частотно-часового ресурсу.

У **додатках** наведено текст комп’ютерної програми на мові С++, яка реалізує методи адаптивного кодування на основі синтезу гніздових згортальних

кодів зі змінними параметрами й гнучким алгоритмом Вітербі. Наведено схему імітаційної моделі системи передавання даних з адаптивними методами захисту інформації. Також надано текст програми на мові С++ визначення значень коефіцієнтів цифрових фільтрів для системи сигналів с гребінчастим спектром. Наведені акти впровадження в навчальний процес кафедри автоматики та управління в технічних системах НТУ «ХПІ», а також при проектуванні комп'ютеризованих інтегрованих систем та мереж управління тренажерними комплексами танків «Оплот», бронемашини БТР-4 (м. Харків КБ ХКБМ).

ВИСНОВКИ

У дисертаційні роботі вирішено науково-практичне завдання щодо вдосконалення апаратно-програмних засобів обробки, захисту і передачі інформації в інформаційних мережах, як елемента комп'ютеризованої інтегрованої системи. Проведені дослідження, спрямовані на вдосконалення алгоритмів захисту даних від помилок, які дозволили вирішити низку завдань щодо розробки уніфікованих методів передачі і захисту інформації. Основні наукові та практичні результати полягають у наступному:

1. На основі аналізу науково-технічних джерел, стану і тенденцій розвитку засобів захисту, обробки та передачі інформації у комп'ютеризованих інтегрованих системах у світі сучасних цифрових технологій обґрунтовано проектування програмно-апаратних елементів, реалізованих на адаптивних методах захисту і передачі інформації, які враховують якість інформаційного каналу в комп'ютеризованих системах.

2. Розроблено методи адаптивного кодування на основі синтезу множини гніздових згортальних кодів на єдиній макроструктурі кодера, які використовуються для достовірного та своєчасного доведення інформації. Для декодування множини гніздових згортальних кодів у адаптивних системах кодування надано гнучкий алгоритм Вітербі, який забезпечує декодування широкого діапазону кодів із різними значеннями ЕВК і з різними вимогами до канальної швидкості. Методи рекомендовані до практичного вживання при створенні апаратно-програмного забезпечення процесів захисту інформації в інформаційних мережах.

3. Розроблені методи визначення якості інформаційного каналу, побудовані на оцінки статистичних характеристик потоку помилок, для оперативного визначення та корекції параметрів синтезованих гніздових згортальних кодів. Наведені теоретичні аспекти дозволяють здійснювати оцінку ефективності використання адаптивних алгоритмів захисту інформації для поточного стану інформаційного каналу в комп'ютеризованих інтегрованих системах.

4. Розроблено методи формування сигналів із штучно створюваними гребінчастими спектрами, які відрізняються від відомих властивостями частотної селекції, високою завадостійкістю і простотою реалізації. На основі вказаних широкосмугових сигналів запропоновано технологію формування системи об'єднання та виділення сигналів, яка дозволяє підвищити на 10 дБ без додаткових енергетичних витрат завадостійкість індивідуальних сигналів до

впливу зосереджених завад. Наведені теоретичні аспекти дозволяють застосовувати їх при розробці сигнально-кодових конструкцій каналоутворювальних компонентів комп'ютерних систем та мереж.

5. Запропоновано співвідношення для розрахунку параметрів системи об'єднання сигналів на основі цифрових гребінчастих фільтрів, забезпечуючи простий і надійний селективний доступ до ресурсів групового тракту обміну інформацією в комп'ютеризованих мережах за рахунок вибору вектора коефіцієнтів одного з ортогональних формуючих цифрових фільтрів.

6. Розроблено технологія побудови сигнально-кодової конструкції для адаптивних систем захисту інформації з системою об'єднання та виділення сигналів с гребінчастим спектром, яка дозволяє знизити питомі витрати частотно-часового ресурсу до 50%, мінімізувати габаритні розміри й енергоспоживання кінцевих станцій. Застосування наведеної технології синтезу сигнально-кодової конструкції в комп'ютеризованих мережах дозволяє без внесення частотної і енергетичної надмірності знизити вплив природних та навмисних перешкод, а також забезпечити захист від перехоплювання та випадкових прослухувань.

7. Запропоновано алгоритми і апаратно-програмні рішення для забезпечення процесів захисту, обробки та передачі інформації в комп'ютеризованих інтегрованих системах, які реалізуються повністю на елементах цифрової техніки, а саме на ПЛІС типу FPGA фірми Altera з використанням вбудованих IP core блоків.

8. Результати дисертаційної роботи впроваджені на державному підприємстві «Харківське конструкторське бюро з машинобудування ім. О.О. Морозова» при розробці комп'ютеризованих систем управління для тактичних тренажерних комплексів танка «Оплот», бронемашин БТР-4, та у навчальному процесі кафедри автоматики та управління в технічних системах НТУ «ХПІ».

СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Крилова В.А. Оценка возможности унификации методов передачи данных в сетях связи с интеграцией служб / В.А. Крилова, В.В. Горбачев // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2005. − №7 – С. 36−40.

Здобувачем проведено дослідження та сформульовано мета і задача розробки уніфікованих засобів захисту інформації в цифрових інформаційних системах зв'язку.

2. Крилова В.А. Результаты экспериментальных исследований методики оценки статистических характеристик потоков ошибок на выходе дискретного канала связи / В.А. Крилова, Д.В. Биднина, В.В Горбачов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2005. − №38 – С.16−21.

Здобувачем проведено експериментальні дослідження визначення якості каналу зв'язку на основі топологічних характеристик системи передачі інформації.

3. Крилова В.А. Методы адаптивного кодирования для каналов с переменными параметрами / В.А. Крилова, В.В. Горбачев, С.Ю. Гавриленко // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2008. − №31 – С.19−26.

Здобувачем розроблені методи адаптивного кодування для каналів зі змінними параметрами.

4. Крилова В.А. Оценка возможности построения универсальных кодеков на основе свёрточных кодов с алгоритмом декодирования Витерби / В.А. Крилова, В.В. Горбачев // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2008. − №57 – С. 44−52.

Здобувачем запропоновано побудова уніфікованих методів захисту інформації на основі згортальних кодів с алгоритмом Вітербі.

5. Крилова В.А. Гибкий алгоритм Витерби для декодирования свёрточных кодов с переменными параметрами / В.А. Крилова, В.В. Горбачов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2010 г. − №20 – С. 45−51.

Здобувачем запропоновано удосконалений гнучкий алгоритм Вітербі для декодування гніздових згортальних кодів в адаптивних системах.

6. Крилова В.А. Метод синтеза гнездовых свёрточных кодов с переменными параметрами / В.А. Крилова // Вісник Національного технічного університету «Харківський політехнічний інститут». – 2011. − №11 − С. 80−86.

7. Крилова В.А. Методика выбора параметров гнездовых свёрточных кодов / В.А. Крилова // Вісник Національного технічного університету «Харківський політехнічний інститут». – 2011. − №57 – С. 74−78.

8. Крилова В.А. Оценка информационного состояния канала связи в адаптивных системах кодирования/декодирования / В.А. Крилова // Вісник Національного технічного університету «Харківський політехнічний інститут». – 2013. − №8(982) – С. 64−70.

9. Крилова В.А. Гнездовые свёрточные коды с переменной параметрами в адаптивных системах кодирования / В.А. Крилова // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева – Алмата: КазАТК, 2013. − №5(84) – С.77−83.

10. Крилова В.А. Реализация адаптивного устройства кодирования/декодирования на ПЛИС / В.А. Крилова // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків : НТУ «ХПІ», 2014. − №15 (1058) – С. 86−90.

11. Крилова В.А. Сигнально-кодовые конструкции для адаптивных методов кодирования в многоканальных системах связи / В.А. Крилова, В.В. Горбачов // Інформаційно-керуючи системи на залізничному транспорті. – Харків : УкрГАЖТ, 2014. − №1(104) – С. 56−58.

Здобувачем запропоновано технологія синтезу сигнально-кодової конструкції для адаптивних систем кодування/декодування.

12. Крилова В.А. Методы адаптивного кодирования для цифровых каналов связи / В.А. Крилова, В.В. Горбачов, С.Ю. Гавриленко // Тези доповідей

XVI Міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 4-6 червня) – Харків : НТУ «ХПІ», 2008. – С. 358 – 359.

Здобувачем запропоновано технологія побудови системи кодування на основі генерації гніздових згортальних кодів з різними характеристиками.

13. Крилова В.А. Алгоритм Витерби для декодирования гнездовых свёрточных кодов / В.А. Крилова, В.В. Горбачов, В.А. Андросов // Тези доповідей XVII Міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 20-22 травня) – Харків : НТУ «ХПІ», 2009 – С. 426 – 427.

Здобувачем запропоновано адаптивний метод декодування згортальних кодів з різними значеннями енергетичного виграшу від кодування та канальної швидкості.

14. Крилова В.А. Гнездовые свёрточные коды с переменной скоростью / В.А. Крилова // Тези доповідей XIV Міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 1-3 травня) – Харків : НТУ «ХПІ», 2011 – С. 116 – 118.

15. Крилова В.А. Оценка информационного состояния канала связи / В.А. Крилова // Тези доповідей XX Міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 15-17 травня) – Харків : НТУ «ХПІ», 2012 – С. 36−37.

16. Крилова В.А. Оценка потенциальных границ для вероятности ошибки декодирования помехоустойчивых кодов / В.А. Крилова // Тези доповідей 26-ой Міжнародної науково-практичної конференції «Внедрение перспективных микропроцессорных систем железнодорожной автоматики и средств телекоммуникаций на базе цифровизации» (Алушта, Крим 23-28 вересня) – Харків : УкрГАЖТ, 2013 – С. 36−37.

17. Крилова В.А. Реализация адаптивного устройства кодирования-декодирования / В.А. Крилова // Тези доповідей 1-ой Науково-технічної конференції студентів, аспірантів та молодих вчених «Актуальні проблемі автоматики та приладобудування України» (Харків, 12-13 грудня) – Харків : НТУ «ХПІ», 2013 – С. 38−40.

18. Крилова В.А. Широкополосные цифровые системы многоканальной связи / В.А. Крилова // Тези доповідей XXII Міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 15-17 травня) – Харків : НТУ «ХПІ», 2014 – С. 123−125.

АНОТАЦІЇ

Крилова В.А. **Розробка уніфікованих методів захисту інформації в комп'ютеризованих інтегрованих системах –** На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний технічний університет «Харківський політехнічний інститут», Харків 2014.

Дисертацію присвячено розробці та вдосконаленню методів, засобів захисту й передачі інформації на основі процедур синтезу сигнально-кодових конструкцій з адаптивним кодуванням/декодуванням для комп'ютеризованих інтегрованих систем.

У дисертаційні роботі розглянуто алгоритми та методи реалізації адаптивного захисту інформації з оцінкою якості інформаційного каналу, а також технології побудови сигнально-кодових конструкцій із системою широкосмугового доступу. Показано шляхи й способи підвищення достовірності, швидкості та ефективності використання частотного ресурсу каналу за рахунок побудови універсальних програмно-апаратних пристроїв захисту інформації в комп'ютеризованих мережах.

Запропоновано метод синтезу множини гніздових згортальних кодів зі змінними параметрами, а також вдосконалені методи декодування гніздових кодів, що дозволяє синтезувати гнучкий алгоритм Вітербі, забезпечивши високу достовірність передачі інформації при мінімальній надмірності коду. Розроблено метод формування сигналів із штучно створюваним гребінчастим спектром, що належать до класу широкосмугових сигналів, який дозволяє підвищувати ефективність використання частотно-часового ресурсу систем передачі шляхом усунення захисних інтервалів між індивідуальними каналами. У роботі наведено технологія синтезу сигнально-кодових конструкцій на основі побудови системи об'єднання сигналів з гребінчастим спектром для реалізації універсальних приладів захисту інформації в комп'ютеризованих мережах та системах.

Розроблено методи і процедури синтезу уніфікованих систем захисту інформації на основі використання гніздових згортальних кодів із гнучким алгоритмом Вітербі, а також системи об'єднання сигналів із гребінчастим спектром. Створення таких пристроїв дозволяє підвищити достовірність і швидкість передачі інформації при мінімальній надлишковості кодера, а також забезпечити ефективне використання частотного ресурсу інформаційного каналу в комп'ютеризованих системах.

Ключові слова: комп'ютеризовані системи і мережі, система захисту інформації, адаптивне кодування, широкосмугові сигнали, гребінчастий спектр сигналу, сигнально-кодова конструкція.

Крылова В.А. Разработка унифицированных методов защиты информации в компьютеризированных интегрированных системах – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Национальный технический университет «Харьковский политехнический институт», Харьков 2014 г.

Диссертация посвящена разработке и усовершенствованию методов, средств защиты, обработки и передачи информации на основе процедур синтеза сигнально-кодовых конструкций с адаптивной коррекцией параметров кодера для компьютеризированных интегрированных систем.

В диссертации обоснована цель, актуальность направления исследования, проведен обзор унифицированных средств обработки, защиты и передачи информации, а также известных способов контроля и оценке качества информационного состояния канала. Проведен анализ вероятностно-временных показателей доставки сообщений в основных информационных направлениях, особенностей используемых каналов в компьютеризированной сети связи, а также требований к достоверности передачи информации. Рассмотрены алгоритмы и методы реализации адаптивного кодирования, а также технология построения сигнально-кодовых конструкций с системой широкополосного доступа. Показаны пути и способы повышения помехозащищенности и эффективности использования частотно-временного ресурса канала за счет использования универсальных программно-аппаратных устройств зашиты от ошибок.

В диссертационной работе предложено решение задачи оперативного нахождения параметров помехоустойчивого кода, обеспечивающих заданную вероятность доведения передаваемого сообщения при минимальной избыточности кода. Получил развитие метод защиты информации на основе свёрточных помехоустойчивых кодов с декодером Витерби. Предложен метод синтеза множества гнездовых свёрточных кодов с переменными параметрами, а также обоснована возможность построения гибкого алгоритма Витерби для адаптивного декодирования, который обеспечивает высокую достоверность и своевременность доведения сообщения в компьютеризированных интегрированных системах. Разработан метод определения качества канала связи на основе оценке статистических характеристик потока ошибок, основанная на топологическом представлении процесса формирования ошибочных символов на длине кодовых последовательностей, которая позволяет определить параметры адаптивных кодов.

В работе предложена технология синтеза сигнально-кодовых конструкций на основе системы сигналов с гребенчатым спектром и адаптивным кодированием. Разработан метод формирования сигналов с искусственно создаваемыми гребенчатыми спектрами, которые принадлежат к классу широкополосных сигналов, позволяющий обеспечить эффективное использование частотно-временного ресурса систем передачи, путем устранения защитных интервалов между индивидуальными каналами. Предложен алгоритм нахождения коэффициентов цифровых фильтров для реализации системы уплотнения сигналов методами условной минимизации переходных помех между объединяемыми сигналами.

Приведены результаты экспериментальных исследований разработанных универсальных методов и средств защиты информации, а также методов контроля качества информационного канала. Полученные теоретические результаты подтверждены результатами вычислительных экспериментов и примерами конкретных алгоритмов и технических решений.

Ключевые слова: компьютеризированные системы и сети, система защиты информации, адаптивное кодирование, широкополосные сигналы, сигнально-кодовые конструкции, гребенчатый фильтр.

20

Krulova V.A. Development of standardized methods for the protection of information in computer-integrated systems. – Manuscript.

Thesis for a Candidate Degree in Technical Sciences: Specialty 05.13.05 – computer system and components. – National Technical University «Kharkov Polytechnic Institute», Kharkov 2014.

Thesis is devoted to the development and improvement of information protection and transmission methods on the basis of synthesis procedures for signal-code structures with adaptive encoding / decoding.

In the thesis work are presented methods and algorithms for implementing adaptive coding and technology of signal-code structures with broadband access construction. The ways and means of error-protection enhancement and effective use of time-frequency channel resource by using the universal software and hardware for error-protection are shown.

A method for synthesis of a set of nested convolutional codes with variable parameters is proposed, and a flexible Viterbi algorithm for adaptive decoding, which provides high reliability and timeliness of messages in the communication channels is presented. The paper presents the technology of synthesis of signal-code structures on the basis of a system of signals with a comb spectrum and adaptive coding. A method of forming signals with artificially created comb spectra that belong to a class of broadband signals is presented, which allows more efficient use of transmission systems time-frequency resource by eliminating the guard intervals between the individual channels.

The methods and procedures for the synthesis of the unified information security systems based on the use of nested convolutional codes with flexible Viterbi algorithm, as well as systems combining signals from the comb spectrum are proposed. The creation of such devices can improve the accuracy and speed of information transmission, with codec minimal redundancy, as well as efficient use of the frequency resource channel.

Keywords: computer systems and networks, information security system, adaptive coding, broadband signals, signal-code construction, the comb filter.

Відповідальний за випуск к.т.н. *М. В.Гунбін*

Підп до друку 09.12.2014 р. Формат 60 × 90 1/16. Папір офісний.
Riso-друк. Гарнітура Таймс. Ум. друк. арк. 0,9. Наклад 100 пр.
Зам. № 127. Ціна договірна.

Видавець і виготовлювач
ТОВ «Видавництво «Підручник НТУ «ХПІ»,
вул. Фрунзе, 21, м. Харків-2, 61002

Свідоцтво суб'єкта видавничої справи ДК № 3656 від 24.12.2009 р.