УДК 681.3;004.432
№ держ.реєстрації 0107U011254
Інв. № _____

Міністерство освіти і науки, молоді та спорту України
Запорізький національний технічний університет (ЗНТУ)
69063, м.Запоріжжя, вул.Жуковського, 64;
тел (0612) 224-42-36

ЗАТВЕРДЖУЮ:
Проректор з НР
д-р техн. наук, проф.
_____ Ю.М.Внуков
“___” _____ 2012 р.

З В І Т
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ
«ТЕОРЕТИЧНІ, ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ»
(заключний)

Шифр роботи шифр 04519

Завідувач каф., керівник НДР
д-р техн. наук, проф. Л.М. Карпуков

2012

СПИСОК АВТОРІВ

Керівник НДР д-р техн. наук, проф., зав. каф.	Л.М. Карпуков
доцент, канд.фіз.- мат.наук	Г.Л. Козіна
доцент, канд.фіз.- мат.наук	С.М. Романенко
доцент, канд.техн.наук	О.В. Щекотихін
доцент, канд.техн. наук	С.І. Лізунов
старший викладач	А.С. Сіренко
старший викладач	Д.М. Данильченко
старший викладач	В.В. Клочко
старший викладач	Р.Ю. Корольков
старший викладач	В.І. Слєпцов
асистент	А.О. Говоров
асистент	Г.І. Нікуліщев
асистент	Д.В. Бєліков
асистент	О.С. Гулін
асистент	С.В. Куцак

РЕФЕРАТ

Звіт: 74 стр., 9 рис., 11 табл., 52 джерела.

Мета роботи – побудова нових ефективних моделей математичного та технічного захисту інформації.

Об'єкт дослідження – комп’ютерні системи та мережі, системи передачі інформації.

В результаті НДР створено нові протоколи колективного електронного цифрового підпису, проведено дослідження криптостійкості асиметричних крипто-систем, запропоновано нові методи оптимізації параметрів волоконно-оптичних ліній зв'язку і методи захисту від інсайдерів.

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, БАГАТОРОЗРЯДНЕ ДВІЙКОВЕ ЧИСЛО, ЕЛІПТИЧНА КРИВА, АСИМЕТРИЧНА КРИПТОСИСТЕМА, КРИПТОСТІЙКІСТЬ, ВОЛОКОННО-ОПТИЧНІ ЛІНІЇ ЗВ'ЯЗКУ, ІНСАЙДЕР.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

ЕЦП	Електронний цифровий підпис
ЦВЗ	Цифровий водяний знак
ВОСП	Волоконно-оптичні системи передачі
НД	Несанкціонований доступ
СДС	Система діагностики стану
ВОТ	Волоконно-оптичний тракт
БДЧ	Багаторозрядне двійкове число
ЕД	Електронний документ
ЕК	Еліптична крива
ФПП	Фотоприйомний пристрій
ВОЛЗ	Волоконно-оптичні лінії зв'язку
ОВ	Оптичне волокно
ОК	Оптичний кабель
ЧМЗ	Частотно-модульоване зондування
ПК	Персональний комп’ютер
ОЗП	Оперативний запам’ятовуючий пристрій

ВСТУП

В останні роки в Україні, згідно із світовими тенденціями, підвищується роль електронного документообігу, а, відповідно, і його захисту. Одним з дієвих засобів захисту електронної документації є електронний цифровий підпис (ЕЦП) [1–5]. На часі разом із завданнями реалізації стандартних систем ЕЦП практичну актуальність і значущість мають реалізації колективного і групового підписів. Поняття колективного підпису співзвучне з широко відомим поняттям групового підпису, проте за своєю сутністю ці поняття різні і використовуються для побудови криптографічних протоколів, що вирішують різні завдання. У протоколі групового підпису вирішується завдання забезпечення можливості будь-якому користувачеві з деякої групи сформувати підпис від імені всієї групи, в якій є суб'єкти, наділені повноваженнями виявлення конкретних осіб, що сформували підпис, тоді як інші суб'єкти не можуть цього зробити. Колективний підпис надає можливість достатньо простої реалізації протоколів одночасного підписання контракту (електронного документа), оскільки він формується в результаті єдиного неподільного перетворення і не може бути розчленований на індивідуальні або інші урізані колективні підписи; крім того, його не можна розширити, тобто вбудувати в нього додатковий підпис ще одного або декількох користувачів [6–8].

Колективний ЕЦП має перспективи різноманітних застосувань в інформаційних системах. Зокрема, подібні схеми дозволяють істотно розширити функціональність існуючих протоколів групового підпису [9 – 11]. Для забезпечення стійкості протоколів на основі цих видів підписів слід дотримуватися правила разового використання рандомізуючих значень. Звичайний підпис в кортежі можна інтерпретувати як окремий випадок колективного ЕЦП. Рівняння перевірки звичайного і колективного ЕЦП можуть бути однаковими. Колективний підпис може також будуватися на основі загального відкритого ключа – такий вид підпису носить назву композиційного. В деяких схемах колективного і композиційного ЕЦП усувається необхідність використання довіреного посередника.

Запропоновано реалізація протоколів колективного цифрового підпису різних документів на базі стандарту електронного цифрового підпису ДСТУ 4145-2002 і з використанням операцій в простому полі [6–8, 10, 12–15]. Кожний учасник протоколу підписує свій електронний документ с використанням свого особистого ключа. Перевірка підпису здійснюється за допомогою відкритих ключів кожного із учасників. Наведені приклади обчислень за протоколами.

Стрімке збільшення в останні роки швидкодії обчислювальної техніки перейшло від фази нарощування тактової частоти до фази збільшення кількості ядер процесорів, а також розвитку багатопроцесорних систем. Все це одночасно з розвитком паралельного програмування відкриває нові можливості підвищення дії

алгоритмів, у тому числі в області криптографії. Останнім часом опубліковано чимало статей, присвячених криптографічним методам [16–19], але зовсім невелика частина з них орієнтована на паралельну реалізацію описуваних алгоритмів. З іншого боку, той же розвиток і доступність систем паралельних обчислень відкриває нові можливості й для зловмисників при зломі систем захисту інформації. Пропонується система для дослідження стійкості криптографічних систем до злому на паралельній системі [20–25].

Розвиток інформаційних технологій привів до широкого розповсюдження об'єктів інформації, представлених у цифровій формі (цифрові фотографії, аудіо-, відео- інформація, коди програм та інше). Разом з тим зросло комп'ютерне піратство – несанкціоноване поширення цифрових матеріалів. Тому актуальною є проблема надійного захисту авторського і майнового права на об'єкти інтелектуальної власності, комерційної таємниці, особистої інформації, представленої в цифровій формі, а також побудова нових моделей та методів захисту.

Одним із підходів до захисту прав інтелектуальної власності інформації, представленої в електронному вигляді, є цифрові водяні знаки. Цифрова стеганографія як наука дуже молода. Вагомий внесок в розвиток стеганографії внесли вітчизняні вчені Азаров О.Д, Шелест М.Є., Яремчук Ю.Є. , Конахович Ф.К., Пузиренко О.Ю., Хорошко В.О. Зарубіжні учені Simmons G.J., Fridrich J., а також Грибунін В.Г., Оков І.М., Турінцев І.В. та інші. Це дозволило закласти основи стеганографії, але в даній області до цього часу залишається велика кількість недосліджених питань.

Для захисту статичних цифрових зображень від підробок передбачається використовування крихких цифрових водяних знаків (ЦВЗ). Вбудовування крихких ЦВЗ надає можливість визначити, чи змінювалося зображення і якщо змінювалось, то в якій саме його частині. Крихкі ЦВЗ руйнуються при незначній модифікації зображення. Відмінність від засобів електронного підпису полягає в тім, що крихкі ЦВЗ допускають деяку модифікацію контента. Це важлива властивість, тому що законний користувач може, наприклад, стиснути зображення. Інша відмінність полягає в тім, що крихкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також визначити вигляд і місце розташування цієї зміни. Для підтвердження авторства власника цифрового зображення необхідно використовувати робастні цифрові водяні знаки. Робастні водяні знаки не повинні руйнуватися при навмисних спотвореннях зображень. Перспективним є використання гібридних методик вбудовування робастних ЦВЗ. Це дозволить забезпечити високу стійкість до поширеного діапазону методів спотворення зображень [26–30].

Сучасні системи передачі даних засновані на використанні волоконно-оптичних технологій.

Для захисту інформації в волоконно-оптичних системах передачі (ВОСП) оптимальним є використання спеціально спроектованих ВОСП на основі серійних елементів з системою фіксації несанкціонованого доступу (НД) [31–34].

Основою системи фіксації НД є система діагностики стану (СДС) волоконно-оптичного тракту. СДС можна побудувати або з аналізом минулого через волоконно-оптичний тракт (ВОТ) сигналу, або з аналізом відбитого сигналу (рефлектометричні СДС).

СДС з аналізом минулого сигналу є найбільш простий варіант діагностичної системи. На приймальній частини ВОСП аналізується минулий сигнал. При НД відбувається зміна сигналу, ця зміна фіксується і передається в передано частину ВОСП в блок керування.

Актуальною є задача виявлення та вимірювання параметрів неоднорідностей волоконно-оптичного тракту.

При передаванні інформації з використанням волоконно-оптичних ліній зв'язку на великі відстані використовують волоконно-оптичні підсилювачі і подають струм зсуву на лазерний діод для підвищення швидкодії. Струм зсуву при передаванні ”двійкового нуля”, породжує допорогове випромінювання, яке при підсилюванні ВОП призводить до прийняття ”двійкового нуля” як ”двійкову одиницю”.

Запропоновано побудову нових криптостійких методів захисту цифрової інформації з використанням цифрових водяних знаків, колективного електронного цифрового підпису (КЕЦП), а також створення розподіленої системи на базі технології J2EE для отримання оцінок криптостійкості крипто- та стегоалгоритмів. Запропоновано спосіб, який дозволяє підвищити завадостійкість ВОЛЗ.

1 АНАЛІЗ ПРАВОВИХ ТА НОРМАТИВНИХ АКТІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СЕРЕДОВИЩ. РОЗРОБКА ОРГАНІЗАЦІЙНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

1.1 Колективний і груповий ЕЦП

На часі разом із завданнями реалізації стандартних систем ЕЦП практичну актуальність і значущість мають реалізації колективного і групового підписів. Поняття колективного підпису співзвучне з широко відомим поняттям групового підпису, проте за своєю сутністю ці поняття різні і використовуються для побудови криптографічних протоколів, що вирішують різні завдання. У протоколі групового підпису вирішується завдання забезпечення можливості будь-якому користувачеві з деякої групи сформувати підпис від імені всієї групи, в якій є суб'єкти, наділені повноваженнями виявлення конкретних осіб, що сформували підпис, тоді як інші суб'єкти не можуть цього зробити. Колективний підпис надає можливість достатньо простій реалізації протоколів одночасного підписання контракту (електронного документа), оскільки вона формується в результаті єдиного неподільного перетворення і не може бути розчленована на індивідуальні або інші урізані колективні підписи; крім того, його не можна розширити, тобто вбудувати в нього додатковий підпис ще одного або декількох користувачів.

Дослідження відносяться до області електрозв'язку і обчислювальної техніки, а конкретніше до області криптографічних способів аутентифікації електронних повідомлень, що передаються по телекомунікаційних мережах і мережах ЕОМ і може бути використана в системах передачі електронних повідомлень (документів), засвідчених колективним електронним цифровим підписом (ЕЦП), представленим у вигляді багаторозрядного двійкового числа (БДЧ). Тут і далі під БДЧ розуміється електромагнітний сигнал в двійковій цифровій формі, параметрами якого є: число бітів і порядок проходження їх одиничних і нульових значень.

1.1.1 Спосіб формування і перевірки ЕЦП на базі алгоритму шифрування RSA

Відомий спосіб формування і перевірки ЕЦП на базі алгоритму шифрування RSA [2, стор. 133-134], [35, стор. 43], якій полягає в такій послідовності дій:

- формують секретний ключ у вигляді трьох простих БДЧ p, q і d, формують відкритий ключ (n, e) у вигляді пари БДЧ n і e, де n – число, що є добутком двох простих БДЧ p і q, і e – БДЧ, яке задовольняє умові: добуток e і d

порівняний з 1 за модулем добутку p і q, зменшених на 1; приймають електронний документ (ЕД), представлений БДЧ H;

- залежно від значення H і значення секретного ключа формують ЕЦП у вигляді БДЧ Q, яке дорівнює H у степені d за модулем n;
- формують перше перевірочне БДЧ A, яке дорівнює H;
- формують друге перевірочне БДЧ B, для чого БДЧ S підносять до цілочисельного ступеня e по модулю n;
- порівнюють сформовані перевірочні БДЧ A і B;
- при збігу параметрів порівнюваних БДЧ A і B роблять висновок про достовірність ЕЦП.

Недоліком цього способу є відносно великий розмір підпису і необхідність збільшення розміру підпису при розробці нових більш ефективних методів розкладання числа n на множники або при зростанні продуктивності сучасних обчислювальних пристроїв. Це пояснюється тим, що значення елементу підпису S обчислюються шляхом виконання арифметичних операцій по модулю n, а стійкість ЕЦП визначається складністю розкладання модуля n на множники p і q.

1.1.2 Спосіб формування і перевірки ЕЦП на базі алгоритму Ель-Гамаля

Відомий також спосіб формування і перевірки достовірності ЕЦП Ель-Гамаля [3, стор. 156-159], який включає такі дії:

- формують просте БДЧ p і двійкове число G, що є первісним коренем по модулю p, генерують секретний ключ у вигляді БДЧ x, залежно від секретного ключа формують відкритий ключ у вигляді БДЧ Y, яке дорівнює G піднесеному до степеня x за модулем p, приймають ЕД, представлений у вигляді БДЧ H, залежно від H і секретного ключа формують ЕЦП Q у вигляді двох БДЧ S і R;
- здійснюють процедуру перевірки достовірності ЕЦП, що включає обчислення двох контрольних параметрів з використанням початкових БДЧ p, G, Y, H і S шляхом зведення БДЧ G, Y, R в дискретний ступінь по модулю p і порівняння обчислених контрольних параметрів;
- при збігу значень контрольних параметрів роблять висновок про достовірність ЕЦП.

Недоліком даного способу також є відносно великий розмір ЕЦП. Це пояснюється тим, що значення елементів підпису S і R обчислюють шляхом виконання арифметичних операцій по модулю $(p - 1)$ і по модулю p, відповідно.

1.1.3 Спосіб формування і перевірки ЕЦП на базі алгоритму Шнорра

Відомий також спосіб формування і перевірки ЕЦП Шнорра [36, стор.53], якій полягає в такій послідовності дій:

- формують просте БДЧ p, як суму добутку N та q і одиниці, де q – просте БДЧ;
- формують просте БДЧ a, таке що $a \neq 1$ і a у степені q за модулем p дорівнює 1;
- методом генерації випадкової рівноімовірної послідовності формують секретний ключ у вигляді БДЧ x;
- формують відкритий ключ у вигляді БДЧ y, яке дорівнює a у степені x за модулем p;
- приймають ЕД, представлений БДЧ M;
- формують ЕЦП у вигляді пари БДЧ (e, s), для чого генерують випадкове БДЧ t, формують БДЧ R, яке дорівнює a у степені t за модулем, формують БДЧ e за допомогою f – деякої специфікованої геш-функції, значення якої має фіксовану довжину (звичні 160 або 256 біт), незалежно від розміру аргументу; аргументом функції виступає об'єднання двох БДЧ M та R, а потім формують БДЧ s, обчислюючи різницю t та добутку e і x за модулем q;
- формують перше перевірочне БДЧ A, для чого генерують БДЧ R' по як добуток a та y, піднесених у степені s та e відповідно, за модулем p і формують БДЧ e' за допомогою функції f від поєднання M та R';
- формують друге перевірочне БДЧ B шляхом копіювання БДЧ e;
- порівнюють сформовані перевірочні БДЧ A і B;
- при збігу параметрів порівнюваних БДЧ A і B роблять висновок про достовірність ЕЦП.

Недоліком способу є відносно висока обчислювальна складність процедури формування і перевірки ЕЦП, що пов'язано з тим, що для забезпечення мінімально необхідного рівня стійкості вимагається використовувати простий модуль p розрядністю не менше 1024 біт.

1.1.4 Спосіб формування і перевірки ЕЦП на базі алгоритму ГОСТ Р 34.10-2001

Відомий також спосіб формування і перевірки ЕЦП ГОСТ Р 34.10-2001 [37, стор. 110-111, 35], прийнятий за прототип, згідно якому ЕЦП формується у вигляді

пари БДЧ *r* і *s*, для чого генерують еліптичну криву (ЕК) у вигляді сукупності точок, причому кожна точка представляється двома координатами в декартовій системі координат у вигляді двох БДЧ, званих абсцисою (*x*) і ординатою (*y*), потім здійснюють операції генерації точок ЕК, складання точок ЕК і множення точки ЕК на число, а також арифметичні операції над БДЧ, після чого в результаті виконаних операцій формуються БДЧ r *i* s. Вказані операції над точками виконуються як операції над БДЧ, є координатами точок, по відомих формулах [37, стор. 110-111]. Операція складання двох точок А і В з координатами (x_A, y_A) і (x_B, y_B), відповідно, виконується по формулах:

$$x_C = k^2 - x_A - x_B \bmod p \text{ і } y_C = k(x_A - x_C) - y_A \bmod p, \quad (1.1)$$

де *k* визначається співвідношенням (1.2), якщо точки А і В не рівні, або співвідношенням (1.2), якщо точки А і В рівні.

$$k = \frac{y_B - y_A}{x_B - x_A} mod\, p, \quad (1.2)$$

$$k = \frac{3x_A - n}{2y_A} mod\, p. \quad (1.3)$$

Операція множення точки А на натуральне число *n* визначається як багатократне складання точки А.

Результатом множення будь-якої точки ЕК на нуль визначається точка **О**, що є нескінченно віддаленою точкою. Дві точки А з координатами (*x*, *y*) і –А з координатами (*x* –*y*) називаються протилежними. Множення на ціле негативне число –*n* визначається через множення протилежної точки на число *n*. За означенням приймають, що сума двох протилежних точок рівна нескінченно віддаленій точці **О**.

Генерується ЕК, що описана рівнянням (1.4):

$$y^2 = x^3 + ax + b \bmod p. \quad (1.4)$$

Тобто генеруються числа *a*, *b* і *p*, яки є параметрами ЕК і однозначно задають множину точок ЕК, абсциса і ордината кожної з яких задовольняє вказаному рівнянню. Спосіб працює таким чином:

- генерують ЕК, яка є сукупністю пар БДЧ, званих точками ЕК, що володіють певними властивостями;

- методом генерації випадкової рівноімовірної послідовності формують секретні ключі у вигляді БДЧ $k_1, k_2, \ldots, k_n$;
- формують відкриті ключі у вигляді точок ЕК $P_1, P_2, \ldots, P_n$, для чого генерують точку G, що має простий порядок q (порядком точки ЕК називається якнайменше позитивне ціле число q, таке що результатом множення даної точки на число q є так звана нескінченно віддалена точка **O**; результатом множення будь-якої точки ЕК на нуль за означенням є точка **O** [37, стор. 98-105]), і обчислюють відкриті ключі шляхом множення точки G на БДЧ $k_1, k_2, \ldots, k_n$;
- приймають ЕД, представлений БДЧ H;
- генерують випадкове БДЧ t в рамках від 0 до q, по якому формують точку R шляхом множення t на G;
- формують ЕЦП Q у вигляді пари БДЧ (r, s), для чого генерують БДЧ r, беручи за модулем q число x_R – абсцису точки R, а потім генерують БДЧ s по формулі (1.5):

$$s = (tH + rk_i) \bmod q, \tag{1.5}$$

де i - індекс, який послідовно приймає значення від 0 до n;

- формують перше перевірочне БДЧ A, для чого генерують БДЧ v п як добуток s і H^{-1} за модулем q, і БДЧ w як різницю q і добутку r та H^{-1} за модулем q, потім генерують точку R′ як суму добутків v та G і w та P_i, після чого БДЧ A отримують, беручи $x_{R'}$ (абсцису точки R′)за модулем q;
- формують друге перевірочне БДЧ B шляхом копіювання БДЧ r;
- порівнюють сформовані перевірочні БДЧ A і B;
- при збігу параметрів порівнюваних БДЧ A і B роблять висновок про достовірність ЕЦП.

Недоліком цього способу є зростання розміру колективної ЕЦП. Тобто ЕЦП, встановлюючій факт підписання деякого заданого документа двома і більш користувачами, пропорційно числу підписувачів заданого ЕД, тому що кожний користувач формує ЕЦП, яка не залежить від ЕЦП інших користувачів.

В основу дослідження поставлене завдання розробки способу формування і перевірки достовірності колектиного ЕЦП, якій засвідчує ЕД, є залежним від довільної сукупності секретних ключів користувачів і має фіксований розмір. Тобто розмір не залежить від числа користувачів, яким належить даний колективний підпис, завдяки чому зменшується розмір колективного ЕЦП.

Поставлене завдання досягається тим, що у відомому способі формування і перевірки достовірності ЕЦП для засвідчення ЕД, полягаючому в тому, що генерують сукупність з $n \geq 2$ секретних ключів у вигляді багаторозрядних двійкових чисел $k_1, k_2, \ldots, k_n$, по секретних ключах формують n відкритих ключів $P_1, P_2, \ldots, P_n$, відповідно, приймають, принаймні, один електронний документ,

представлений багаторозрядним двійковим числом H, залежно від прийнятого електронного документа і від значення, принаймні, одного секретного ключа формують колективний електронний цифровий підпис Q у вигляді двох або більш багаторозрядних двійкових чисел, формують перше A і друге B перевірочні багаторозрядні двійкові числа, порівнюють їх і при збігу їх параметрів роблять висновок про достовірність колективного електронного цифрового підпису, причому додатково генерують колективний відкритий ключ залежно від m відкритих ключів P_{α_1}, P_{α_2}, …, P_{α_m}, де α_1, α_2, …, α_m – натуральні числа, m береться в рамках від 2 до n, α_j не більше n і $j = 1, 2, \ldots, m$, причому, принаймні, одне з перевірочних багаторозрядних двійкових чисел формують залежне від колективного відкритого ключа.

Системи електронного цифрового підпису використовуються для забезпечення цілісності й автентичності оброблюваної й переданої інформації. Кожний абонент в таких системах має два ключі - секретний і відкритий, які повинні бути пов'язані один з одним співвідношенням, що не дозволяє за прийнятний час знайти секретний ключ по відкритому [4, 35, 36]. Час підбору секретного ключа по відкритому залежить від параметрів співвідношення.

Розвиток методів прискорених обчислень, у тому числі застосування багатопроцесорних систем паралельних рішень створює небезпеку зниження ступеня захисту систем електронного цифрового підпису. Тому для оцінки надійності систем захисту та їх удосконалювань необхідне вивчення ефективності застосування методів паралельних обчислень для злому секретного ключа.

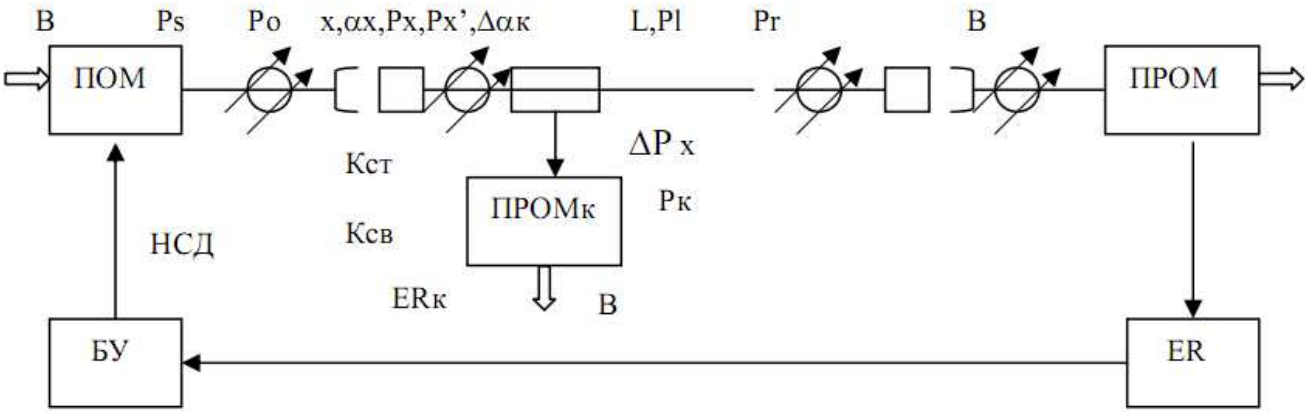
1.2 Аналіз способів захисту від НД в ВОСП

Для захисту інформації в ВОСП оптимальним є використання спеціально спроектованих ВОСП на основі серійних елементів з системою фіксації НД [31–34].

Основою системи фіксації НД є СДС волоконно-оптичного тракту. СДС можна побудувати або з аналізом минулого через ВОТ сигналу, або з аналізом відбитого сигналу (рефлектометричні СДС).

СДС з аналізом минулого сигналу є найбільш простий варіант діагностичної системи. На приймальній частини ВОСП аналізується минулий сигнал. При НД відбувається зміна сигналу, ця зміна фіксується і передається в передано частину ВОСП в блок керування.

При використанні аналізу коефіцієнта помилок на приймальному модулі ВОСП (рис. 1.1) СДС реалізується при мінімальних змінах апаратури ВОСП, практично всі необхідні модулі є в складі апаратури ВОСП. Недоліком є відносно низька чутливість до змін сигналу.

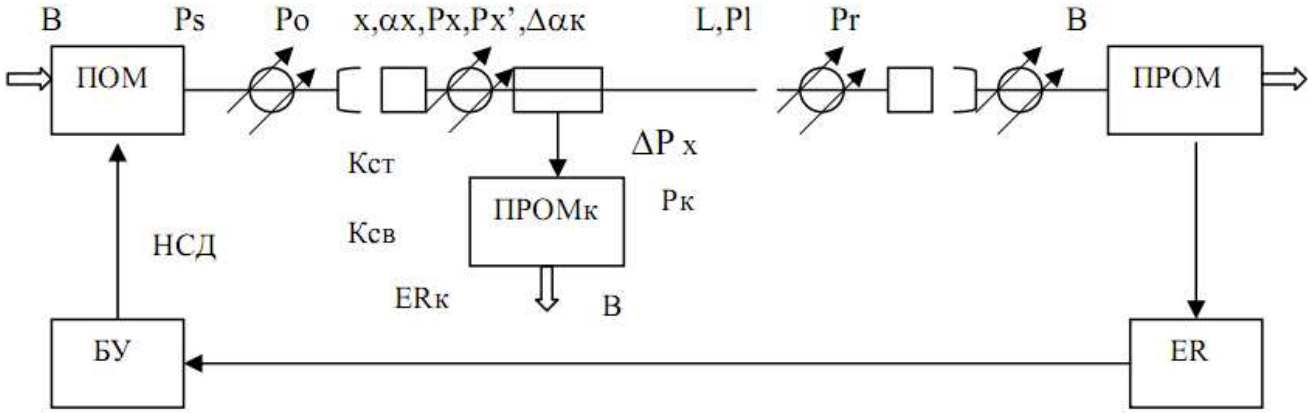


Ps - сигнал, що зондує на виході джерела оптичного сигналу;
Po - сигнал, що зондує на вході ВОТ;
Pr - відбитий сигнал на вході приймача рефлектометру;
Кст, Ксв – коефіцієнти зв'язку;
ПОМ – передавальний оптичний модуль;
ПРОМ - приймальний оптичний модуль;
ПРОМк – проміжний приймальний оптичний модуль;
БУ – блок управління;
ER – діагностичний модуль.

Рисунок 1.1 - ВОСП з системою діагностики аналізу коефіцієнта помилок

Для підвищення чутливості до складу СДС з аналізом минулого сигналу необхідно використовувати фото прийомний пристрій (ФПП) з граничною чутливістю не гірше 10 пВт і нелінійного перетворення не гірше 0.0001, а також забезпечувати високу стабільність передаючого блоку СДС, або організовувати роботу з опорним каналом і вимірювати відношення оптичних сигналів.

Основним недоліком СДС з аналізом минулого сигналу є відсутність інформації про координати з'явившоїся неоднорідності, що не дозволяє проводити більш тонкий аналіз змін режимів роботи ВОСП для зняття помилкових спрацьовувань системи фіксації НД. По мірі вдосконалення техніки вимірювання оптичного сигналу, збільшення чутливості ФПП ВОСП, ФПП пристрої НД та СДС все складніше буде розділяти вплив при НД від природних флуктуацій параметрів ВОСП, при цьому буде збільшуватися ймовірність помилкових спрацьовувань системи фіксації НД. СДС з аналізом відбитого сигналу (рефлектометричні СДС) дозволяють найбільшою мірою підвищити надійність ВОСП. У ВОСП на передавальному кінці (рис. 1.2) до ВОТ за допомогою оптичного розгалуджувачу підключається апаратура оптичного рефлектометру. Контроль стану волоконно-оптичного тракту дозволяє при цьому виявляти неоднорідності, які з'явилися, аналіз яких дозволяє фіксувати НД, що викликали цю неоднорідність.



Ро - сигнал, що зондує на вході ВОТ;
Ps - сигнал, що зондує на виході джерела оптичного сигналу;
Pr - відбитий сигнал на вході приймача рефлектометру;
Кст, Ксв – коефіцієнти зв'язку;
ПОМ – передавальний оптичний модуль;
ПРОМ - приймальний оптичний модуль;
ПРОМк – проміжний приймальний оптичний модуль;
БУ – блок управління;
ER – діагностичний модуль

Рисунок 1.2 - ВОСП з рефлектометричними системами діагностики стану ВОТ

При цьому сигнал тривоги «НД» виробляється в блоці передавальної апаратури і знімається проблема передачі цього сигналу для управління ВОСП. Найважливішою перевагою є можливість визначення координати місця передбачуваного НД.Апаратура оптичного рефлектометру є основою СДС з аналізом відбитого сигналу. В даний час найбільш розвинений метод імпульсного рефлектометру (OTDR). Основною перевагою СДС з аналізом відбитого сигналу на основі методу імпульсної рефлектометра є висока ступінь технічної проробки (серійно випускаються прилади).

В даний час оптичні рефлектометри мають динамічний діапазон вимірювання до 46 дБ для $\lambda = 1.3$ мкм і 41.5 дБ для $\lambda = 1.55$ мкм. До складу рефлектометру, крім джерела потужного сигналу малої тривалості, який зондує, фотоприймач і розгалужувач входить потужний блок обробки, що забезпечує широкі функціональні можливості приладів (отримання, обробку, запис, зберігання та аналіз рефлектограм).

1.2.1 Рефлектометричні методи вимірювання параметрів волоконно-оптичних ліній зв’язку (ВОЛЗ)

В даний час при вимірі загасання волоконно-оптичного тракту ВОЛЗ використовується метод оптичної рефлектометру і метод внесених втрат. У другому випадку значення загасання ВОТ визначається по відношенню оптичних сигналів на вході і виході тракту. При цьому обладнання (оптичні тестери) є простим і дешевим, а затухання ВОТ визначається надійно і з хорошою точністю.

Однак при необхідності більш детального аналізу стану волоконно-оптичного тракту використовуються рефлектометричні методи. Рефлектометричні методи забезпечують перевірку цілісності оптичного волокна, вимірювання довжини оптичного волокна, визначення відстані до місця неоднорідності (обриву) оптичного волокна, визначення величини втрат у місцях неоднорідності оптичного волокна (нероз'ємних і роз'ємних з'єднувачів), контроль процесу монтажу (зварювання) оптичних кабелів, визначення загасання і коефіцієнта загасання оптичного волокна та ін.

Всі оптичні рефлектометри мають власне програмне забезпечення для занесення обмірюваних параметрів магістралі у внутрішню пам'ять чи гнучкий магнітний диск, з можливістю друкування результатів вимірювань на зовнішньому (вбудованому) принтері.

Удосконалення оптичних рефлектометрів йде в напрямку збільшення динамічного діапазону, довжини вимірювання оптичного волокна, дозволеної відстані загасання, об'єму пам'яті та інших сервісних функцій.

Виміри можна проводити з одного кінця волоконно-оптичного тракту, а результати вимірювань наочно представляти у графічному вигляді (рис. 1.3).

Основними достоїнствами методу оптичного рефлектометру є:

- велика інформативність (вимірюється розподіл загасання вздовж ВОЛЗ);
- доступ до одного входу ВОЛЗ.

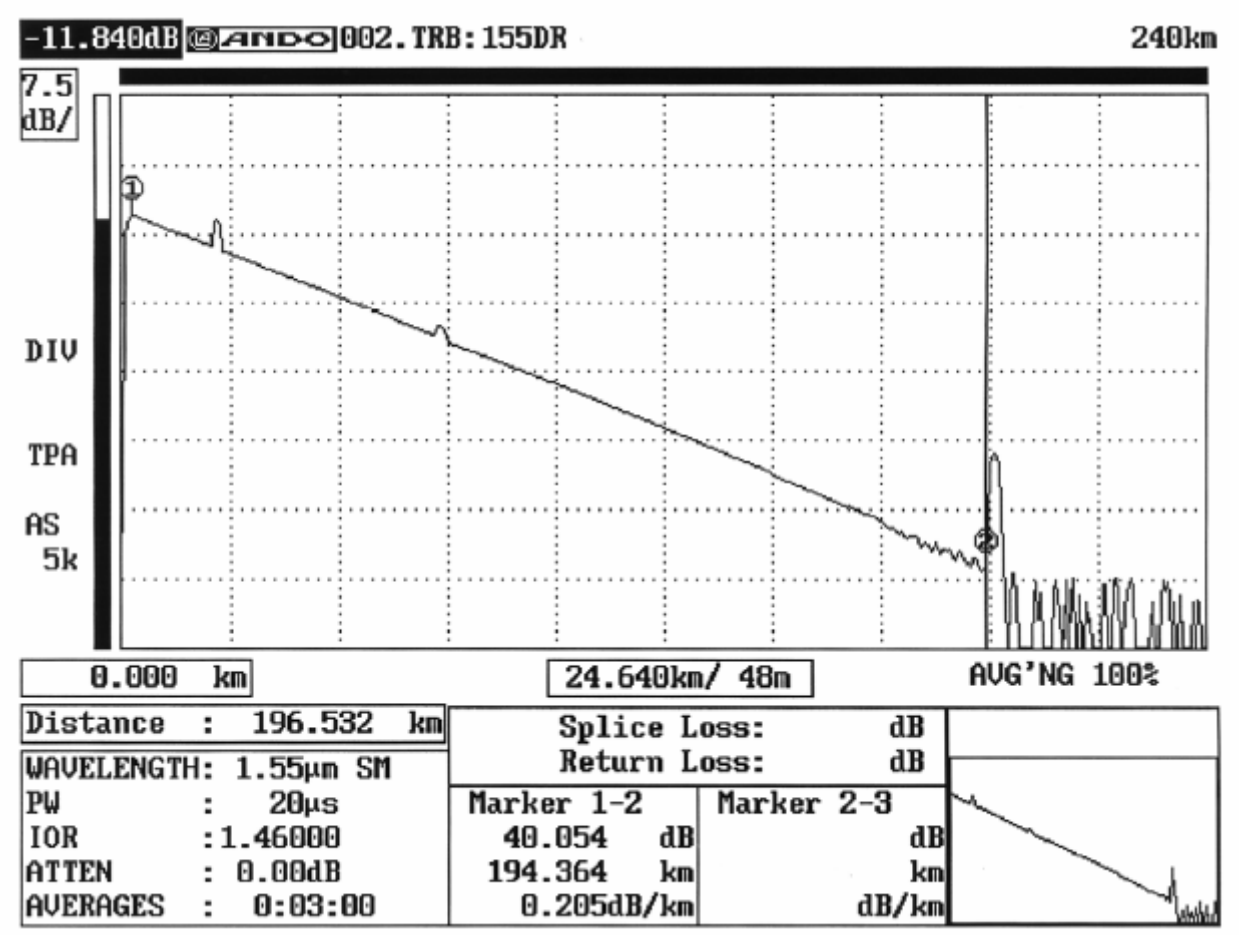
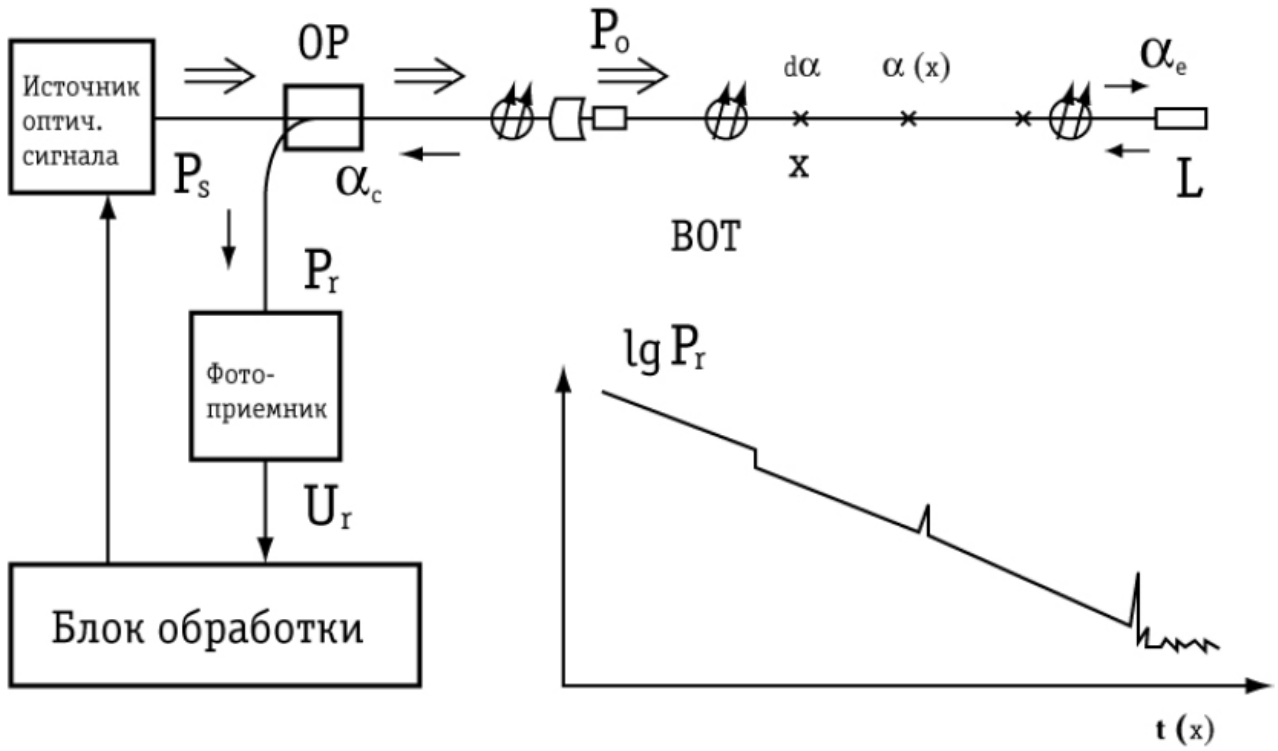


Рисунок 1.3 - Рефлектограма волоконно-оптичного тракту довжиною 200 км

Метод оптичного рефлектометру дозволяє ефективно вимірювати всі основні параметри волоконно-оптичного тракту ВОЛЗ. Найважливішою перевагою методу є можливість виявляти і аналізувати неоднорідності волоконно-оптичного тракту, що в умовах експлуатаційного обслуговування дозволяє не тільки виявляти несправності, але прогнозувати їх.

Принцип оптичного рефлектометру заснований на зондуванні досліджуваного оптичного волокна пробним оптичним сигналом Pp та аналізі відбитого в волоконно-оптичному тракті оптичного сигналу Pr (t) (рис. 1.4).



Ps - сигнал, що зондує на виході джерела оптичного сигналу;

Po - сигнал, що зондує на вході ВОТ;

Pr - відбитий сигнал на вході приймача рефлектометру;

Ur - сигнал на виході фотоприймача;

αc, αe - втрати сигналу, що зондує і відбитого сигналу на оптичному розголуджувачі;

ОР-оптичний розгалуджувач;

L – довжина тракту;

ВОТ – волоконно-оптичний тракт

Рисунок 1.4 - Метод оптичного рефлектометру

Пробний сигнал, що зондує Рр у оптичному волокні змінюється за рахунок втрат:

$$Pp(x) = Po \exp(-\mu x) = Po\ 10^{-0.1 \alpha x}, \quad (1.2)$$

де Po - потужність сигналу, що зондує, на вході оптичного волокна;

μ - коефіцієнт загасання (НП / м);

α - коефіцієнт загасання (дБ / м);

μ = 0,23 α.

Втрати оптичного сигналу відбуваються за рахунок поглинання в матеріалі оптичного волокна і розсіювання на його неоднорідності. На відстані x від початку оптичного волокна, при Δx <<x, втрати сигналу ΔР рівні:

$$\Delta P\ (\Delta x) = P\ x\ \Delta x\ \mu r + Px\ \Delta x\ \mu l = \Delta PR\ (\Delta x) + \Delta Pl\ (\Delta x), \qquad (1.3)$$

де μr - коефіцієнт загасання, пов'язаний з розсіянням;

μl - коефіцієнт загасання, пов'язаний з поглинанням;

Δx - просторовий дозвіл.

В даний час технологія виробництва оптичного волокна (ОВ) і оптичного кабелю (ОК) забезпечує мінімальні втрати які пов'язані з поглинанням та з розсіянням. Складова втрат на розсіювання визначається релеевським розсіянням оптичного сигналу на мікронеоднорідностях оптичного волокна.

Частина розсіяного релеевского dPR сигналу ΔPR (Δx) захоплюються оптичним волокном і поширюється в ОВ назустріч зондирующему сигналу Pp (рис.1.5).

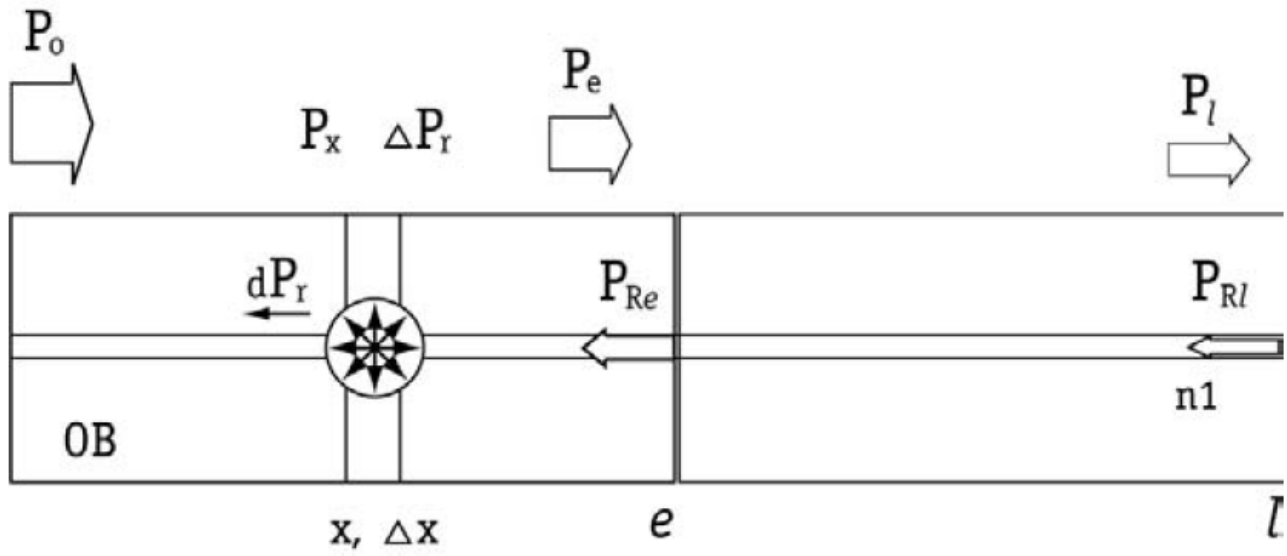


Рисунок 1.5 - Втрати і зворотне розсіювання сигналу в ОВ

Величина зворотньорозсіяного релеевского сигналу dPR залежить від фактора зворотнього розсіювання S:

$$dPR = \Delta P\ (\Delta x)\ S. \qquad (1.4)$$

Фактор зворотного розсіювання в основному залежить від числової апертури ОВ і приблизно дорівнює:

S = - 30 дБ, для одномодових волоконних світловодів;

S = - 23 дБ, для багатомодового волоконних світловодів.

Можна ввести коефіцієнт зворотнього релеевського розсіювання, який залежить від довжини ділянки ОВ - Δx, від загасання - μr (складової, пов'язаної з розсіянням) і від фактора зворотного розсіювання - S:

$$GR = \Delta x \, \mu r \, S. \quad (1.5)$$

Тоді

$$dPR(x) = GR \, Px. \quad (1.6)$$

Потужність зворотнього розсіяного сигналу в ОВ пропорційна потужності сигналу, що зондує, в даній точці оптичного волокна

Таким чином, вимірюючи відбитий сигнал dPR (x), можна відновити еволюцію сигналу Pp, що зондує і потім визначити всі необхідні параметри ВОТ: коефіцієнт загасання α та його розподіл вздовж ВОТ α (x), сумарне затухання αL і втрати в з'єднувачі dα. З розподілу загасання визначаються координати неоднорідностей, зварювання та обриву ОВ.

Для відновлення розподілу сигналу Pp(x) в рефлектометричних методах відбитий сигнал вимірюють з урахуванням затримки τ яку має відбитий сигнал щодо зондірующего з урахуванням проходження зондірующего сигналу у прямому напрямку і відбитого сигналу в зворотньому:

$$\tau = 2nx / C, \quad (1.7)$$

де n - показник заломлення серцевини ОВ;

c - швидкість світла у вакуумі;

x - координата, від початку ВОТ, відповідна затримці.

Затримка відбитого сигналу 10 нс відповідає відстані 1 м , 2.5 мс - 250 км (таблиця 1.1).

Таблиця 1.1 - Затримка відбитого сигналу до ВОТ

Параметр	Значення							
τ	1 нс	10 нс	0,1 мкс	1 мкс	10 мкс	20 мкс	1 мс	2,5 мс
x	0,1 м	1 м	10 м	100 м	1 км	2 км	100 км	250 км

Отже, у методі оптичного рефлектометру в тестовому ОВ вводять оптичний сигнал, що зондує.

Частина релеевского розсіяного сигналу відбивається і відбитий сигнал вимірюється. Аналіз відбитого сигналу в залежності від затримки щодо зондірующего сигналу і дозволяє знайти еволюцію оптичного сигналу вздовж волоконно-оптичного тракту, а потім всі необхідні його параметри.

Основні проблеми оптичного рефлектометру.

При розробці оптичного рефлектометру необхідно враховувати наступне.

Оптичний рефлектометра повинен забезпечувати вимір відображених сигналів мінімальних рівнів потужності.

Коефіцієнт зворотного релеевського розсіювання Gr безпосередньо залежить від довжини хвилі зондірующего випромінювання як λ-4. Тому при збільшенні довжини хвилі значення μr зменшується, зменшується і Gr.

Відбитий сигнал додатково і досить істотно знижується за рахунок подвійного загасання в волоконно-оптичному тракті. При сумарному затухання ВОТ 2αL = 90 дБ з урахуванням Gr = -70 дБ, затухання зондірующего відбитого сигналу досягає 160 дБ.

Динамічний діапазон приймальної частини рефлектометру повинен бути не менше 2αL (не менше 90 дБ).

Крім розподіленогорелеевского розсіювання в назад розсіяному сигнал присутні відбиття від точкових неоднорідностей, найважливішим з яких є френелєвське відображення.

Френелєвське відображення присутнє на межі двох середовищ, що мають різні показники заломлення n1, No.

Відбитий френелевскій сигнал PF дорівнює:

$$PF = ((n1-No) / (n1-No)) \, 2 \, Px = GF \, Px. \qquad (1.8)$$

Для границі оптичне волокно-повітря (n1 = 1.4, No = 1) Gf = 4% = -14 дБ

Таблиця 1.2 - Коефіцієнт зворотного релеевского розсіювання і співвідношення френелевского і релеевского сигналів для різних просторових дозволів

Параметр	Значення			
Δx, м	1	10	100	1000
Gr, дБ	-73	-63	-53	-43
Gf/Gr, дБ	60	50	40	30

Великий френелевскій сигнал значною мірою ускладнює роботу рефлектометра. В першу чергу це пов'язано з тим, що фотоприймача рефлектометра входить в режим насичення, що призводить до неможливості проводити виміру - з'являються «мертві зони», тобто ділянки, де помилки вимірювань перевищують допустимий рівень.

Отже, принцип дії оптичних рефлектометра полягає в тому, що в оптичне волокно (ОВ) направляється оптичний сигнал, що зондує і вимірюється відбитий сигнал, який є результатом зворотного релеевского і френелевского отражений зондіруючего сигналу. Аналіз затримки відбитого сигналу щодо зондіруючего і дозволяє відновити еволюцію зондіруючего сигналу вздовж вимірюється тракту і отримати всі необхідні параметри (сумарнезатухання, розподіл коефіцієнта загасання і зворотні втрати тракту, координати неоднорідностей, оптичні втрати і коефіцієнти відображення внеоднорідності). В оптичної рефлектометра використовуються два основних методу. Це метод імпульсної рефлектометра - метод OTDR (optical timedomain reflectometer), тобто рефлектометра з аналізом у часовій області та метод частотної рефлектометра, метод частотно-модульованого зондування (ЧМЗ) - метод OFDR (optical frequency domain reflectometer), тобто . рефлектометра з аналізом в частотної області.

1.2.2 Метод класичної OTDR

У методі імпульсної рефлектометрії (рiс.1.6) у досліджуваний волоконно-оптичний тракт вводиться короткий оптичний імпульс тривалістю Δt і потужністю Ps. Цей сигнал P (x), поширюючи в тракті загасає за рахунок розподілених втрат α в оптичному волокні (ОВ) і за рахунок втрат нанеоднорідності Δα (у місцях зварювання, в рознімних судинних і пр). Частина зондіруючего сигналу, що визначається коефіцієнтами зворотногорелеевского рассеяния GR та френелевского відображення GF, поширюється в протилежному напрямку.

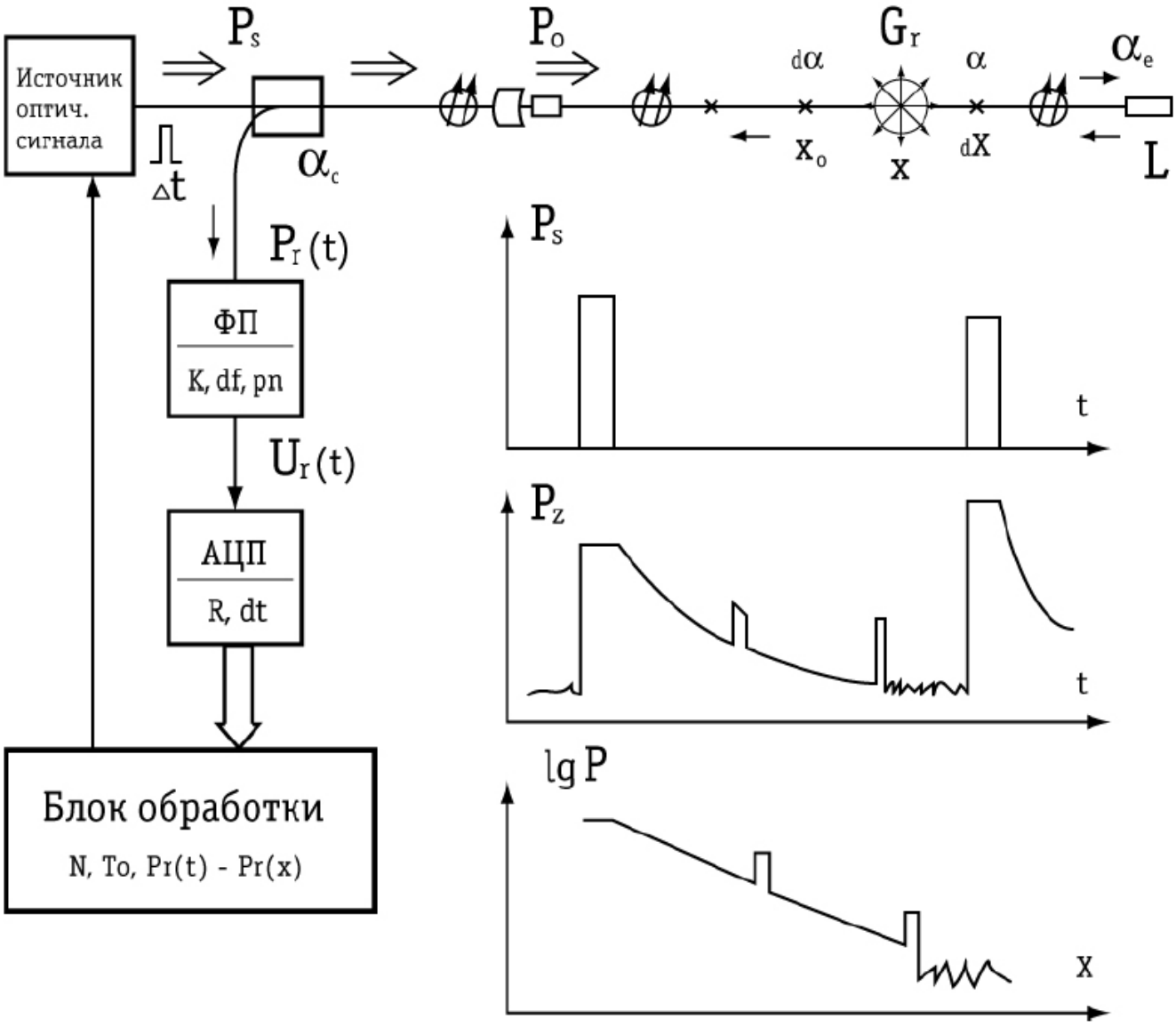


Рисунок 1.6 - Метод імпульсної рефлектометрії

Через фотоприемное пристрій (ФПП) та аналого-цифровий перетворювач (АЦП) відбитий сигнал Pr (t) у вигляді цифрової інформації надходить в блок обробки, де перетворюється у функцію Pr (x) = GR P (x) α c, Вт:

$$GR = \mu r \, S\Delta x \qquad (1.9)$$

де μr - складова коефіцієнта загасання, пов'язана з розсіянням;

S - фактор зворотного розсіювання ОВ;

Δx - довжина ОВ, з якою збирається сигнал PR;

αc - втрати на оптичному розгалуджувачі.

Для переходу від тимчасової залежності відбитого сигналу до розподілу Pr (x) використовується залежність:

$$x = (c/2n)\, t, \qquad (1.10)$$

де x - відстань від початку ОВ,

t - затримка відбитого сигналу щодо зондирующего,

c - швидкість світла в вакуумі,

n - показник заломлення серцевини ОВ

1.2.3 Дзеркальний релеевський сигнал. Вплив дозволу на величину релеевського відбитого сигналу

Проблеми оптичної рефлектометра, і методу OTDR зокрема, пов'язані з малою величиною відбитого сигналу. На вхід ФПП надходить сигнал,відбитий від різних ділянок ОВ вимірюється як:

$$Pr(x) = Ps - \alpha c - 2\alpha x + GR, \text{ дБм}, \quad (1.11)$$

де Ps - потужність на виході джерела оптичного зондирующего сигналу, дБм;

αc - втрати зондирующего і відображених сигналів в оптичному Разветвитель, дБ;

2αx - втрати зондирующего і відображених сигналів у волоконно - оптичному тракті до ділянки з координатами x, дБ;

GR - коефіцієнт зворотного релеевского розсіювання, дБ.

Типові значення параметрів наступні: Ps = 10 дБм .... 20 дБм, αc = 6 дБ.

Коефіцієнт зворотного релеевского рассеяния вносить значний вклад в зменшення відбитого сигналу (для Δ x = 1 м , Λ = 1,55 мкм і волокна фірмиCorning GR = - 73 дБ).

Друга причина зменшення відбитого сигналу - це втрати сигналу при проходженні тракту. Дзеркальний сигнал (в дБм) лінійно зменшується при збільшенні довжини аналізованого тракту і при x = L (L - довжина тракту) він мінімальний Prmin:

$$Prmin(L) = Ps - \alpha c - 2\alpha L + GR, \text{ дБм}. \quad (1.12)$$

Оцінки для Ps = 20 дБм та 2αL = 90 дБ дають величину Prmin = -150 дБм (Prmin = 10-18 Вт, т. Е. Порядка 10 фотонів / с)

Для збільшення релеевского відбитого сигналу, який і дозволяє визначити характеристики ОВ, доводиться збільшувати Δx - ділянка тракту, з якого збирається відбитий сигнал, т. Е доводиться збільшувати (погіршувати) дозвіл приладу.

Для обліку впливу Δx на параметри рефлектометра введемо GR0 - коефіцієнт зворотного релеевского розсіювання при Δx = Δx0:

$$Gr = Gr0 + 10 \log (\Delta x. \Delta x0) \text{ [дБ]}, \quad (1.13)$$

Тоді залежність величини релеевского відбитого сигналу від дозволу рефлектометра має вигляд:

$$Pr (x, \Delta x) = Ps - \alpha c - 2\alpha x + GR0 + 10 \log (\Delta x / \Delta x\ 0) \text{ [дБм]}. \quad (1.14)$$

При вимірах необхідно забезпечити співвідношення сигнал / шум більше одиниці, тобто Pr (x)більше або дорівнюєPn. Це співвідношення і визначає динамічний діапазон рефлектометра:

$$D = \alpha L = 0.5 [Ps - \alpha c + GRo + 10 \log (\Delta X / \Delta Xo) - Pn], \text{ дБ} \quad (1.15)$$

Таким чином, для збільшення відбитого сигналу необхідно підвищувати вводиться в ОВ оптичну потужність зондирующего сигналу, знижувати втрати в Разветвитель і збільшувати дозвіл. Збільшення Ps обмежено можливостями лазера та вимогами безпеки обслуговуючого персоналу, а також порогом виникнення нелінійних ефектів у ОВ.

1.2.4 Шуми фотоприємного пристрою і вимірювання затухання

При вимірах необхідно забезпечити, щоб мінімальний відбитий сигнал був більше шумів ФПП:

$$Prmin \geq Pn \quad (1.16)$$

У методі оптичної рефлектометра, як показано вище, мінімальний рівень відображуваного релеевского сигналу на вході ФПП визначається потужністю зондирующего оптичного сигналу Ps і втратами в Разветвитель αc, а також типом ОВ і довжиною хвилі зондування - GR і роздільною здатністю приладу Δx.

У методі OTDR рівень шумів ФПП залежить від дозволу Δx. Справа в тому, що в цьому методі дозвіл визначається тривалістю зондирующего імпульсу:

$$\Delta x = (c / 2n) \Delta t. \quad (1.17)$$

При цьому необхідно забезпечити смугу пропускання ФПП не менше:

$$\Delta f = 1/\Delta t = (c/2n\ \Delta x). \quad (1.18)$$

При поліпшення дозволу Δx необхідно зменшувати тривалість зондирующего імпульсу, розширювати смугу пропускання ФПП, а це викликає збільшення шумів Pn, які можна оцінювати як:

$$Pn = pn\ (\Delta f)\ 1 / 2, \quad (1.19)$$

де pn - спектральна щільність шуму, В т (Гц) -1 / 2.

Для зменшення шумів необхідно використовувати ФПП з мінімальною pn і звужувати смугу пропускання Δf.

У таблиці 1.3 наведені оцінки необхідної тривалості зондирующего імпульсу, смуги пропускання ФПП та потужності шуму в залежності від дозволу для спектральної щільності pn = 1·10-14 В т (Гц) -1 / 2

Таблиця 1.3 - Тривалість зондирующего імпульсу

Параметр	Значення				
Δx, м	1	10	100	1000	2000
Δt, нс	10	100	1000	10000	20000
Δf, МГц	100	10	1	0,1	0,05
Pn, пВт	100	30	10	3	2

Для обліку впливу Δx введемо Pn0 - приведені до входу оптичні шуми ФПП при заданому дозволі Δx0. Тоді Pn = Pno - 5 log (Δ x o / Δx) і максимальна величина вимірюється загасання тракту - динамічний діапазон рефлектометра визначається як:

$$\alpha L \leq 0.5\ x\ (Ps - Pno - \alpha c + GRo + 15\ log\ (\Delta x / \Delta xo))\ [дБ], \quad (1.20)$$

У таблиці 1.4 наведені оцінки динамічного діапазону OTDR (Δxo = 1м, GRo = - 73 дБ; Pno = - 70 дБм; Ps = 20 дБм; αc = 6 дБ) для різних дозволів.

З таблиці 1.4 видно, що при великих Δx рефлектометра забезпечує вимірювання волоконно-оптичного тракту з непоганими параметрами (Δx = 2 км , AL = 30 дБ), але при поліпшенні дозволу допустиму затухання тракту значно зменшується, при Δx = 1м αL всього 5.5 дБ.

Таблиця 1.4 - Оцінки динамічного діапазону OTDR

Параметр	Значення				
Δx, м	1	10	100	1000	2000
15 log (Δx / Δxo), дБ	0	15	30	45	49,5
Gr, дБ	-73	-63	-53	-43	-40
Pn, пВт	100	30	10	3	2
αL, дБ	5,5	13	18,5	28	30

Сучасні OTDR успішно вирішують завдання зниження шумів ФПП і відповідно підвищення величини вимірюється загасання. При цьому використовується той факт, що параметри тракту квазіпостоянни, а отже сигнал Pr (x) за час змін не змінюється і усереднення сигналу при накопиченні забезпечує зниження шумів приймальні частини.

При цьому зондіруючіе імпульси посилаються постійно з періодом Tm не меншим ніж величина подвоєного добутку n та L, поділеного на c. Сигнали від кожної точки P (x i) сумуються в блоці обробки і ростуть як NP (xi), а шуми як Pn у вигляді усередненого за N значення Pn0 за винятком1/2, де N - число усереднення. Накопичення сигналу еквівалентно зменшенню смуги пропускання.

Таким чином, для OTDR величина вимірюється загасання тракту визначається як:

$$\alpha L \leq 0{,}5 \text{ x } (Ps - \alpha c + GRo - Pno - 15\log (\Delta x / \Delta xo) + 5\log (N)) \text{ [дБ]}, \quad (1.21)$$

Видно, що динамічний діапазон αL залежить від типу ОВ і довжини хвилі зондіруючого випромінювання, а також від необхідного дозволу. Для збільшення динамічного діапазону необхідно збільшувати вводиться в ОВ оптичну потужність, знижувати втрати в Разветвитель і використовувати ФПП з мінімальними шумамі. Крім цих параметрів рефлектометра необхідно також оптимізувати режим його роботи - вибирати оптимальне значення роздільної здатності та числа усереднення.

Таблиця 1.5 - Затухання тракту Δα

Код	Значення								
K	8	10	12	14	16	18	20	22	24
N	256	1024	4096	16384	65536	262144	1048576	4194304	16777216
Δα, дБ	6	7,5	9	10,5	12	13,5	15	16,5	18
To, с	0,6	2,5	10	40	160	660	2640	10800	43200

У таблиці 1.5 наведені оцінки збільшення вимірюється загасання тракту Δα, часу вимірювання (обробки) при накопиченні To (при L = 250 км). У таблиці 1.6

наведені значення для динамічного діапазону для OTDR при Δxo = 1м, GRo = - 73 дБ; Pno = - 70 дБм; Ps = 20 дБм; αc = 6 дБ, N = 216 для різних дозволів Δx

Таблиця 1.6 - Значення динамічного діапазону OTDR

Параметр	Значення				
Δx, м	1	10	100	1000	2000
αL, дБ	17,5	25	32,5	40	42

Висновки. Основними проблемами імпульсної рефлектометра було значне зниження динамічного діапазону при підвищених вимогах на просторовий дозвіл. При цьому динамічний діапазон зменшується як за рахунок зменшення відображуваного релеевского сигналу, так і за рахунок збільшення шумів ФПП при розширенні смуги пропускання.

У сучасних OTDR успішно вирішені зазначені вище проблеми. Використання малошумящіх фотоприємних пристроїв, швидкодіючих АЦП і обчислювальної техніки дозволило створити високоефективні вимірювальні прилади. При цьому вирішальне умова успіху - використання можливостей сучасної обчислювальної техніки. Це, по-перше, попередня обробка, цифрове накопичення сигналу, що дозволило значно знизити рівень шумів і підвищити динамічний діапазон рефлектометра. Вторинна обробка отриманих рефлектограмм розширила функціональні можливості рефлектометра.

В даний час оптичні рефлектометри мають динамічний діапазон вимірювання до 45 дБ і просторовий дозвіл у кілька метрів. До складу рефлектометру крім джерела потужних зондірующіх імпульсів малої тривалості, розгалуджувач, ФПП і АЦП входить блок обробки, що забезпечує розширення функціональних можливостей приладу (отримання, обробку, запис, зберігання та аналіз рефлектограмм). При цьому забезпечується як вимірювання коротких оптичних шнурів, так і контроль тракту довжиною понад двісті кілометрів. Таким чином, сучасні імпульсні рефлектометра, володіючи високими параметрами, успішно вирішують завдання вимірювання параметрів волоконно-оптичного тракту при монтажі і, значною мірою, при експлуатації ВОЛЗ. Але підвищення параметрів у OTDR в основному забезпечується накопиченням сигналу і роботою з просторовим дозволом на межі допустимого (найбільшого з можливих Δ x).

2 АНАЛІЗ МЕТОДІВ ПОШУКУ ОПТИМАЛЬНИХ РІШЕНЬ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ І РОЗРОБКА ТЕОРЕТИЧНИХ ОСНОВ МАТЕМАТИЧНИХ ТА ТЕХНІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Розвиток інфраструктури відкритих ключів в Україні, створення регіональних центрів сертифікації ключів дозволяє клієнтам отримати та надавати послуги електронного цифрового підпису [1]. Крім класичної схеми однократного цифрового підпису існують інші схеми, зокрема колективний цифровий підпис.

На сьогодні з'явилися нові схеми колективного цифрового підпису в різних постановах. Наприклад, колективний цифровий підпис може бути сформований під одним електронним документом, який завіряє деяка група осіб [2,3] (підписання договорів різними рівноправними учасниками). Кожен учасник створює свою частину підпису, здійснюється обмін відкритими параметрами по мережах зв’язку, після чого формується колективний підпис. Для перевірки колективного підпису формується колективний відкритий ключ, який залежить від відкритих ключів учасників підписання електронного документа.

Однак, якщо учасники підписання не є рівноправними, може виникнути необхідність підписання різних документів групою осіб, кожна із котрих має право підписувати тільки свій документ. Наприклад, директор, бухгалтер, завідувач відділу кадрів, технолог підписують кожний свій електронний документ с використанням свого особистого ключа. С метою зменшення довжини підпису пропонується формування єдиного, колективного підпису різних документів на базі елементів особистих підписів. Перевірка такого колективного підпису потребує знання відкритих ключів кожного із учасників підписання і відповідних кожному електронних документів.

2.1 Колективне підписання електронного документу рівноправними учасниками протоколу

Пропонується реалізація протоколів колективного цифрового підпису електронного документу на еліптичної кривої і з використанням операцій в простому полі [36].

2.1.1 Протокол колективного цифрового підпису електронного документу на еліптичної кривої

Відкриті ключі P_1, P_2, …, P_n генерують у вигляді точок еліптичної кривої, для чого генерують еліптичну криву у вигляді сукупності точок, кожна з яких визначається парою багаторозрядних двійкових чисел, що є відповідно абсцисою і ординатою даної точки еліптичної кривої в декартовій системі координат, причому точки P_1, P_2, …, P_n еліптичній кривій генерують як добуток k_i та G, де $i = 1, 2, \ldots, n$, G – додатково згенерована точка еліптичної кривої, що має порядок q, де q – просте багаторозрядне двійкове число, а колективний електронний цифровий підпис формують у вигляді пари багаторозрядних двійкових чисел e і s, для чого генерують m випадкових багаторозрядних двійкових чисел t_{α_1}, t_{α_2}, …, t_{α_m}, генерують m точок R_{α_1}, R_{α_2}, …, R_{α_m} еліптичної кривої як добуток t_i та G, генерують точку R еліптичної кривої як суму всіх R_α після чого формують перше багаторозрядне двійкове число e колективного електронного цифрового підпису як добуток абсциси точки R x_R та H за модулем допоміжного простого багаторозрядного двійкового числа δ, потім генерують m багаторозрядних двійкових чисел s_{α_1}, s_{α_2}, …, s_{α_m} як рзницю відповідного t_α і добутку e та відповідного k_α за модулем q, після чого генерують друге багаторозрядне двійкове число s колективного електронного цифрового підпису як суму всіх s_α за модулем q, причому колективний відкритий ключ генерують у вигляді точки P еліптичної кривої, яка являє собою суму всіх точок P_α, і перше перевірочне багаторозрядне двійкове число A формують за модулем q із $x_{R'}$ – абсциси точки R′ еліптичної кривої, обчисленої як суму точок eP та sQ, а друге перевірочне багаторозрядне двійкове число B формують рівним e.

Приклад роботи протоколу.

У даному прикладі використовується ЕК, секретні і відкриті ключі користувачів такі ж як і в попередньому прикладі. В прикладі використовується ЕК, визначувана такими параметрами:

a = 552176786573763455539041630059977662234733359784, b = 9717196 і p = 552176786573763455539041630059977662234733359787.

Дана ЕК містить кількість точок, рівну простому числу V = 552176786573763455539041622878388691333982384172 3, тобто будь-яка її точка має порядок q, рівний значенню V.

Розглянемо колектив з трьох користувачів. При формуванні і перевірці достовірності колективного ЕЦП (підписом є пара БДЧ e і s) виконують таку послідовність дій.

Крок 1. Генерують ЕК з параметрами вказаними вище.

Крок 2. Формують секретні ключі у вигляді випадкових БДЧ:

k_1 = 818210889089289010146733343 4019 – ключ першого користувача;

k_2 = 39525045394037582788085810247 91 – ключ другого користувача;

k_3 = 97631609416000926319355206580 71 – ключ третього користувача.

Крок 3. Формують відкриті ключі у вигляді точок ЕК P_1, P_2, P_3, для чого

Крок 3.1. Генерують точку G:

G = (40581389988176995699766783582333359584950379694 65,
76856892633603682571849521891630868249411614416 0);

Крок 3.2. Генерують точки P_1, P_2, P_3 як добуток власного ключа та точки G:

P_1 = (24067676659281588994469061658217472188835746023 71,
56237764852169229068903150720500806020534563699 1);

P_2 = (34870810837802708535738941404482523792268351073 2,
14020261919960801963994827704684725980760525998 09)

P_3 = (43071660778335193010633225330241620050910250203 13,
52802963125491560281489059142155706555149862175 09).

Крок 4. Приймають ЕД, представлений, наприклад, наступним БДЧ H (як H може бути узята, зокрема, хэш-функція від ЕД):

H =89259990268711451315203376121177786806591925760 33.

Крок 5. Формують ЕЦП Q у вигляді двох БДЧ e і s, для чого виконують наступні дії.

Крок 5.1. Перший, другий і третій користувачі генерують випадкові БДЧ t_1, t_2 і t_3, відповідно:

t_1 = 20908809226259826835844601678623823 79;

t_2 = 53603835268566637005838962052664183 41;

t_3 = 76771188107231423520123174534008874 49.

Крок 5.2. Потім перший, другий і третій користувачі генерують точки R_1, R_2 і R_3, як добуток відповідних випадкових чисел та точки G:

R_1 = (45333600752924466088506644003647115922051366184 60,
11750613370622321795843486864773247621011640500 95);

R_2 = (19582792238279020473793364652858954353301401854 77,
88365089082562329551442342429704943185648525 73);

R_3 = (50386160288529598775095540817896674368537947535 57,
20961315793304467792455168848453471303884146891 3).

Крок 5.3. Генерують точку R сумуванням результатів попереднього кроку:

R = (25970979702636108635460694368339945800021054185 69,
33049150401044008138023742824739855500155219733 83).

Крок 5.4. Формують перше БДЧ e електронного підпису, беручи добуток x_R – абсциси точки R та H за модулем допоміжного простого БДЧ δ (δ = 71181982186593210289890 11):

e = 50790082330769320874737 89.

Крок 5.5. Перший, другий і третій користувачі генерують БДЧ s_1, s_2 і s_3, відповідно, як різницю t_i та добутку e і k_i за модулем q, де q' дорівнює N і i = 1,2,3:

s_1 = 359849983424274307716254877984953159149283598626;

s_2 = 222847150339927145184417458803419579201368620755 1;

s_3 = 332129573838505588102024832636380356481377340244 8.

Крок 5.6. Генерують друге БДЧ s колективного електронного цифрового підпису, сумуючи s_1, s_2, s_3 за модулем q:

s = 387849359470967085190261563599065602636919366902.

Крок 6. Формують перше перевірочне БДЧ A, для чого виконують таку послідовність дій.

Крок 6.1. Формують колективний відкритий ключ у вигляді точки P, сумуючи P_1, P_2 та P_3:

P = (259709797026361086354606943683399458000210541856 9,

330491504010440081380237428247398555001552197338 3).

Крок 6.2. Генерують точку R′, як суму добутків eP та sG:

eP = (146955471348564375364922408624400975297984578370,

506748749888997175271628334751609221739781710787 0);

sG = (292535746865117796446681364223363153817497171251 3,

599550386022153150210626227063281723596625174740);

R′= (259709797026361086354606943683399458000210541856 9,

330491504010440081380237428247398555001552197338 3);

Крок 6.3. Генерують БДЧ A, беручи добуток $x_{R'}H$ за модулем δ, де додаткове БДЧ δ приймає значення 71181982186593210289890 11;

A = 492712487159295979332971 1.

Крок 7. Формують друге перевірочне БДЧ B шляхом копіювання БДЧ e:

$B = e$ = 507900823307693208747378 9.

Крок 8. Порівнюють перше A і друге B перевірочні БДЧ.

Порівняння показує, що параметри БДЧ A і B співпадають. Збіг значень A і B означає, що колективний ЕЦП є справжним, тобто відноситься до прийнятого ЕД, представленому БДЧ H, і сформований трьома користувачами, по відкритих ключах, по яких був сформований колективний відкритий ключ, використаний для перевірки достовірності підпису.

2.1.2 Протоколи колективного цифрового підпису електронного документу в простому полі

В протоколі 1 відкриті ключі P_1, P_2, …, P_n генерують у вигляді багаторозрядних двійкових чисел, для чого генерують просте багаторозрядне двійкове число p, на одиницю більше добутку Nz^2, де N – парне натуральне

багаторозрядне двійкове число і z – просте w-разрядное двійкове число, $w > 64$, причому багаторозрядні двійкові числа $P_1, P_2, \ldots, P_n$ генерують, беручи значення k_i^z по модулю p, де $i = 1, 2, \ldots, n$, а колективний електронний цифровий підпис формують у вигляді пари багаторозрядних двійкових чисел R і S, для чого генерують m випадкових багаторозрядних двійкових чисел t_{α_1}, t_{α_2}, …, t_{α_m}, генерують m допоміжних багаторозрядних двійкових чисел R_{α_1}, R_{α_2}, …, R_{α_m}, підносячи відповідні t_α до степеня z і беручи за модулем p, генерують перше багаторозрядне двійкове число R колективного електронного цифрового підпису як добуток всіх R_α за модулем p, після чого формують допоміжне багаторозрядне двійкове число E, беручи добуток R і H за модулем δ, де δ – додаткове просте багаторозрядне двійкове число; потім генерують m багаторозрядних двійкових чисел S_{α_1}, S_{α_2}, …, S_{α_m} по формулі (2.1):

$$S_{\alpha_j} = k_{\alpha_j}^E t_{\alpha_j} \bmod p, \tag{2.1}$$

після чого генерують друге багаторозрядне двійкове число S колективного електронного цифрового підпису як добуток всіх S_α за модулем p, причому колективний відкритий ключ генерують у вигляді багаторозрядного двійкового числа P, як добуток всіх P_α за модулем p, і перше перевірочне багаторозрядне двійкове число A формують, беручи S, піднесене до степеня z, по модулю p, а друге перевірочне багаторозрядне двійкове число B формують по формулі (2.2):

$$B = P^E R \bmod p. \tag{2.2}$$

Приклад роботи протоколу 1.

Цей приклад представляє варіант реалізації способу, що заявляється, з використанням обчислень по простому модулю. Ті БДЧ, що приводяться в прикладі, записані скорочено у вигляді десяткових чисел, які в обчислювальних пристроях представляються і перетворяться в двійковому вигляді, тобто у вигляді послідовності сигналів високого і низького потенціалу. При формуванні і перевірці достовірності колективного ЕЦП, сформованого двома користувачами (підписом є пара чисел R і S.), виконують таку послідовність дій.

Крок 1. Формують просте число, таке що $p - 1$ N раз містить квадрат великого простого числа z, де N – парне число:

p = 4153476369892465269012870897623282390047400100719, де

z = 132104433635297779312031;

N = 238.

Крок 2. Формують секретний ключ у вигляді випадкового БДЧ

k_1 = 3526378981324543353612;

k_2 = 113464575688245433235 1.

Крок 3. Формують відкриті ключі першого і другого користувачів у вигляді БДЧ P_1 і P_2, підносячи секретні ключі до степеня z за модулем p:

P_1 = 38648581002193529403697748477885520183670551977 06;

P_2 = 10075249248403728279512402030796599343804488887 0.

Крок 4. Приймають ЕД, представлений, наприклад, БДЧ H (як H може бути узята, зокрема, хэш-функція від ЕД):

H = 73568790119017231823457.

Крок 5. Формують ЕЦП у вигляді пари чисел (R, S), для чого виконують таки дії:

Крок 5.1. Перший і другий користувачі генерують випадкові числа

t_1 = 87193323415243553115136314;.

t_2 = 13341235311683513436277397.

Крок 5.2. Перший і другий користувачі формують значення R_1 і R_2 , підносячи згенеровані числа до степеня z за модулем p:

R_1 = 19651943943290548836692335934353542255535285430 48;

R_2 = 18014941387790054614314619927124592845743655680 04.

Крок 5.3. Перший і другий користувачі формують спільний елемент R колективного підпису як добуток R_1 і R_2 за модулем p:

R = 15108522836051412651675481428884418878061960455 89.

Крок 5.4. Генерують допоміжне БДЧ E як добуток R та H за модулем δ, де додаткове просте БДЧ δ = 35488784369499179:

E = 28456867839200835.

Крок 5.5. Перший і другий користувачі формують значення S_1 і S_2 шляхом виконання операцій, що задаються формулою (2.1):

S_1 = 41485352112321591481267980910899397329856966175 14;

S_2 = 27301620646443911870899752806815310581883250164 51.

Крок 5.6. Формують елемент S колективного підпису шляхом перемножування значень S_1 і S_2:

S = 84191676295568477011571339629580601840581279844 9.

Крок 6. Формують перше перевірочне БДЧ A, підносячи S до степеня z за модулем p:

A = 37065567156119986070173861358597621499579760340 58.

Крок 7. Формують друге перевірочне БДЧ B, для чого виконують такі дії.

Крок 7.1. Обчислюють колективний відкритий ключ, відповідний першому і другому користувачам, перемножуючи особисті відкриті ключі:

P = 29901347341033605721977138079588389857348000979 71.

Крок 7.2. Обчислюють друге перевірочне БДЧ B по формулі (2.2):

$P^E \bmod p$ = 94046480227905964534423883395762098563827934 2075;

B = 37065567156119986070173861358597621499579760340 58.

Крок 8. Порівнюють (наприклад, порозрядно) параметри першого і другого перевірочних БДЧ A і B. Порівняння показує, що параметри БДЧ A і B співпадають, що указує на достовірність колективного ЕЦП, що належить першому і другому користувачам, яка означає, що документ, представлений БДЧ H, підписаний як першим, так і другим користувачами.

Це доводиться теоретично співвідношенням (2.3). Для ЕЦП, сформованого з використанням правильного значення секретного ключа маємо:

$$S = S_1 S_2 = (k_1^E t_1)(k_2^E t_2) = (k_1 k_2)^E (t_1 t_2) mod\ p \Rightarrow S^z = (k_1 k_2)^{zE} \times (t_1 t_2)^z = (k_1^z k_2^z)^E (t_1^z t_2^z) = P^E R\ mod\ p, \quad (2.3)$$

тобто для колективного ЕЦП, сформованого з використанням секретних ключів першого і другого користувачів відповідно до процедур прикладу, рівняння перевірки підпису виконується.

В протоколі 2 відкриті ключі P_1, P_2, …, P_n також генерують у вигляді багаторозрядних двійкових чисел, для чого генерують просте багаторозрядне двійкове число p, на одиницю більше добутку Nz^2, де N – парне натуральне багаторозрядне двійкове число і z – просте w-розрядне двійкове число, $w > 64$, причому багаторозрядні двійкові числа P_1, P_2, …, P_n генерують, беручи значення k_i^z по модулю p, де $i = 1, 2, \ldots, n$, а колективний електронний цифровий підпис формують у вигляді пари багаторозрядних двійкових чисел R і S, для чого генерують m випадкових багаторозрядних двійкових чисел t_{α_1}, t_{α_2}, …, t_{α_m}, генерують m допоміжних багаторозрядних двійкових чисел R_{α_1}, R_{α_2}, …, R_{α_m}, підносячи відповідні t_α до степеня z і беручи за модулем p, генерують перше багаторозрядне двійкове число R колективного електронного цифрового підпису як добуток всіх R_α за модулем p, після чого формують допоміжне багаторозрядне двійкове число E, беручи добуток R і H за модулем δ, де δ – додаткове просте багаторозрядне двійкове число; потім генерують m багаторозрядних двійкових чисел S_{α_1}, S_{α_2}, …, S_{α_m} по формулі (2.1), після чого генерують друге багаторозрядне двійкове число S колективного електронного цифрового підпису як добуток всіх S_α за модулем p, причому колективний відкритий ключ генерують у вигляді багаторозрядного двійкового числа P, як добуток всіх P_α за модулем p, а перше і друге B перевірочні багаторозрядні двійкові числа A формують по формулі (2.4), а друге B дорівнює E:

$$A = (S^z P^{-E} \bmod p) H \bmod \delta. \quad (2.4)$$

Приклад роботи протоколу 2.

Цей варіант забезпечує ЕЦП скороченого розміру при використовуванні обчислень по простому модулю. В даному прикладі генерують колективний ЕЦП, в якому одне з БДЧ, складових підпис (E, S), має зменшену довжину, що дозволяє скоротити загальний розмір підпису.

Крок 1. Формують просте число, таке ще $p - 1$ *N раз* містить квадрат великого простого числа z, де N – парне число:

p = 4153476369892465269012870897623282390047400100719, де

z = 132104433635297779312031;

N = 238.

Крок 2. Формують секретні ключі у вигляді випадкових БДЧ k_1, k_2 і k_3:

k_1 = 3526378981324543353612;

k_2 = 5161833476248544287957;

k_3 = 1134645756882454332351.

Крок 3. Формують відкриті ключі трьох користувачів у вигляді БДЧ P_1, P_2 і P_3, підносячи секретні ключі до степеня z за модулем p:

P_1 = 3864858100219352940369774847788552018367055197706;

P_2 = 1114137187563681248610918988022794168709765920068;

P_3 = 1007524924840372827951240203079659934380448888870.

Крок 4. Приймають ЕД, представлений, наприклад, БДЧ H (як H може бути узята, зокрема, хэш-функція від ЕД):

H = 73568790119017231823457.

Крок 5. Формують ЕЦП у вигляді пари чисел (E, S), для чого виконують такі дії:

Крок 5.1. Перший і третій користувачі генерують випадкові числа

t_{α_1} = 87193323415243553115136314;.

t_{α_2} = 13341235311683513436277397,

де $\alpha_1 = 1$ і $\alpha_2 = 3$.

Крок 5.2. Перший і третій користувачі формують значення R_{α_1} і R_{α_2} підносячи згенеровані числа до степеня z за модулем p:

R_{α_1} = 19651943943290548836692335934353542255535285430 48;

R_{α_2} = 18014941387790054614314619927124592845743655680 04.

Крок 5.3. Перший і третій користувачі формують спільне значення R як добуток R_1 і R_2 за модулем p:

R = 151085228360514126516754814288844188780619604558 9.

Крок 5.4. Генерують перше БДЧ колективного підпису у вигляді БДЧ E, як добуток R та H за модулем δ, де додаткове просте БДЧ δ = 35488784369499179:

E = 28456867839200835.

Крок 5.5. Перший і третій користувачі формують значення S_{α_1} і S_{α_2} шляхом виконання операцій, що задаються формулою (2.1):

S_{α_1} = 41485352112321591481267980910899397329856966175 14;

S_{α_2} = 27301620646443911870899752806815310581883250164 51.

Крок 5.6. Формують друге БДЧ *S* колективного підпису шляхом перемножування значень S_{α_1} і S_{α_2}:

S = 84191676295568477011571339629580601840581279844 9.

Крок 6. Формують перше перевірочне БДЧ *A*, для чого виконують такі дії.

Крок 6.1. Обчислюють колективний відкритий ключ, відповідний першому і третьому користувачам, перемножуючи особисті відкриті ключі:

P = 29901347341033605721977138079588389857348000979 71.

Крок 6.2. Обчислюють перше перевірочне БДЧ *A* по формулі (2.4)

$S^z \bmod p$ = 37065567156119986070173861358597621499579760340 58;

$p - E - 1 \bmod p$ = 41534763698924652690128708976232514945488456974 44;

$P^{p-E-1} \bmod p$ = 26799997978613223056744278298820339148040349597 74;

$E' = S^z P^{p-E-1} \bmod p$ =

= 15108522836051412651675481428884418878061960455 89;

$A = E' H \bmod \delta$ = 28456867839200835.

Крок 7. Формують друге перевірочне БДЧ *B* рівне *E*:

B = *E* = 28456867839200835.

Крок 8. Порівнюють (наприклад, порозрядно) параметри першого і другого перевірочних БДЧ *A* і *B*. Порівняння показує, що параметри БДЧ *A* і *B* співпадають, що указує на достовірність колективного ЕЦП, тобто прийнятий колективний ЕЦП відноситься до прийнятого ЕД, представленого БДЧ *H*, і сформован першим і третім користувачами, яким відповідає колективний відкритий ключ, рівний добутку їх відкритих ключів, узятому по модулю *p*. Достовірність колективної ЕЦП, що належить першому і третьому користувачам, означає, що документ, представлений БДЧ *H*, підписаний як першим, так і третім користувачами.

В протоколі 3 відкриті ключі генерують у вигляді багаторозрядних двійкових чисел P_1, P_2, …, P_n, для чого генерують просте багаторозрядне двійкове число *p*, причому багаторозрядні двійкові числа P_1, P_2, …, P_n генерують підносячи додаткове згенеруване багаторозрядне двійкове число *g*, що має порядок *q*, у степінь секретного ключа по модулю *p*, де *q* – просте багаторозрядне двійкове число, а колективний електронний цифровий підпис формують у вигляді пари багаторозрядних двійкових чисел *E* і *S*, для чого генерують *m* випадкових багаторозрядних двійкових чисел t_{α_1}, t_{α_2}, …, t_{α_m}, генерують *m* допоміжних багаторозрядних двійкових чисел R_{α_1}, R_{α_2}, …, R_{α_m} ,підносячи *g* у степені відповідних t_α по модулю *p*, генерують багаторозрядне двійкове число R як добуток всіх R_α, після чого формують перше багаторозрядне двійкове число *E* колективного електронного цифрового підпису як добуток *R* і *H* за модулем δ, де δ – додаткове просте багаторозрядне двійкове число, потім генерують *m* багаторозрядних двійкових чисел S_{α_1}, S_{α_2}, …, S_{α_m} по формулі (2.5):

$$S_{\alpha_j} = \left(t_{\alpha_j} + Ek_{\alpha_j} \right) \bmod q \,, \tag{2.5}$$

після чого генерують друге багаторозрядне двійкове число S колективного електронного цифрового підпису як суму всіх S_α причому колективний відкритий ключ генерують у вигляді багаторозрядного двійкового числа P, обчислюваного як добуток всіх P_α, і перше перевірочне багаторозрядне двійкове число A формують як добуток R' та H по модулю δ, де R' – багаторозрядне двійкове число, обчислене по формулі (2.6):

$$R' = P^{-E} g^{s} \bmod p \,, \tag{2.6}$$

а друге перевірочне багаторозрядне двійкове число B формують по формулі приймають рівним E.

Приклад роботи протоколу 3.

Цей варіант забезпечує скорочення двох БДЧ, складових ЕЦП, при використовуванні обчислень по простому модулю. Для скорочення прикладу розглядається формування колективного ЕЦП у вигляді двох БДЧ E і S, що відноситься до двох користувачів, проте аналогічним чином можна сформувати і перевірити колективний ЕЦП, що відноситься до довільного числа користувачів.

Крок 1. Формують просте число, таке що (p – 1) N' разів містить простий множник q, де N'– парне число:

p = 4153476369892465269012870897623282390047400100719, де

q = 132104433635297779312031;

N'=31440855205200871476263378.

Крок 2. Формують секретні ключі у вигляді випадкових БДЧ

k_1 = 3526378981324543353612;

k_2 = 1134645756882454332351.

Крок 3. Формують відкриті ключі першого і другого користувачів у вигляді БДЧ P_1 и P_2, відповідно, для чого виконують таку послідовність дій:

Крок 3.1. Генерують додаткове БДЧ g, підносячи випадкове вибиране число α в степінь N', α = 174658:

g = 109254265205735408361699659944844910548930750915 5.

Одержане додаткове БДЧ g має порядок q.

Крок 3.2. Генерують відкриті ключі підносячи додаткове згенеруване багаторозрядне двійкове число g у степінь секретного ключа по модулю p:

P_1 = 343333456853771254091394619802004827170019141 6922;

P_2 = 386399438563945559677942203763500148256012559 6243.

Крок 4. Приймають ЕД, представлений, наприклад, БДЧ H (як H може бути узята, зокрема, хэш-функція від ЕД):

H = 73568790119017231823457.

Крок 5. Формують ЕЦП у вигляді пари чисел (R, S), для чого виконують такі дії:

Крок 5.1. Перший і другий користувачі генерують випадкові числа

t_1 = 87193323415243553115136314;.

t_2 = 13341235311683513436277397.

Крок 5.2. Перший і другий користувачі формують значення R_1 і R_2 підносячи g у степені відповідних t_α по модулю p:

R_1 = 31027673547509324711260716186321176909895494679 53;

R_2 = 27366509207045295831927478487637948681548021750 76.

Крок 5.3. Перший і другий користувачі формують спільне значення R_{12} як добуток R_1 і R_2 за модулем p:

R_{12} = 46124962342862671563301241127072281251944012875.

Крок 5.4. Генерують елемент E колективного підпису у вигляді БДЧ, як добуток R_{12} та H за модулем δ, де додаткове просте БДЧ δ = 35488784369499179:

E = 1310719285759554.

Крок 5.5. Перший і другий користувачі формують значення S_1 і S_2 шляхом виконання операцій, що задаються формулою (2.5):

$S_1 = Ek_1 + t_1 \bmod q$ = 7283108635732968306 03;

$S_2 = Ek_2 + t_2 \bmod q$ = 56086667770983024235244.

Крок 5.6. Формують елемент S колективного підпису шляхом складання значень S_1 і S_2:

S = 56814978634556321065847.

Крок 6. Формують перше перевірочне БДЧ A, для чого виконують такі дії.

Крок 6.1. Обчислюють колективний відкритий ключ, відповідний першому і другому користувачам як добуток особистих відкритих ключів:

P = 10683374366544621250718743106767340408233023503 99.

Крок 6.2. Обчислюють перше перевірочне БДЧ A як добуток R' та H по модулю δ, де R' – багаторозрядне двійкове число, обчислене по формулі (2.6):

$g^S \bmod p$ = 29906182756670709877812239800903751404144814976 89;

$q - E$ = 13210443232457849355247 7;

$P^{q-E} \bmod p$ = 32306083684856029375751061718518906641550521549 57;

$E' = g^S P^{q-E} \bmod p$ = 46124962342862671563301241127072281251944012875;

$A = E' H \bmod \delta$ = 1310719285759554.

Крок 7. Формують друге перевірочне БДЧ $B = E$:

$B = R$ = 1310719285759554.

Крок 8. Порівнюють (наприклад, порозрядно) параметри першого і другого перевірочних БДЧ A і B. Порівняння показує, що параметри БДЧ A і B співпадають, що указує на достовірність колективного ЕЦП, тобто прийнятий колективний ЕЦП відноситься до прийнятого ЕД, представленому БДЧ H, і сформований двома користувачами, яким відповідає колективний відкритий ключ, рівний добутку

відкритих ключів цих користувачів, узятому по модулю *p*. Достовірність колективного ЕЦП, що належить першому і другому користувачам, означає, що документ, представлений БДЧ *H*, підписаний як першим, так і другим користувачами.

У цьому прикладі перевірка достовірності колективного ЕЦП фактично здійснюється по формулах:

$$E' = y^{-E} g^{S} \bmod p\,,\ A = E'H \bmod \delta\,,\ B = E \text{ и } A = B\,. \tag{2.7}$$

Коректність процедур формування і перевірки підпису доводиться для довільних розмірів БДЧ, використаних в даному прикладі, таким чином:

$$\begin{aligned} A = E'H \bmod \delta &= \left(y^{-E} g^{S} \bmod p \right) H \bmod \delta = \\ = \left(y^{-E} g^{S} \bmod p \right) H \bmod \delta &= \left(\left(y_1 y_2 \right)^{-E} g^{S_1+S_2} \bmod p \right) H \bmod \delta = \\ = \left(\left(g^{-Ek_1} g^{-Ek_2} \right) g^{Ek_1+t_1+Ek_2+t_2} \bmod p \right) H \bmod \delta &= \\ = \left(g^{t_1+t_2} \bmod p \right) H \bmod \delta = \left(g^{t_1} g^{t_2} \bmod p \right) H \bmod \delta &= \\ = \left(R_1 R_2 \bmod p \right) H \bmod \delta = R_{12} H \bmod \delta = E = B\,. \end{aligned} \tag{2.8}$$

Користувачі, сукупність яких складає колектив, що формує колективний підпис до електронного документа, заздалегідь генерують випадкові БДЧ, по яких вони обчислюють параметри для обчислення першого елементу підпису *R*. Параметр *R* фіксує вибрані ними випадкові значення, проте жоден з користувачів не може обчислити випадкове число, використане яким-небудь іншим користувачем. Завдяки цьому забезпечується з одного боку стійкість колективної ЕЦП, а з іншою можливість кожному користувачу обчислити свою частку в другому елементі колективного підпису (значення S_j) підпису. Підсумовування всіх часток підпису S_j формує другий елемент колективного підпису. Оскільки всі ці частки вироблені з використанням секретного ключа кожним з користувачів, то колективний підпис може бути перевірений за допомогою перевірочного рівняння, в яке входить колективний відкритий ключ, обчислюваний по відкритих ключах користувачів, які складають колектив підписуючих. При цьому колективний ключ виявляється залежним від секретних ключів всіх цих користувачів, але жоден з користувачів не розкривав свого особистого секретного ключа, тому колективний підпис є безпечним. У відомих способах-аналогах і в прототипі не використовується процедура обчислення колективного елементу *R* як першого елементу колективної ЕЦП і формування долей підпису S_j, тому немає можливісті згортки

(підсумовування) окремих підписів користувачів в єдиний колективний підпис порівняно малого розміру і перевірки її по колективному відкритому ключу.

Пропонований спосіб може бути використаний для числа n користувачів, що задовольняє умові $n \geq 2$. Користувачі умовно позначаються номерами $i = 1, 2, \ldots, n$. Цей номер використовується як індекс, вказуючий на те, якому користувачу належить секретний і відкритий ключі, або на те, який з користувачів генерує відзначені індексом БДЧ або точки ЕК. З сукупності n користувачів деяка їх підмножина, що складається з m довільно вибраних користувачів, може бути задана номерами користувачів, що входять в дану підмножину, наприклад номерами α_1, $\alpha_2, \ldots, \alpha_m$, кожний з яких вибирається з множини чисел $1, 2, \ldots, n$. Таким чином, числа α_j, де $j = 1, 2, \ldots, m$, є вибіркою довільних m номерів з множини $\{1, 2 ., n\}$, при цьому m не більше n. Відповідно цьому сукупність відкритих ключів, наприклад, точок $\mathrm{P}_{\alpha_1}, \mathrm{P}_{\alpha_2}, \ldots, \mathrm{P}_{\alpha_m}$ ЕК є вибіркою з множини всіх відкритих ключів $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n$, а сукупність секретних ключів $k_{\alpha_1}, k_{\alpha_2}, \ldots, k_{\alpha_m}$ є вибіркою з множини всіх секретних ключів $k_1, k_2, \ldots, k_n$, де $i = 1, 2, \ldots, n$.

Коректність заявленого способу доводиться теоретично. Розглянемо, наприклад, варіант реалізації способу по п. 3 формули корисної моделі. Колективний відкритий ключ, відповідний підмножині користувачів з умовними номерами $\alpha_1, \alpha_2, \ldots, \alpha_m$, є точкою:

$$\mathrm{P} = \mathrm{P}_{\alpha_1} + \mathrm{P}_{\alpha_2} + \ldots + \mathrm{P}_{\alpha_m} = k_{\alpha_1}\mathrm{G} + k_{\alpha_2}\mathrm{G} + \ldots + k_{\alpha_m}\mathrm{G} = \left(\sum_{j=1}^{m} k_{\alpha_j} \right) \mathrm{G} \quad . \quad (2.9)$$

Значення s_{α_j}, які є «частками» користувачів в колективному підпису, генеруються по формулі (2.5) використовуючи віднімання замість додавання, тому:

$$\sum_{j=1}^{m} s_{\alpha_j} \equiv \sum_{j=1}^{m} t_{\alpha_j} - \sum_{j=1}^{m} e k_{\alpha_j} \equiv \sum_{j=1}^{m} t_{\alpha_j} - e \sum_{j=1}^{m} k_{\alpha_j} \bmod q \, . \quad (2.10)$$

Значення точки R', що використовується для формування першого перевірочного БДЧ A, генерується по формулі $\mathrm{R}' = e\mathrm{P} + s\mathrm{G}$, тобто воно рівне

$$\mathrm{R}' = e\mathrm{P} + s\mathrm{G} = e\left(\sum_{j=1}^{m} k_{\alpha_j} \right) \mathrm{G} + \left(\sum_{j=1}^{m} t_{\alpha_j} - e \sum_{j=1}^{m} k_{\alpha_j} \right) \mathrm{G} =$$

$$= \left(e \sum_{j=1}^{m} k_{\alpha_j} + \sum_{j=1}^{m} t_{\alpha_j} - e \sum_{j=1}^{m} k_{\alpha_j} \right) \mathrm{G} = \left(\sum_{j=1}^{m} t_{\alpha_j} \right) \mathrm{G} = \mathrm{R} \quad . \quad (2.11)$$

Отже, A дорівнює B, тобто правильно сформований колективний підпис задовольняє процедурі перевірки підпису, а значить коректність процедур генерації і перевірки ЕЦП доведена.

Розглянемо приклади реалізації заявленого технічного рішення з використовуванням ЕК, описуваної рівнянням (2.7):

$$y^2 = x^3 + ax + b \bmod p, \tag{2.12}$$

де конкретні значення використаних параметрів описані в чисельних прикладах, що наводяться нижче. Використані в прикладах ЕК були згенерувані за допомогою програми, розробленої спеціально для генерації ЕК, генерації точок ЕК, включаючи точки із заданим порядком, і виконання операцій над точками ЕК. Ті БДЧ, що приводяться в прикладі, записані скорочено у вигляді десяткових чисел, які в обчислювальних пристроях представляються і перетворяться в двійковому вигляді, тобто у вигляді послідовності сигналів високого і низького потенціалу.

Розглянуті приклади експериментально підтверджують коректність реалізації способу, якій заявляється, що доповнює приведені вище математичні докази коректності описаних конкретних реалізацій заявленого способу формування і перевірки колективного ЕЦП, якій завіряє ЕД.

Таким чином, показано, що спосіб, що заявляється, може бути встановлений в основу стійких систем колективного ЕЦП, що забезпечують зменшення розміру колективного ЕЦП.

Приведені приклади і математичне обгрунтовування показують, що пропонований спосіб формування і перевірки достовірності ЕЦП працює коректно, технічно реалізовуваний і дозволяє досягти сформульованого технічного результату.

2.2 Колективне підписання різних документів нерівноправними учасниками протоколу

2.2.1 Протокол колективного цифрового підпису різних документів на базі стандарту електронного цифрового підпису ДСТУ 4145-2002

Пропонується реалізація протоколів колективного цифрового підпису різних документів на базі стандарту електронного цифрового підпису ДСТУ 4145-2002 [38, 39] і з використанням операцій в простому полі [10].

Загальні параметри стандарту ДСТУ 4145-2002:

- основне поле – скінченне поле $GF(2^m)$, яке є розширенням степеня m поля GF(2);

- m – просте число в інтервалі [163, 509];
- еліптична крива над основним полем

$$y^2 + xy = x^3 + Ax^2 + B, \tag{2.13}$$

де A, $B \in GF(2^m)$, $B \neq 0$, $A \in \{0,1\}$, разом із приєднаною нескінченно віддаленою точкою O;

- базова точка еліптичної кривої P , що не збігається 3 O простого порядку n, така що nP дорівнює O і kP не збігається з O, k обирається врамках від 0 до n;
- H(•) — функція хешування, припустимо використання стандарту [40] та інших.

Генерація ключів.

Кожний і-ий (i = 1, 2, …, t) користувач має два ключа - особистий (секретний) d_i в рамках від 2 до n-1 та відкритий Q_i , який являє собою точку, зворотню точці d_iP.

Формування колективного підпису.

Нехай користувач i(i = 1, 2, …, t), підписує електронний документ M_i з геш-образом H_i. В бітовому вигляді геш-образу Hі використовуються молодші $|n| - 1$ розряди, які формують десяткове число h_i.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, в рамках від 2 до n-1, обчислює координати точки R_i , множачи k_i на P та надає їх для колективного використання.

Далі обчислюється сума всіх точок R_i, i = 1, 2, …, t:

$$R = \sum_{i=1}^{t} R_i = (xR, yR), \tag{2.14}$$

після чого формується перше число колективного електронного цифрового підпису:

$$r = xR \bmod n. \tag{2.15}$$

При $r = 0$ обираються нові випадкові секретні ключи k_i.

Потім кожний користувач і за допомогою свого секретного ключа d_i та значення k_i обчислює свою долю підпису:

$$s_i = (k_i + d_i\, h_i\, r) \bmod n, \tag{2.16}$$

після чого генерується s – друге число колективного електронного цифрового підпису:

$$s = \sum_{i=1}^{t} s_i \bmod n \,. \tag{2.17}$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Колективним підписом є пара чисел (r, s).

Перевірка колективного підпису.

Перевірка підпису здійснюється за допомогою додаткової точки еліптичної кривої , яка залежить від відкритих ключів Q_i учасників підписання і відповідних геш-образів електронних документів h_i, і являє собою суму їхніх добутків.

Обчислюється точка R' еліптичної кривої:

$$R' = sP + rQ = (xR', yR'), \tag{2.18}$$

після чого формується:

$$r' = xR' \bmod n. \tag{2.19}$$

Якщо $r' = r$, колективний цифровий підпис різних документів M_i, i = 1, 2, …, t, признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки колективного підпису:

$$\begin{aligned} R^{'} = sP + rQ = \left(\sum_{i=1}^{t} s_i\right)P + r\left(\sum_{i=1}^{t} h_i Q_i\right) = \left(\sum_{i=1}^{t} k_i + d_i h_i r\right)P + \\ + r\left(\sum_{i=1}^{t} h_i(-d_i P)\right) = \left(\sum_{i=1}^{t} k_i\right)P = \sum_{i=1}^{t} R_i = R \end{aligned} \tag{2.20}$$

Оскільки R' дорівнює R, то і r' дорівнює r.

Приклад роботи протоколу колективного цифрового підпису різних документів.

Оберемо загальні параметри відповідно стандарту ДСТУ 4145-2002:

- основне поле – скінченне поле $GF(2^{163})$;
- еліптична крива над основним полем задана рівнянням (2.13),

$A = 1$, B = `5FF6108462A2DC8210AB403925E638A19C1455D21`;

- базова точка еліптичної кривої

P = (`7D`, `4ED6F4E822394A68280E0FB970141836354F3A91C`);

- порядок базової точки

n = `40000000000000000002BEC12BE2262D39BCF14D`.

Генерація ключів.

Нехай число користувачів t=3. Відповідні секретні ключі є

d_1 = `3FD35EB7CE4F03AD82BB6D2`,

d_2 = `13672B1490E5D5489F4B87`,

d_3 = `11DF05AC8F8C6D68E3980D1`.

Тоді відкрити ключі:

Q_1 = (`487453D2214684B2DAE4C1CC71E9E3EFCAC88C92D`, `69795D60DEFC9A16F030A263410956D375B5B037A`),

Q_2 = (`50E57454230C9561A9CBCFFC83106344F0F1E0B27`, `63C72C5B04DA3403FB25DA6087252615B6AAFEA8A`),

Q_3 = (`3807F2C265E68A922C7D7B0446F5280395F1A4927`, `52805BA4AAA49EAD23CAADC98B661918A15C4F442`).

Формування колективного підпису.

Нехай геш-образи відповідних документів

h_1 = `21C230E5C8C262B440608E8`,

h_2 = `1C626836D58154B65580012`,

h_3 = `19599F3265E53C16D7000B9`.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i,

k_1 = `B2B6391DF149F75BAF0B6D2`,

k_2 = `2DC76FBC5DE7A15F93315`,

k_3 = `58D64BFA7C579B51B8A3D`.

та обчислює координати точки R_i

R_1 = (`3414ABBA613ED416B196128C035F4CA4CCB21CDEB`, `754FBC2C79CBCD611EAB81F864CF2F1B8A9AB0CA7`),

R_2 = (`6E53AE38B19CC3C84A121A614170BBC364E147F04`, `275E2F0A84A35FDE9DC5A568FC0BF8CC24841B368`),

R_3 = (`1E827FBED97E2D8675A6C186D9F186703E22C0DF6`, `3B26FE08304AA7B196EC81BA62A84FD8603E19990`).

Далі обчислюється сума всіх точок R_i:

R = (`52E438B27721D2C0994C06D1E080ACC43C0DB9A38`, `4BEE5DF62431A88470660D3ED0EA31D2663DFF939`),

після чого формується r – перше число колективного електронного цифрового підпису:

r = `12E438B27721D2C0994BDAE5CDC28A616871EA8EB`.

Потім кожний користувач і за допомогою свого секретного ключа d_i та значення k_i обчислює свою долю підпису :

s_1 = `C7A626802F1252BDBD021547A3C1A77BF5F7DEFE`,

s_2 = `34673E30277D23F25BBE72198768F2A02F467DA09`,

s_3 = `12596FCD2F145438FC773AF6EC0982A62BD908239`,

після чого генерується s – друге число колективного електронного цифрового підпису:

s = `133B106559829D573405A278DAF06D5B46E3349F3`.

Колективним підписом є пара чисел

(r, s) = (`12E438B27721D2C0994BDAE5CDC28A616871EA8EB`,
`133B106559829D573405A278DAF06D5B46E3349F3`).

Перевірка колективного підпису.

Перевірка підпису здійснюється за допомогою додаткової точки еліптичної кривої Q, яка залежить від відкритих ключів Q_i учасників підписання і відповідних геш-образів електронних документів h_i:

Q = (`52E38E8AC810DC5345234D89EEC2FB440C09C25CE`,
`484926A6E01AFFA37DDEC15062B62E53EAE3BB86A`).

Обчислюється точка R′ еліптичної кривої

sP = (`29ED5AF0480C7D9159A15DB5A6F607E55AC56D781`,
`6A32FF934D611AB404E3FC01E87D8D7E1BADF09C4`),

rQ = (`4E099EC88C1E50045D1AAB71CD0AC5E8504EFF366`,
`691BDE1A476CC99C726572F38023922EE1EC419BA`),

R' (`52E438B27721D2C0994C06D1E080ACC43C0DB9A38`,
`4BEE5DF62431A88470660D3ED0EA31D2663DFF939`),

r' = `12E438B27721D2C0994BDAE5CDC28A616871EA8EB`.

Якщо $r' = r$, колективний цифровий підпис різних документів M_i признається справжнім.

Запропонований протокол колективного цифрового підпису може бути інтегровано в існуючу інфраструктуру відкритих ключів.

2.2.2 Протокол колективного цифрового підпису різних документів з використанням операцій в простому полі

Загальні параметри:

- p – просте число, таке що таке що (p – 1) N разів містить простий множник z;
- N – парне натуральне число, z – просте число, $z > 2^{64}$,
- H(•) — функція хешування, припустимо використання стандарту [40] та інших.

Генерація ключів.

Кожний і-ий (i = 1, 2, …, t) користувач має два ключа: особистий (секретний) x_i в рамках від 2 до p-1 та відкритий y_i , який отримується піднесенням особистого ключа до степені z за модулем p.

Формування колективного підпису.

Нехай користувач i, i = 1, 2, …, t, підписує електронний документ M_i з геш-образом H_i. В бітовому вигляді геш-образу Ні використаються молодші $|p| - 1$ розряди, які формують десяткове число h_i.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, в рамках від 2 до p-1, обчислює відкритий r_i, який отримується піднесенням особистого ключа до степені z за модулем $p = k_i^z \bmod p$, та надає їх для колективного використання.

Далі обчислюється добуток всіх R_i, i = 1, 2, …, t:

$$r = \prod_{i=1}^{t} r_i \bmod p, \tag{2.21}$$

де r – перше число колективного електронного цифрового підпису. При $r = 0$ обираються нові випадкові секретні ключи k_i.

Потім кожний користувач і за допомогою свого секретного ключа x_i та значення k_i обчислює свою долю підпису:

$$s_i = x_i^{rh_i} \; k_i \bmod p, \tag{2.22}$$

після чого генерується s – друге число колективного електронного цифрового підпису:

$$s = \prod_{i=1}^{t} s_i \bmod p. \tag{2.23}$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Колективним підписом є пара чисел (r, s).

Перевірка колективного підпису.

Перевірка підпису здійснюється за допомогою додаткового числа

$$y = \prod_{i=1}^{t} y_i^{h_i} \bmod p, \tag{2.24}$$

яке залежить від відкритих ключів y_i учасників підписання і відповідних геш-образів електронних документів h_i.

Якщо

$$s^z = (y^r \cdot r) \bmod p\,, \tag{2.25}$$

колективний цифровий підпис різних документів M_i, i = 1, 2, …, t, признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки 50оллективного підпису:

$$s^z = \left(\prod_{i=1}^{t} s_i\right)^z \bmod p = \left(\prod_{i=1}^{t} x_i^{zh_i}\right)^r \left(\prod_{i=1}^{t} k_i\right)^z \bmod p = \left(\prod_{i=1}^{t} y_i^{h_i}\right)^r \cdot \left(\prod_{i=1}^{t} r_i\right) \bmod p =$$
$$= (y^r \cdot r) \bmod p\,. \tag{2.26}$$

Приклад роботи протоколу колективного цифрового підпису різних документів.

Оберемо загальні параметри:

p = 5016532319260500262833579836643990377764 1,

z = 35413741398151157021.

Генерація ключів.

Нехай число користувачів t=3. Відповідні секретні ключі є

x_1 = 156758769780,

x_2 = 57869879875,

x_3 = 87697098098098.

Тоді відкрити ключі:

y_1 = 10888347551054112724481415051902837765574,

y_2 = 48485941766163329949274968777985639618768,

y_3 = 33731328335007308785829793117152674477075.

Формування колективного підпису.

Нехай геш-образи відповідних документів

h_1 = 1754698098876532,

h_2 = 14356475686824,

h_3 = 3465867599709.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i,

$k_1 = 42344769879$,

$k_2 = 11809875644$,

$k_3 = 20457089$

та обчислює значення r_i

$r_1 = 1043809209968646425278089612951543504869 7$,

$r_2 = 1208153961094469835768517101625601339244 3$,

$r_3 = 4202143136802684229174368791841205523678 8$.

Далі обчислюється добуток всіх r_i:

r = 889698798082340056151415969113810482724 4 – перше число колективного електронного цифрового підпису.

Потім кожний користувач і за допомогою свого секретного ключа x_i та значення k_i обчислює свою долю підпису :

$s_1 = 45725823840994203644906181284301023362599$,

$s_2 = 23734973385614987164918223107345158206628$,

$s_3 = 50162056813870998489648526071915537056 57$,

після чого генерується s – друге число колективного електронного цифрового підпису:

$s = 11948786941732176432163958499853693284223$.

Колективним підписом є пара чисел

(r, s) = (889698798082340056151415969113810482724 4,

11948786941732176432163958499853693284223).

Перевірка колективного підпису.

Перевірка підпису здійснюється за допомогою додаткового значення y, яке залежить від відкритих ключів y_i учасників підписання і відповідних геш-образів електронних документів h_i:

$y = 37005486959365706400864847606902300469516$.

Обчислюються

$s^z \mod p = 389125211184713920426199021649717715513 71$

та

$(y^r \cdot r) \mod p = 389125211184713920426199021649717715513 71$.

Оскільки s^z дорівнює добутку $y^r \cdot$ та r за модулем p, колективний цифровий підпис різних документів M_i признається справжнім.

Запропонований протокол колективного цифрового підпису не потребує апарату еліптичних кривих и може бути використаний в корпоративних мережах зв’язку.

2.3 Дослідження можливості злому секретного ключа електронного цифрового підпису за допомогою розподіленої комп'ютерної системи

Найбільш достовірним методом оцінки трудомісткості вирішення завдання є безпосереднє визначення часу й параметрів обчислень. З огляду на високий рівень розвитку сучасних мережних комп'ютерних технологій й апаратної частини, стає очевидною доцільність розробки системи на базі кластера як з фінансової, так і практичної точок зору. З огляду на це виникає необхідність у побудові високопродуктивного розподіленого програмного комплексу. Для вирішення описаного завдання авторами пропонується система – програмний комплекс, що реалізує методи паралельних обчислень.

Декомпозиція системи дозволила виділити п'ять основних елементів: підсистема віддаленого доступу, розподіляюча підсистема, підсистема генерації параметрів, обчислювальна підсистема, сервер баз даних для накопичення результатів обчислень.

При проектуванні системи було ухвалене рішення організувати можливість доступу клієнта до системи через будь-який найпростіший web-браузер. Тому підсистема віддаленого доступу дозволяє клієнтові за допомогою форм web-сторінок вводити вхідні дані й вибирати необхідне завдання, після вирішення якого підсистема виводить результати на новій сторінці.

Після запуску вирішення завдання розподіляюча підсистема аналізує дані, отримані від користувача, і рівними порціями розподіляє завдання між обчислювальними вузлами. Цей елемент є основною ланкою всієї системи, оскільки через нього відбувається взаємодія з клієнтом, сервером баз даних, і обчислювальними вузлами.

Підсистема генерації параметрів необхідна для генерації ряду вхідних параметрів при проведенні досліджень. Вона може перебувати на тому ж елементі кластера, що й розподіляюча підсистема, і повинна бути пов'язана із клієнтською частиною для внесення клієнтом параметрів. Вона також повинна бути пов'язана з підсистемою розподілу завдань для передачі сгенерованих параметрів.

Обчислювальна підсистема являє собою всі обчислювальні вузли системи, завданням яких є виконання основних математичних операцій.

Сервер баз даних для накопичування результатів обчислень являє собою будь-який ПК із встановленою на ньому системою керування базами даних. Поля таблиці бази даних містять таку інформацію: вхідні дані, введені користувачем, кількість ПК, що беруть участь в обчисленні, результат обчислень, затрачений час.

В основу системи закладено використання технології Java2 Enterprise Edition (J2EE), що дозволяє зняти обмеження щодо апаратного й програмного забезпечення елементів кластера [41; 42].

Підсистема віддаленого доступу побудована на базі технології JSP-сторінок (складової технології J2EE). Обробкою даних, введених користувачем, компіляцією java-тегів, JavaBean-компонентів й JSP-сторінок займається web-сервер Tomcat, встановлений на сервері-розподільнику й підтримуючий механізм JSP.

Розподіляюча підсистема являє собою JavaBean-компоненту, що взаємодіє з JSP-сторінкою. Вона створює потоки (кількість яких дорівнює кількості обчислювальних вузлів) і розподіляє між ними весь діапазон необхідних обчислень. Кожен потік запускає методи віддалених об'єктів EJB-компонентів (EJB - основна складова технології J2EE). Усі EJB-компоненти виконуються в середовищі контейнера J2EE-сумісного сервера додатків JBOSS на обчислювальних вузлах. Вони і виконують основні математичні перетворення. Після отримання даних, EJB-компонента починає роботу над завданням. Коли якась із компонентів знаходить вирішення, розподіляюча підсистема зупиняє роботу всіх інших компонентів.

Пропонована авторами система може бути розгорнута в локальній або в глобальній комп'ютерній мережі. Фізична топологія при цьому може бути довільною. Одна машина виділяється під сервер-розподільник, одна машина під сервер баз даних, а всі інші - під обчислювальні вузли. Клієнт може бути як елементом мережі, так і окремо підключеним до сервера розподільника по виділеній лінії, або через Інтернет.

За допомогою побудованої авторами системи вирішувалася математична задача: знайти x зі співвідношення a у степені порівняне з b за модулем p, де a, b й p – відомі (параметри, що задаються користувачем). Значення x відповідає секретному ключу, значення b відповідає відкритому ключу. Для невеликих значень параметрів таке завдання легко вирішується на одному комп'ютері. При збільшенні значень параметрів час обчислення x значно зростає. Перед авторами стояло завдання – визначити межу прийнятного часу обчислення секретного ключа на розподіленій комп'ютерній системі.

Для вирішення завдання використовувався розпаралелений алгоритм більших-малих кроків [43, 44], а також проводилася оцінка ефективності цього підходу.

Система була випробувана на базі кластера з 15 ПК конфігурації: AMD Sempron 2800+ 1,60 Ггц, 512 МБ ОЗП. Був визначений середній час обчислення дискретного логарифма залежно від кількості біт модуля p. Результати представлені в таблиці 2.1.

Таблиця 2.1– Результати обчислень

Параметр	Значення			
Кількість біт модуля p	35	40	43	45
Середній час обчислення, мс	26	358	4081	12620

Випробування показали, що ефективність обчислень при розпаралелюванні алгоритму більших-малих кроків значно перевищує традиційно визнану верхню межу, рівну 1. Однак обчислення секретного ключа в межах реального часу навіть при використанні 500 обчислювальних вузлів можливо тільки при довжині параметра p до 70-75 біт. При збільшенні кількості біт параметра p до рівня 500 і вище вирішення завдання за прийнятний час неможливо.

Таким чином, можливі спроби злому систем захисту інформації, побудованих на основі функції: піднесення до степеня по модулю, шляхом обчислення дискретного логарифму паралельним методом більших-малих кроків, на сьогодні не являють собою небезпеку.

3 РОЗРОБКА ТЕХНІЧНИХ ПРИНЦИПІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС

3.1 Оптимізація параметрів оптичного рефлектометра для виявлення неоднорідності

Виявлення та вимірювання параметрів неоднорідності волоконно-оптичного тракту – актуальна задача. Ці завдання виникають при монтажі тракту та обслуговуванні ВОСП. Зварювання оптичних волокон сучасними зварювальними апаратами забезпечує затухання в місці з'єднання $\Delta\alpha$ <0,01 дБ. При експлуатації ВОСП необхідно виявляти неоднорідності тракту, в тому числі і при НД. Діапазон локальних затухань при цьому лежить в області $\Delta\alpha$ = 0,01 -0,5 дБ.

Розглянемо можливості й умови оптимального знаходження неоднорідності в тракті в разі використання класичного методу OTDR.

У методі OTDR фіксується відбитий в тракті сигнал Рх, що зондує, а затухання на ділянці Δx визначається за формулою:

$$\Delta\alpha = 10 \log (Px - \Delta P) / Px, \quad (3.1)$$

де ΔP - втрати сигналу, що зондує на ділянці Δx.

Відповідно неоднорідність $\Delta\alpha$ викликає зміну сигналу ΔP / Рх на рівні 0,23 від $\Delta\alpha$.

У таблиці 3.1 наведені значення загасання $\Delta\alpha$ і викликаної їм зміна сигналу ΔP / Рх.

Таблиця 3.1 - Значення загасання $\Delta\alpha$ для сигналу ΔP / Рх

Параметр	Значення			
$\Delta\alpha$, дБ	0,1	0,5	0,01	0,05
ΔP / Рх	$2{,}3\cdot10^{-2}$	10^{-3}	$2{,}3\cdot10^{-3}$	10^{-4}

Ці втрати, як правило, залежать від величини зондірующего сигналу Рх, величини ділянки Δx та коефіцієнта загасання μ:

$$dP (\Delta x) = Px \, \Delta x \, \mu. \quad (3.2)$$

У випадку наявності на ділянці локальної неоднорідності до розподілених втрат додаються локальні втрати з-за цієї неоднорідності dP:

$$\Delta P = dP ((\Delta x) + dP). \quad (3.3)$$

Умова впевненого знаходження локальних неоднорідностей: локальні втрати сигналу перевищують розподілені втрати:

$$dP \geq dP\ (\Delta x). \qquad (3.4)$$

З урахуванням отримуємо величину впевненого знаходження локального загасання dα:

$$d\alpha \geq 4{,}3\ dP / Px = 4.3\ \Delta x\ \mu = 4.3\ GR\ (\Delta x) / S, \qquad (3.5)$$

де GR - коефіцієнт зворотного релеевського розсіювання ВС;

S - фактор зворотного розсіювання ВС.

Оцінки: для ОВС GR = -73 дБ (для Δx = 1 м), S = -30 дБ, для МВС S = -23 дБ

Ввівши GR o (Δxo) - коефіцієнт зворотного релеевского розсіювання при Δx = Δxo, отримуємо залежність величини мінімального локального загасання від просторового дозволу рефлектометру:

$$d\ \alpha\ (\Delta x) \geq 4.3\ (GR\ (\Delta x\ o)\ \Delta x) / S. \qquad (3.6)$$

У таблиці 3.2 для одномодового волокна наведені значення мінімального локального загасання при різних дозволах рефлектометру, отримані з умови (3.6).

Таблиця 3.2 - Значення мінімального локального загасання

Параметр	Значення						
Δx, м	1	5	10	50	100	500	1000
dα, дБ	$2\cdot10^{-4}$	10^{-3}	$2\cdot10^{-3}$	10^{-2}	$2\cdot10^{-2}$	0,1	0,2

Відношення сигнал / шум в точці виміру - x повинно бути більше відносної зміни сигналу від неоднорідності в тракті.

Звідси випливають вимоги на відношення сигнал / шум у точці вимірювання для різних значень локального загасання (табл. 3.3).

Таблиця 3.3 - Вимоги на ставлення сигнал / шум

Параметр	Значення			
Δα, дБ	0,1	0,05	0,01	0,001
$(Ps/Px)^{-1}$	0,023	0,0115	0,0023	0,000115
(Ps/Px)·x, дБ	16	19	26	36

Як показано вище, для відношення (Ps / Pn) = 1 величина загасання αL залежить від параметрів рефлектометру:

$$\alpha L = 0{,}5\ [Ps - Pno - \alpha c + GRo + 15 \log (\Delta x / \Delta xo) + 5 \log (N)]. \quad (3.7)$$

Для забезпечення вимірювання локального загасання dα необхідно забезпечити додатковий запас по відношенню сигнал-шум (Ps / Pn) dα і відповідно αL зменшиться:

$$\alpha L = 0{,}5\ [Ps - Pno - \alpha c + GRo + 15 \log (\Delta x / \Delta xo) + 5 \log (N) - (Ps / Pn)\ d\alpha] \quad (3.8)$$

У таблиці 3.4 наведені величини загасання αL, довжини ділянок контролю L в яких гарантується вимір локального загасання dα і часи вимірювань T для різних значень числа усереднення N, просторових дозволів dx. При цьому прийнято Δx o = 1м, GRo = -73 дБ, Pno = -70 дБм, Ps = 10дБм, αc = 6 дБ, α = 0,2 дБ / км.

Таблиця 3.4 – Величини загасання αL, довжини ділянок контролю L

Код	N (при dα =0,001 дБ , Δx = 5 м)				N (при dα = 0,01 дБ, Δx = 50 м)				N (при dα = 0,1 дБ, Δx = 500 м)			
	10^3	10^4	10^5	10^6	10^3	10^4	10^5	10^6	10^3	10^4	10^5	10^6
αL, дБ	-	2	4,5	7	7,5	10	12,5	15	20	22	24	27
L, км	-	10	22	35	37	50	62	75	100	110	120	135
T, с	-	1	22	350	0,37	5	62	750	1	11	120	1350

Таким чином, величина гарантованого (мінімального) локального загасання визначається параметрами рефлектометру і характеристиками волокна, а також режимами роботи рефлектометру:

$$d\alpha = 4.3\ 10 - 0.1\ [Ps - Pno - \alpha c + Gro - 2\alpha X + 15 \log (\Delta x / \Delta xo) + 5 \log (N)] \quad (3.9)$$

При постійному dα кордон режиму гарантованого виявлення локального загасання визначається виразом:

$$Ps - Pno - \alpha\ c + Gro - 2\alpha\ X + 15 \log (\Delta x / \Delta x\ o) + 5 \log (N) = A - const\ (39) \quad (3.10)$$

Особливості виявлення НД.

У цьому випадку аналіз можливостей гарантованого виявлення локального загасання необхідно вести з урахуванням обмежень по часу вимірювань Тізм для заданої довжини ВОСП - L.

При цьому маємо наступне Tm дорівнює подвоєнному добутку nL, поділеному на C, а Тизм приймає значення добутка Nта Tm, тоді:

$$d\alpha = 4.3\ 10 - 0.1\ [Ps - Pno - \alpha c + Gro - 2\alpha\ L + 15\ \log\ (\Delta x / \Delta xo) + 5\ \log\ (Тізм\ C / /2nL)] \quad (3.11)$$

При збільшенні часу вимірювань чутливість у виявленні локального загасання покращується, а збільшення довжини ВОСП знижує цю чутливість.

3.2 Завадостійкий спосіб передачі інформації в системах оптичного зв'язку

У традиційних системах передачі інформації використання повторювачів необхідно на протяжних лініях, оскільки за допомогою стандартного термінального устаткування може бути здійснений зв'язок тільки на обмежені стандартні відстані [50]. Підвищення бюджету потужності лінії передачі досягається шляхом використання електронних ретрансляторів або ВОП. Оптичні лінії зв'язку з використанням каскаду з декількох ВОП останнім часом успішно знаходять застосування в первинних мережах.

Однак з'єднання лазерних діодів, які працюють із використанням струму зсуву Ізс для підвищення швидкодії, з каскадом ВОП, які збільшують відстань між передавачем і приймачем, приводить до збільшення шуму.

Якщо на вході підсилювача сигнал дорівнює нулю, то на його виході спостерігається наявність шуму, обумовленого підсиленим спонтанним випромінюванням (ASE). Другий вид шуму обумовлений квантовою природою світла та визначається виразом:

$$\Delta n \Delta \varphi \geq 1\,, \quad (3.12)$$

де φ - фаза світлової хвилі;

n - число квантів, усереднені по оптичній ширині смуги Δv підсилювача та за часом Δt.

У реальному оптичному підсилювачі з коефіцієнтом підсилення GA та смугою пропускання Δx до цього квантового шуму додається згаданий вище шум спонтанного випромінювання.

Коефіцієнт шуму ВОП визначається з наступного виразу:

$$NF = \frac{2P_{ASE}}{h\nu_C \Delta\nu (G_n - 1)} \quad (3.13)$$

де P_{ASE} - потужність підсиленого спонтанного випромінювання;

h - постійна Планка;

υ_c - частота сигналу.

Для ербієвих оптичних підсилювачів (EDFA), широко застосовуваних у сучасних ВОСП із $G_n \gg 1$, типове значення NF лежить у межах 3 дБ ≤NF≤6дБ.

При включенні оптичних підсилювачів каскадно згідно [51] шум-фактор (NF) для двокаскадного підсилювача дорівнює:

$$NF_{2k} = NF_1 + \frac{NF_2 - 1}{G_1} \quad , \tag{3.14}$$

де NF_{2k} – сумарний шум-фактор або коефіцієнт шуму;

NF_1 - шум-фактор першого підсилювача;

NF_2 - шум-фактор другого підсилювача.

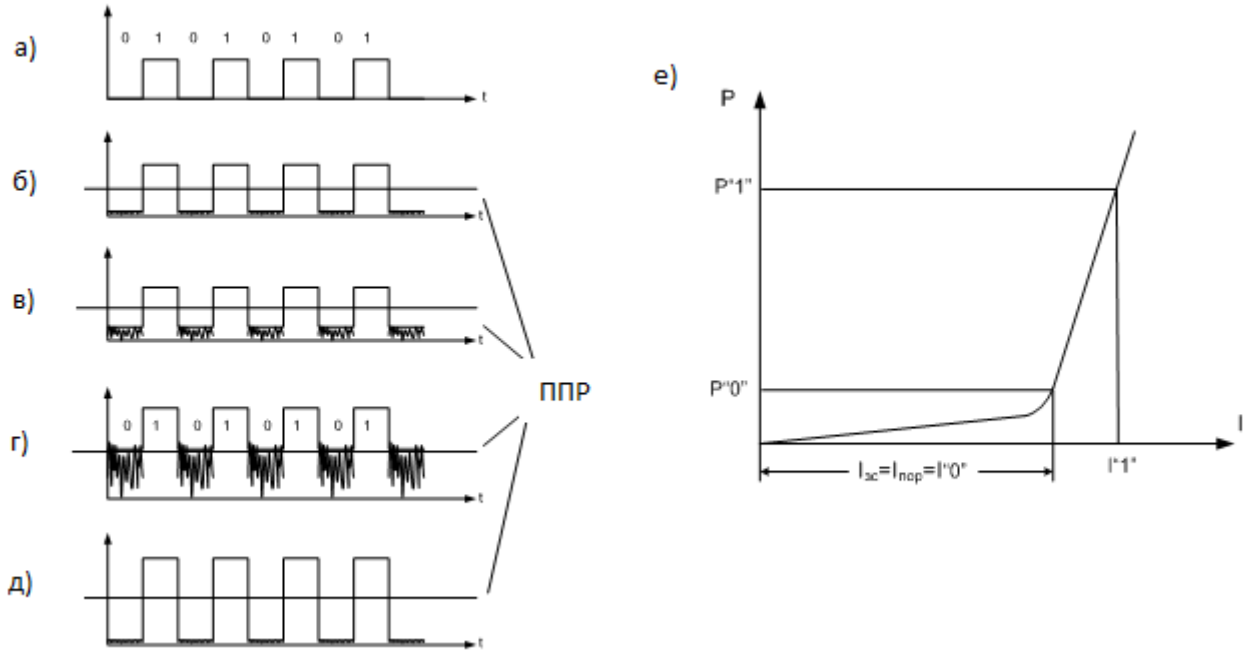
Для багатокаскадного підсилення із числом каскадів і, коефіцієнт шуму дорівнює:

$$NF_{2k} = NF_1 + \frac{NF_2}{G_1} + \cdots \frac{NF_i - 1}{G_1 G_2 \ldots G_i} \quad , \tag{3.15}$$

Крім шумів, створюваних ВОП у ВОЛЗ присутні шуми лазерного діода й волоконно-оптичного кабелю, що надходять на вхід ВОП. До цих складових шуму додається рівень потужності залишкового випромінювання накачування – допорогове випромінювання, яке створюється струмом зсуву Ізс.

При модуляції інтенсивності цифровими сигналами зростає затримка між стрибком струму інжекції та початком випромінювання [52]. Після стрибка струму спочатку збільшується напруга, а потім із затримкою на tc і часом наростання τ починається випромінювання. Ці величини визначають частотну характеристику джерела випромінювання.

Для того, щоб зменшити затримку tc між стрибком струму й початком випромінювання при цифровій модуляції, потрібно подати на джерело випромінювання струм зсуву Ізс близький до величини порогового струму Іп (рис. 3.1).



а) дані (електричний сигнал);
б) оптичний сигнал до подачі струму зсуву;
в) оптичний сигнал при подачі струму зсуву;
г) оптичний сигнал після оптичного підсилювача;
д) сигнал після схеми компенсації;
е) ват-амперна характеристика лазерного діоду.
ППР – поріг прийняття рішення.

Рисунок 3.1 – Діаграми оптичних сигналів

Струм зсуву Ізс підвищує швидкодію лазерного діода, одночасно створюючи значний рівень потужності залишкового випромінювання накачування, який є основною складовою шуму на вході ВОП.

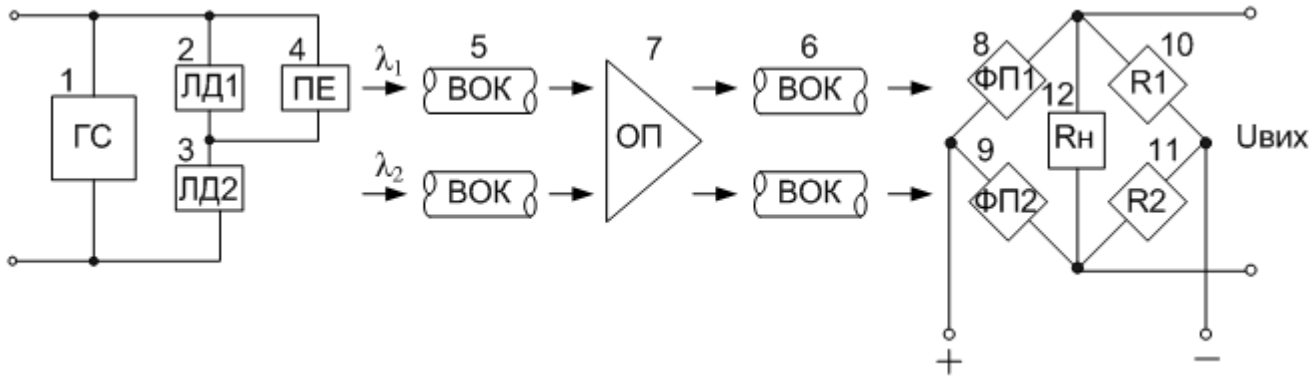
Варто враховувати, що особливістю роботи ВОП є підвищення підсилення слабких вхідних сигналів і зменшення підсилення більших вхідних сигналів. Це пояснюється тим [51], що в процесі збільшення оптичного сигналу відбувається поступове збідніння населеності інверсного середовища. Оскільки інверсне середовище ВОП розподілене по всій довжині активного волокна, ступінь збідніння в міру поширення посилюваного сигналу зростає і у квантово-енергетичному відношенні середовище прагне до насичення, тобто стану, коли населеності метастабільного основного рівня вирівнюються. Швидкість і ступінь збідніння населеності залежить від середньої потужності посилюваного оптичного сигналу, тобто від числа фотонів, яці переносяться сигнальним випромінюванням. У міру зростання числа сигнальних фотонів компенсоване число електронів на метастабільному рівні поступово слабшає та при деякім значенні потужності

вхідного оптичного сигналу наступає насичення. При цьому коефіцієнт підсилення прагне до одиниці, а при подальшому збільшенні потужності він навіть зменшується.

У цифрових системах при використанні каскаду ВОП наявність вищеописаних шумів може приводити до збільшення коефіцієнта помилок. При передачі “двійкової одиниці” додавання шумів до корисного сигналу не небезпечно, а навіть корисно, тому що сигнал одиниці додатково підсилюється. При передачі ”двійкового нуля” наявність шумів - слабкого сигналу, значно посилюваного каскадом ВОП, у порівнянні зі слабким підсиленням ”двійкової одиниці” може привести на прийомній стороні до розпізнавання ”двійкового нуля” як ”двійкової одиниці”.

Для підвищення завадостійкості ВОСП пропонується спосіб компенсації шумів [31], що придушує більшість складових шуму в лінії зв'язку, і саме головне, придушує основну складову шуму - залишкове випромінювання накачування - додаткове випромінювання, створюване струмом зсуві Ізс.

Рішення даного завдання досягається тим, що інформацію передають по оптичній лінії зв'язку одночасно по двох каналах від двох послідовно включених лазерних діодів на окремі фотоприймачі (рис. 3.2), після чого роблять порівняння переданих сигналів одним з відомих способів при передачі ”двійкового нуля”.

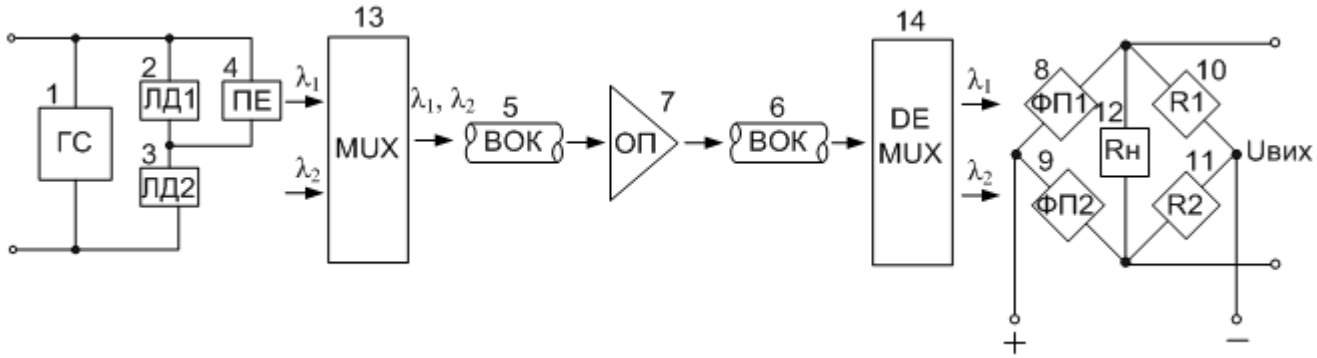


1- генератор електричних сигналів;
2, 3 - лазерні діоди;
4 - електронний перемикаючий елемент;
5, 6 - волокна волоконно-оптичного кабелю зв'язку;
7 - оптичний підсилювач;
8, 9 – фотоприймачі;
10, 11- резистори;
12 - резистор навантаження.

Рисунок 3.2 – Оптична лінія зв’язку

Схема порівняння відрізняється тим, що при передачі ”двійкового нуля” регулюють величину вихідного сигналу близької до нуля. Це дозволяє істотно понизити величину сумарного шуму, що надходить на фотоприймачі. Для коректного прийому ”двійкової одиниці” паралельно одному з лазерних діодів підключають електронний перемикач, що виконує його шунтування при досягненні значення струму накачування величини більшої порогової (рис. 3.1), тобто Ін>Іп.

Для скорочення кількості оптичних волокон сигнали від обох лазерних діодів випромінюючих на різних довжинах хвиль, мультиплексують, передають по одному оптоволокну, а на прийомній стороні після демультиплексування подають на фотоприймачі схеми порівняння (рис. 3.3).



1- генератор електричних сигналів;
2, 3 - лазерні діоди;
4 - електронний перемикаючий елемент;
5, 6 - волокна волоконно-оптичного кабелю зв'язку;
7 - оптичний підсилювач;
8, 9 – фотоприймачі;
10, 11- резистори;
12 - резистор навантаження.

Рисунок 3.3 – Оптична лінія зв’язку з застосуванням мультиплексорів

В запропоновоному способі передавання інформації по волоконно-оптичній або атмосферній лінії зв'язку по двох каналах при передачі двійкового нуля й по одному каналі при передачі двійкової одиниці, і компенсації шумів, які виникають при поданні струму накачування, що дорівнює граничному, а також дробових і теплових шумів, що виникають у лінії зв'язку на боці прийому, збільшує відношення сигнал/шум і підвищує надійність роботи каналу зв'язку при передаванні двійкового нуля.

Це дає змогу отримати технічний результат - підвищення завадостійкості системи передачі інформації, а саме підвищення відношення сигнал/шум без

зниження швидкості передавання цифрових даних і підсилення слабких шумів оптичним підсилювачем при передаванні двійкового нуля.

Сутність запропонованого способу пояснюється на прикладі одного з можливих устроїв, реалізуючих запропонований спосіб, де подана структурна схема способу (див. рис. 3.2, 3.3) та ват-амперна характеристика лазерного діода і діаграми передавання оптичного сигналу (див. рис. 3.1)

На рис.3.2 подана структурна схема способу передавання інформації по двох-волоконно-оптичній лінії зв'язку. Фотоприймачі 8, 9, резистори 10, 11, резистор навантаження 12 відтворюють один з можливих варіантів схеми порівняння.

На рис. 3.1 подано ват-амперна характеристика лазерного діоду, де Ізс - струм зсуву, Іпор - пороговий струм переходу лазерного діода з області спонтанного випромінювання в область вимушенного випромінювання, Р“0” - потужність випромінювання при Ізс рівному Іпор, що дорівнює передаванню двійкового нуля, Р“1” - потужність випромінювання при передаванні двійкової одиниці.

На рис.3.1 також наведені діаграми, що ілюструють передавання інформаційного сигналу, в оптичних лініях зв'язку, без схеми компенсації та зі схемою.

За першим варіантом пристрій працює наступним чином (див. рис. 3.2, 2.3): Цифровий сигнал двійкового нуля від генератора електричних сигналів 1 подається на лазерні діоди 2 і 3. Електронний перемикаючий елемент 4 є вимкненим і оптичні потужності Р01 та Р02, які випромінюються лазерними діодами 2 і 3 відповідно при подачі на них струмів зміщення Ізм1 та Ізм2, що дорівнюють пороговим струмам Іпор1 та Іпор2 лазерних діодів дозволяє підвищити швидкодію цих лазерних діодів, передається по волокну волоконно-оптичного кабелю зв'язку 5, 6, підсилюються оптичними підсилювачами 7 які значно більше підсилюють слабкі оптичні сигнали, ніж потужні і подається на фотоприймачі 8 і 9 які включені в схему порівняння і перетворюються в електричні сигнали. Резистори 10, 11 дозволяють відрегулювати схему порівняння так, що складові шумових завад, які виникають при передаванні по оптичній лінії оптичних сигналів Р01 та Р02, які суттєво підсилюються оптичними підсилювачами, компенсуються.

Це дозволяє суттєво знизити складову шуму на резисторі навантаження 12 схеми порівняння і завадити прийняттю оптичного випромінювання Р0 як випромінювання Р1 і підвищити завадостійкість лінії зв'язку. При передаванні двійкової одиниці електронний перемикаючий елемент 4 вимикає лазерний діод 2 і оптичне випромінювання потужністю Р1 від лазерного діода 3 подається в лінію зв'язку і далі на фотоприймач 9 схеми порівняння, де перетворюється на електричний сигнал який подається на резистор навантаження 12 і подальшу апаратуру зв'язку.

Завдяки тому, що електричні сигнали при передаванні двійкового нуля, віднімаються один з іншого в схемі порівняння, а електричний сигнал при

передаванні двійкової одиниці повністю передається й з'являється на вихід схеми порівняння, суттєво підвищується завадостійкість лінії зв'язку.

За іншим варіантом пристрій працює наступним чином (див. рис. 3.3). Схема працює аналогічно варіанту один крім того, що оптичні сигнали P01 та P02 на різних хвилях λ1, λ2 подаються на спектральний мультиплексор 13, де об'єднуються і подаються в одне волокно волоконно-оптичного кабелю зв'язку 5, підсилюються оптичним підсилювачем 7 і далі на спектральний демультиплексор 14, де розділяються за довжиною хвилі та подаються на фотоприймачі 8 та 9. Завдяки цьому виникає можливість у двічі зменшити кількість оптичних волокон у лінії зв'язку.

Завдяки тому, що у волоконно-оптичній лінії зв'язку виконується компенсація постійних складових шуму і компенсація залишкового випромінювання накачування P0, які виникають при передаванні потужностей P01 та P02, що відповідають двійковому нулю, для підвищення швидкодії лінії зв'язку завдяки використанню постійного струму зміщення, стає можливо суттєво підвищити завадостійкість без зниження швидкодії.

3.3 Модель автоматизованої системи малого підприємства, захищеної від інсайдерів

В області інформаційної безпеки найбільшу увагу організації приділяють, як правило, захисту від зовнішніх атак та конкурентної розвідки. З цієї причини майже всі кошти, що виділяються на забезпечення безпеки, спрямовуються на захист вразливих точок периметра мережі підприємства. Ситуація, що склалася, знайшла відповідне відображення і на ринку продуктів інформаційної безпеки — останніми роками пропонується широкий спектр різних засобів захисту від вірусів, хробаків, троянських програм та інших загроз ззовні.

Проте, поступово керівники підприємств починають усвідомлювати нову небезпеку. Вона надходить не від хакерів, спаму або випадкових вірусів, а від власних співробітників. Інсайдери знаходяться всередині самої організації і наділені цілком легальними повноваженнями, тому їм набагато простіше отримати доступ до необхідної інформації, ніж будь-якому зловмисникові ззовні. Відстежити випадки таких порушень політики безпеки теж набагато складніше, оскільки не відбувається несанкціонованого проникнення до автоматизованої системи. За статистикою останніх років, до 30% порушень політики безпеки відбувається внаслідок зловживань службовим становищем і повноваженнями або халатного відношення з боку працівників організації, і ще 30% порушень заподіюються колишніми працівниками підприємств [45].

Під автоматизованою системою малого підприємства автори розуміють комп'ютерну мережу, що складається з декількох автоматизованих робочих місць користувачів та комп'ютера адміністратора безпеки, який виконує функції сервера. До складу мережі також можуть входити комп'ютери керівників підприємства. Можливо також, що фунції адміністратора безпеки виконує один з керівників малого підприємства.

Найбільш вразливе для инсайдерів місце в такій системі - USB порти, оскільки через них можна скопіювати інформацію на різні переносні пристрої: флеш-карти, мобільні телефони, фотоапарати, плеєри тощо. Також певну загрозу представляють пристрої читання CD та DVD дисків, що підтримують функцію запису. Комерційні продукти, покликані вирішити цю проблему, зазвичай являють собою програмне забезпечення, яке надає можливість обмежувати і контролювати доступ до портів USBі дискових пристроїв. Вартість таких програм може сягати 500 у.о. [46]

Запропонована модель захищеної мережі малого підприємства передбачає замість використання програмних засобів розмежування доступу до USB портів і дискових пристроїв їхню фізичну відсутність [47, 48]. Авторами пропонується не обладнувати автоматизовані робочі місця користувачів системи пристроями читання дисків, а USB порти відключати від материнської плати. Якщо фізичне відключення неможливе, відсутність доступу до портів пропонується забезпечити засобами BIOS, доступ до налаштувань якого має захищатися паролем [49].

Модель, запропонована авторами, передбачає наявність робочих портів USB і пристроїв читання CD та DVD дисків на машинах керівного складу та/або адміністратора безпеки. Таким чином, згідно з моделлю, запис інформації з мережі на зовнішні пристрої і її зчитування з них відбувається під контролем відповідальних осіб. Ризик витоку інформації описаним шляхом мінімізується.

В результаті, запропонована модель дозволяє економити кошти підприємства, по-перше, на пристроях читання CD та DVD дисків і, по-друге, на програмному забезпеченні, яке використовується для розмежування доступу до цих пристроїв і портів USB. Надійність запропонованого методу забезпечується фізичним відключенням потенційно небезпечних пристроїв та портів.

ВИСНОВКИ

Розроблено математичні та технічні моделі захисту інформації від несанкціонованого доступу в комп’ютерних системах та мережах.

Запропоновані та запатентовані нові протоколи колективного цифрового підпису для захисту електронних документів, їх цілісності та підтвердження авторства. Нові протоколи дозволяють підписувати електронні документи колективу авторів, при цьому учасники підписання можуть бути як рівноправними, так і нерівноправними, й підписувати єдиний документ, або кожен свій електронний документ. Наведено процедури перевірки підписаних документів. Запропоновані протоколи ілюструються числовими прикладами з використанням реальних розмірів параметрів.

Збудовано розподілена комп'ютерна система для дослідження можливості злому секретного ключа електронного цифрового підпису. Практичне доведено поріг криптостійкості систем електронного цифрового підпису на прикладі схеми ЕЦП ЕльГамаля. Описано програмний комплекс, в якому реалізуються паралельні обчислення для прискорення знаходження секретного ключа електронного цифрового підпису.

Запропоновані нові технічні рішення захисту інформації в системах передачі даних, яки засновани на використанні волоконно-оптичних технологій. Розроблено методи оптимізації параметрів оптичного рефлектометра для виявлення неоднорідності волоконно-оптичного тракту. Запропоновано та запатентовано новий спосіб, який дозволяє підвищити завадостійкість волоконно-оптичних ліній зв’язку. Рішення даного завдання досягається тим, що інформацію передають по оптичній лінії зв'язку одночасно по двох каналах від двох послідовно включених лазерних діодів на окремі фотоприймачі, після чого роблять порівняння переданих сигналів одним з відомих способів при передачі ”двійкового нуля”.

Збудовано модель автоматизованої системи малого підприємства, захищеної від інсайдерів. Інсайдери знаходяться всередині самої організації і наділені цілком легальними повноваженнями, тому їм набагато простіше отримати доступ до необхідної інформації, ніж будь-якому зловмисникові ззовні. Запропонована модель дозволяє економити кошти підприємства, по-перше, на пристроях читання CD та DVD дисків і, по-друге, на програмному забезпеченні, яке використовується для розмежування доступу до цих пристроїв і портів USB. Надійність запропонованого методу забезпечується фізичним відключенням потенційно небезпечних пристроїв та портів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Брассар, Ж. Современная криптология [Текст] / Брассар Ж. – М.: Изд-во ПОЛИМЕД, 1999. – 180 с.

2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Текст] / М.А. Иванов. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.

3. Молдовян, А.А. Криптография [Текст] / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов; Серия «Учебники для вузов. Специальная литература». – СПб.: Изд-во «Лань», 2000. –224 с.

4. Фергюсон, Н. Практическая криптография [Текст] / Н. Фергюсон, Б. Шнайер – М.: Диалектика, 2005. – 424 с.

5. Смарт, Н. Криптография [Текст] / Н. Смарт – М.: Техносфера, 2005. – 528 с.

6. Неласая, А.В. Протоколы коллективной цифровой подписи. [Текст] / А.В. Неласая , Г.Л. Козина // Збірник наукових статей «Управління розвитком». - 2008.- №7, С.9-10.

7. Неласая, А.В Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривих [Текст] / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Радіоелектроніка, інформатика, управління. - 2008. - № 1. - С. 127-133.

8. Нікуліщев, Г.І. Колективний електронний цифровий підпис [Текст] / Нікуліщев Г.І.// Світ інформації та телекоммунікацій-2008. Матеріали V Міжнародної науково-технічної конференції студентства та молоді, 9-10 квітня 2008 р., Київ. – 2008, С. 58.

9. Артамонов А.В. Применение алгоритма Шнорра в протоколе коллективной подписи [Текст] / А.В. Артамонов, Е.Б. Маховенко // Проблемы информационной безопасности в системе высшей школы: Материалы XIV Всероссийской научной конференции, Санкт-Петербург, 6-9 марта 2007. – С. 17-18.

10. Гортинская Л.В. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 [Текст] / Л.В. Гортинская, Н.А. Молдов'ян, Г.Л. Козина // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – 2007. – №.2(15). – С.82-86.

11. Галанов, А.И. Множественная подпись: новые решения на основе понятия коллективного открытого ключа [Текст]/ А.И. Галанов, Н.А. Молдовян, М.А. Еремеев // Информационно-управляющие системы, №1, 2008 – С. 34-36.

12. Пат. 31105 Україна, МПК (2006) H03M 5/00, G09C 1/00, H03M 7/00. Спосіб формування і перевірки достовірності колективного електронного цифрового

підпису для засвідчення електронного документа [Текст] / Л.М. Карпуков , Г.Л. Козіна , О.А. Молдов'ян , М.А. Молдов'ян ; заявник і патентовласник Запорізький національний технічний університет. – № u200713254; заявл. 28.11.07; опубл. 25.03.08, Бюл. № 6.

13. Неласая, А.В. Специальные схемы электронной цифровой подписи. [Текст] / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008., С. 212-213

14. Козина, Г.Л. Мультиагентная модель коллективной цифровой подписи по схеме Шнорра. [Текст] / Г.Л. Козина, А.С. Горецкий // Збірник наукових статей «Управління розвитком». - 2008. -№15, С.32-33

15. Андрущенко, Д.М. Реализация процедур выработки параметров для системы электронной цифровой подписи по ГОСТ 34.310–95 [Текст] / Д.М. Андрущенко, Г.Л. Козина // Тези доповідей науково-практичної конференції "Захист в інформаційно-комунікаційних системах". – Киев: НАУ, 2007. – С. 38–39.

16. Ростовцев, А. Г. Методы криптоанализа классических шифров [Текст] / А. Г. Ростовцев, Н. В. Михайлова –М.: Наука, 1995. –208 с.

17. Горбенко И.Д. Сравнительный анализ блочных симметричных шифров, представленных в проекте NESSIE [Текст] / И.Д. Горбенко, С.А. Головашич, А.Н. Лепеха // Радиотехника: Всеукр. межвед. науч.-техн. сб., 2003. Вып. 134. С. 26 –40

18. Шнайер Б. Слабые места криптографических систем [Электронный ресурс]. – Режим доступу: http://algolist.manual.ru/defence/attack/cryptholes.php

19. Никулищев, Г.И. Оценка стойкости блочно-потокового шифра и методы ее повышения [Текст] / Г.И. Никулищев, Г.Л. Козина // Технології безпеки інформації: Збірка тез доповідей учасників IV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (14 квітня 2006 р., м. Київ) / Уклад.: А.А. Співак. К.: 2006. – С.31

20. Андрущенко, Д.М. Об эффективности параллельных вычислений при проведении криптоанализа асимметричных алгоритмом [Текст] / Д.М. Андрущенко, Г.Л. Козина, Д.М. Пиза // Методы и технические средства обеспечения безопасности информации: Материалы XVI Общероссийской научно-технической конференции. – СПб.: Изд-во Политехн. ун-та, 2007. – С. 57

21. Андрущенко, Д.М. Про можливості злому секретного ключа електронного цифрового підпису за допомогою розподіленої комп'ютерної системи [Текст] / Д.М. Андрущенко, Г.Л. Козіна, С.В. Вармінський // Удосконалення діяльності ОВС України з попередження й розкриття злочинів та інших правопорушень: Матеріали Всеукраїнської науково-практичної конференції. – Запоріжжя: Юридичний ін-т МВС України, 2007. – Ч.1. – С. 102–104.

22. Андрущенко, Д.М. Практическая оценка стойкости асимметричных криптосистем [Текст] / Д.М. Андрущенко, Г.Л. Козина, Д.М. Пиза // Проблемы информационной безопасности. – 2008. - № 1. – С. 57-62.

23. Андрущенко, Д.М. Тестирование и анализ решения задачи дискретного логарифмирования на распределенной вычислительной системе [Текст] / Д.М. Андрущенко, Д.И. Бондаревич, Г.Л. Козина // Технології безпеки інформації. Збірка тез доповідей учасників V Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (19 квітня 2007 р., м. Київ) / Уклад.: Б.В. Берлог. – К., 2007. – С. 16-17.

24. Андрущенко, Д.М. Параллельный алгоритм решения задачи дискретного логарифмирования [Текст] / Д.М. Андрущенко, Г.Л. Козина, Л.М. Карпуков // Технології безпеки інформації: Збірка тез доповідей учасників V Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (19 квітня 2007 р., м. Київ) / Уклад.: Б.В. Берлог. – К., 2007. – С. 16-17.

25. Андрущенко, Д.М. Система параллельного решения задачи дискретного логарифмирования [Текст] / Д.М. Андрущенко, Г.Л. Козина, Р.К. Кудерметов // Захист в інформаційно-комунікаційних системах: Тези доповідей науково-практичної конференції. – Київ: НАУ, 2007. – С. 43–44.

26. Нікуліщев, Г.І. Стеганографічні методи захисту інформації на основі мережевих протоколів. [Текст] / Г.І. Нікуліщев // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008., С. 210-211

27. Андрущенко, Д.М. Анализ стойкости цифровых водяных знаков к компрессии изображений [Текст] / Д.М. Андрущенко, Г.Л. Козина // Збірник наукових робіт «Управління розвитком». – 2008. – №7. – С. 4–5.

28. Андрущенко, Д.М. Программный комплекс «ПКАЭРСС» для анализа эффективности робастных стеганосистем [Текст] / Д.М. Андрущенко, Г.Л. Козина // Збірник наукових робіт «Управління розвитком». – 2008. – №15. – С. 9–11.

29. Андрущенко, Д.М. Выбор параметров метода Коха и Жао стеганографического [Текст] / Д.М. Андрущенко, Г.Л. Козина // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008. С. 216–217.

30. Андрущенко, Д.М. Анализ стойкости метода Коха-Жао стеганографического встраивания информации в статические изображения [Текст] / Д.М. Андрущенко, Г.Л. Козина // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2008. № 2 (17). С. 70–74.

31. Пат. 17646 Україна, МПК (2006) H04B10/12. Спосіб передачі інформації в системах оптичного зв'язку [Текст] / О.В. Щекотихін, Р.Ю. Корольков, В.І.

Корнійчук; заявник і патентовласник Запорізький національний технічний університет. – № u20060234; заявл. 03.03.2006; опубл. 16.10.2006, Бюл. № 10.

32. Карпуков, Л.М. Защита информации в волоконно-оптических линиях связи [Текст] / Л.М. Карпуков, О.В. Щекотихін, В.И. Мысленков // Вісник Хмельницького національного університету. – 2007. №2. С.180-182.

33. Карпуков, Л.М. Завадостійкий спосіб передачі інформації в системах оптичного зв'язку [Текст] / Л.М. Карпуков, О.В. Щекотихін, Р.Ю. Корольков // Вісник Хмельницького національного університету. –2007, №2. С.188-192.

34. Щекотихин, О.В. Анализ возможности НСД в атмосферных лазерных системах передачи [Текст]/ О.В. Щекотихин, И.Н. Сметанин, Л.М. Карпуков // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008. С.90-92

35. Ростовцев, А.Г. Введение в криптографию с открытым ключом [Текст] / А.Г. Ростовцев, Е.Б. Маховенко – С-Петербург: Мир и семья, 2001. – 312 с.

36. Молдовян, Н.А. Практикум по криптосистемам с открытым ключом [Текст] / Н.А. Молдовян – СПб.: БХВ-Петербург, 2007. – 304с.

37. Рябко, Б.Я. Криптографические методы защиты информации [Текст] / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия – Телеком, 2005. – 229с.

38. ДСТУ 4145: 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння [Текст]: – Чинний від 2002-03-13. – К.: Держстандарт України, 2002. – 38 с. – (Національний стандарт України).

39. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Текст].– 12 с. – (Государственный стандарт Российской Федерации).

40. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования [Текст]: 1995. – Чинний від 1998-04-16. – К.: Держстандарт України, 1995. – 12 с. – (Межгосударственный стандарт).

41. Кэри, И.А. Разработка корпоративных Java-приложений с использованием J2EE и UML [Текст] / И.А. Кэри, Х.З. Ахмед– М.: Издательский дом "Вильямс", 2002. – 272 с.

42. Хорстманн, К.С. Библиотека профессионала. Java 2. Том 2. Тонкости программирования [Текст] / К. С. Хорстманн, Г. Корнелл – М.: Издательский дом "Вильямс", 2002. – 1120 с.

43. Menezes, A. A handbook of applied cryptograhy [Текст] / A. Menezes, P. van Oorchot, S. Vanstone – CRC Press, 1996. – 603 с.

44. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии [Текст] / О.Н. Василенко – М.: МЦНМО.– 2003. – 328 с.

45. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности [Текст] / В. Ю. Скиба, В. А. Курбатов– СПб.: Питер, 2008. – 320 с.

46. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / А.В Соколов, В.Ф. Шаньгин. – М.:ДМК Пресс, 2002. – 656 с.

47. Говоров, А.О. Модель автоматизованої системи малого підприємства, захищеної від інсайдерів [Текст] / А.О. Говоров, Г.І. Нікуліщев // Збірник наукових статей «Управління розвитком», 2008.- №7, С.31-32.

48. Govorov, A. “The Model of a Small Corporate Network, Protected from Insiders” [Текст] / A. Govorov, G. Nikulischev, Y. Grosfeld //Modern problems of radio engineering, telecommunicarions and computer science: Conference papersTCSET’2008. Lviv-Slavsko, 2008. – p. 474.

49. Белунцов В., Настройка BIOS. Практическое руководство Серия: Гарантированный результат [Текст] / В. Белунцов. – Издательство: ТехБук, 2004. – 400 с.

50. Корнейчук В.И. Волоконно-оптические системи передачи [Текст] / В.И. Корнейчук, И.П. Панфілов - Одесса: Друк, 2001. - 435 с.

51. Скляров О.К. Волоконно-оптические сети системі святи [Текст] / О.К. Скляров - М: Салон-Пресс, 2004. -265 с.

52. Оптические системы передачи [Текст] / Под ред. В.И. Иванова. -М.: Радио и связь, 1994. -224с.

Додаток А
Перелік публікацій за тематикою НДР

1. Неласая, А.В. Протоколы коллективной цифровой подписи. [Текст] / А.В. Неласая , Г.Л. Козина // Збірник наукових статей «Управління розвитком» - 2008.- №7, С.9-10.

2. Неласая, А.В Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривих [Текст] / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Радіоелектроніка, інформатика, управління. - 2008. - № 1. - С. 127-133.

3. Нікуліщев, Г.І. Колективний електронний цифровий підпис [Текст] / Нікуліщев Г.І.// Світ інформації та телекоммунікацій-2008. Матеріали V Міжнародної науково-технічної конференції студентства та молоді, 9-10 квітня 2008 р., Київ. – 2008, С. 58.

4. Гортинская Л.В. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 [Текст] / Л.В. Гортинская, Н.А. Молдов'ян, Г.Л. Козина // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – 2007. – №.2(15). – С.82-86.

5. Пат. 31105 Україна, МПК (2006) H03M 5/00, G09C 1/00, H03M 7/00. Спосіб формування і перевірки достовірності колективного електронного цифрового підпису для засвідчення електронного документа [Текст] / Л.М. Карпуков , Г.Л. Козіна , О.А. Молдов'ян , М.А. Молдов'ян ; заявник і патентовласник Запорізький національний технічний університет. – № u200713254; заявл. 28.11.07; опубл. 25.03.08, Бюл. № 6.

6. Неласая, А.В. Специальные схемы электронной цифровой подписи. [Текст] / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008., С. 212-213

7. Козина, Г.Л. Мультиагентная модель коллективной цифровой подписи по схеме Шнорра. [Текст] / Г.Л. Козина, А.С. Горецкий // Збірник наукових статей «Управління розвитком» - 2008. -№15, С.32-33

8. Андрущенко, Д.М. Реализация процедур выработки параметров для системы электронной цифровой подписи по ГОСТ 34.310–95 [Текст] / Д.М. Андрущенко, Г.Л. Козина // Захист в інформаційно-комунікаційних системах: Тези доповідей науково-практичної конференції. – Киев: НАУ, 2007. – С. 38–39.

9. Никулищев, Г.И. Оценка стойкости блочно-потокового шифра и методы ее повышения [Текст] / Г.И. Никулищев, Г.Л. Козина // Технології безпеки інформації: Збірка тез доповідей учасників IV Всеукраїнської науково-практичної

конференції студентів, аспірантів та молодих вчених (14 квітня 2006 р., м. Київ) / Уклад.: А.А. Співак. К.: 2006. – С.31

10. Андрущенко, Д.М. Об эффективности параллельных вычислений при проведении криптоанализа асимметричных алгоритмом [Текст] / Д.М. Андрущенко, Г.Л. Козина, Д.М. Пиза // Методы и технические средства обеспечения безопасности информации: Материалы XVI Общероссийской научно-технической конференции. – СПб.: Изд-во Политехн. ун-та, 2007. – С. 57

11. Андрущенко, Д.М. Про можливості злому секретного ключа електронного цифрового підпису за допомогою розподіленої комп'ютерної системи [Текст] / Д.М. Андрущенко, Г.Л. Козіна, С.В. Вармінський // Удосконалення діяльності ОВС України з попередження й розкриття злочинів та інших правопорушень: Матеріали Всеукраїнської науково-практичної конференції. – Запоріжжя: Юридичний ін-т МВС України, 2007. – Ч.1. – С. 102–104.

12. Андрущенко, Д.М. Практическая оценка стойкости асимметричных криптосистем [Текст] / Д.М. Андрущенко, Г.Л. Козина, Д.М. Пиза // Проблемы информационной безопасности. – 2008. - № 1. – С. 57-62.

13. Андрущенко, Д.М. Тестирование и анализ решения задачи дискретного логарифмирования на распределенной вычислительной системе [Текст] / Д.М. Андрущенко, Д.И. Бондаревич, Г.Л. Козина // Технології безпеки інформації. Збірка тез доповідей учасників V Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (19 квітня 2007 р., м. Київ) / Уклад.: Б.В. Берлог. – К., 2007. – С. 16-17.

14. Андрущенко, Д.М. Параллельный алгоритм решения задачи дискретного логарифмирования [Текст] / Д.М. Андрущенко, Г.Л. Козина, Л.М. Карпуков // Технології безпеки інформації: Збірка тез доповідей учасників V Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (19 квітня 2007 р., м. Київ) / Уклад.: Б.В. Берлог. – К., 2007. – С. 16-17.

15. Андрущенко, Д.М. Система параллельного решения задачи дискретного логарифмирования [Текст] / Д.М. Андрущенко, Г.Л. Козина, Р.К. Кудерметов // Захист в інформаційно-комунікаційних системах: Тези доповідей науково-практичної конференції. – Київ: НАУ, 2007. – С. 43–44.

16. Нікуліщев, Г.І. Стеганографічні методи захисту інформації на основі мережевих протоколів. [Текст] / Г.І. Нікуліщев // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008., С. 210-211

17. Андрущенко, Д.М. Анализ стойкости цифрових водяных знаков к компрессии изображений [Текст] / Д.М. Андрущенко, Г.Л. Козина // Збірник наукових робіт «Управління розвитком». – 2008. – №7. – С. 4–5.

18. Андрущенко, Д.М. Программный комплекс «ПКАЭРСС» для анализа эффективности робастных стеганосистем [Текст] / Д.М. Андрущенко, Г.Л. Козина // Збірник наукових робіт «Управління розвитком». – 2008. – №15. – С. 9–11.

19. Андрущенко, Д.М. Выбор параметров метода Коха и Жао стеганографического [Текст] / Д.М. Андрущенко, Г.Л. Козина // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008. С. 216–217.

20. Андрущенко, Д.М. Анализ стойкости метода Коха-Жао стеганографического встраивания информации в статические изображения [Текст] / Д.М. Андрущенко, Г.Л. Козина // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. –2008. № 2 (17). С. 70–74.

21. Пат. 17646 Україна, МПК (2006) H04B10/12. Спосіб передачі інформації в системах оптичного зв'язку [Текст] / О.В. Щекотихін, Р.Ю. Корольков, В.І. Корнійчук; заявник і патентовласник Запорізький національний технічний університет. – № u20060234; заявл. 03.03.2006; опубл. 16.10.2006, Бюл. № 10.

22. Карпуков, Л.М. Защита информации в волоконно-оптических линиях связи [Текст] / Л.М. Карпуков, О.В. Щекотихін, В.И. Мысленков // Вісник Хмельницького національного університету. – 2007. №2. С.180-182.

23. Карпуков, Л.М. Завадостійкий спосіб передачі інформації в системах оптичного зв'язку [Текст] / Л.М. Карпуков, О.В. Щекотихін, Р.Ю. Корольков // Вісник Хмельницького національного університету. – 2007. №2. С.188-192.

24. Щекотихин, О.В. Анализ возможности НСД в атмосферных лазерных системах передачи [Текст]/ О.В. Щекотихин, И.Н. Сметанин, Л.М. Карпуков // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: Тези доповідей IV Міжнародної науково-практичної конференції (24–26 вересня 2008 р., м. Запоріжжя). – Запоріжжя: ЗНТУ, 2008. С.90-92

25. Говоров, А.О. Модель автоматизованої системи малого підприємства, захищеної від інсайдерів [Текст] / А.О. Говоров, Г.І. Нікуліщев // Збірник наукових статей «Управління розвитком» - 2008.- №7, С.31-32.

26. Govorov, A. "The Model of a Small Corporate Network, Protected from Insiders" [Текст] / A. Govorov, G. Nikulischev, Y. Grosfeld //Modern problems of radio engineering, telecommunicarions and computer science: Conference papersTCSET'2008. Lviv-Slavsko, 2008. – p. 474.