

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ. О. С. ПОПОВА
КОЛЕДЖ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ**

IV студентська науково-технічна конференція

**ТЕЛЕКОМУНІКАЦІЙНІ, ІНФОРМАЦІЙНІ
ТА КОМП'ЮТЕРНІ МЕРЕЖІ І СИСТЕМИ:
ТЕПЕРІШНЄ ТА МАЙБУТНЄ**

22 лютого 2014 року

Збірка тез

Одеса, 2014

Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє: матеріали IV студентської науково-технічної конференції, м. Одеса, 22 лютого 2014 року – Одеса, КЗІ ОНАЗ, 2014. – 34 с.

Дана збірка містить тези матеріалів, що представлені на IV студентську науково-технічну конференцію «**Телекомунікаційні, інформаційні та комп'ютерні мережі та системи: теперішнє та майбутнє**», що проводиться 22 лютого 2014 р. в коледжі зв'язку та інформатизації Одеської національної академії зв'язку ім. О.С. Попова.

До збірки включені тези доповідей за секціями:

- телекомунікаційних систем та мереж;
- радіозв'язку, радіомовлення та телебачення;
- інформаційних мереж та комп'ютерних наук.

Робоча мова конференції – українська, російська.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Петрусенко С. Ю.	голова оргкомітету, директор коледжу зв'язку та інформатизації ОНАЗ ім. О. С. Попова
Горлінська О. Ю.	заступник голови оргкомітету, заступник директора з навчальної роботи
Козаченко Л. О.	голова циклової комісії систем радіозв'язку, радіомовлення та телебачення
Кокорєва З. Р.	голова циклової комісії телекомунікаційних систем та мереж
Орлова Л. Б.	секретар оргкомітету, викладач циклової комісії інформаційних мереж та оргтехніки
Малюта С. О.	викладач циклової комісії інформаційних мереж та оргтехніки
Трофименко Ю. В.	завідувач денного відділення, викладач циклової комісії систем радіозв'язку, радіомовлення та телебачення
Коровкін В. В.	голова ради студентського самоврядування, студент групи О-41

ЖУРІ КОНФЕРЕНЦІЇ

Каптур В. А.	голова, к.т.н, с.н.с., проректор з наукової роботи ОНАЗ ім. О. С. Попова
<i>секція телекомунікаційних систем та мереж</i>	
Бондаренко О. В.	д.т.н, професор, зав. кафедри волоконно-оптичних ліній зв'язку ОНАЗ ім. О. С. Попова
Лісової І. П.	д.т.н, професор, професор кафедри телекомунікаційних систем ОНАЗ ім. О. С. Попова
<i>секція систем радіозв'язку, радіомовлення та телебачення</i>	
Тігарєв А. М.	к.т.н., доцент, доцент. кафедри комп'ютерно-інтегрованих технологічних процесів і виробництв ОНАЗ ім. О. С. Попова
Баляр В. Б.	старший викладач кафедри телебачення та радіомовлення ОНАЗ ім. О. С. Попова

секція інформаційних мереж та комп'ютерних наук

Васілю Є. В.	д.т.н, доцент, директор навчально-наукового інституту радіо, телебачення, електроніки ОНАЗ ім. О. С. Попова
Рожновський М. В.	к.т.н., доцент кафедри технічної електродинаміки та систем радіозв'язку ОНАЗ ім. О. С. Попова

ЗМІСТ

Секція телекомунікаційних систем та мереж

1. Орел М. М. Дослідження багатомодульної конструкції оптичного кабелю
2. Кравцов К. В., Язаджи М. М. Використання оптичних підсилювачів в системах DWDM
3. Зубенко М. Г., Омельченко О. П. Проблеми та перспективи впровадження пасивних оптичних мереж PON
4. Коровкіна К. В. Використання вейвлет-функцій для відновлення неперервних сигналів

Секція радіозв'язку, радіомовлення та телебачення

1. Таранішин А. О. Інтегроване (гібридне) мовне широкосмугове телебачення
2. Царев А. А. Застосування чипів серії nRF 24 L у сучасній техніці зв'язку
3. Кислов Д. Ф. Голограма як високоперспективний носій інформації

Секція інформаційних мереж та комп'ютерних наук

1. Вешкін Д. С. Стеганографія в сучасному світі
2. Палій О. Г. Дослідження покриття WLAN AP NanoStation loco M 2
3. Міненко В. А. Асиметрична криптосистема RSA та цифровий підпис на її основі

**ДОСЛІДЖЕННЯ БАГАТОМОДУЛЬНОЇ КОНСТРУКЦІЇ
ОПТИЧНОГО КАБЕЛЮ**

Орел М.М., студент 4 курсу, група О-412, спеціальність 5.05090302
«Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки».

Науковий керівник: викладач вищої категорії **Кокорєва З.Р.**

***Анотація.** Наведено розрахунок та оптимізацію багатомодульних багатоповивних конструкцій осердя оптичних кабелів. Подано рекомендацію щодо послідовності вибору конструктивних елементів осердя багатомодульних оптичних кабелів.*

На сьогоднішній день [1] оптичні кабелі (ОК) отримали широке застосування на транспортних телекомунікаційних мережах зв'язку і на мережах абонентського доступу, і сприяють передачі великої кількості каналів на задані відстані. Тим самим забезпечують більшу пропускну та інформаційну здатність волоконно-оптичних систем передачі. Сьогодні в Україні для цієї мети виробляють ОК модульного типу з повивним скручуванням, який наведено на рис. 1.

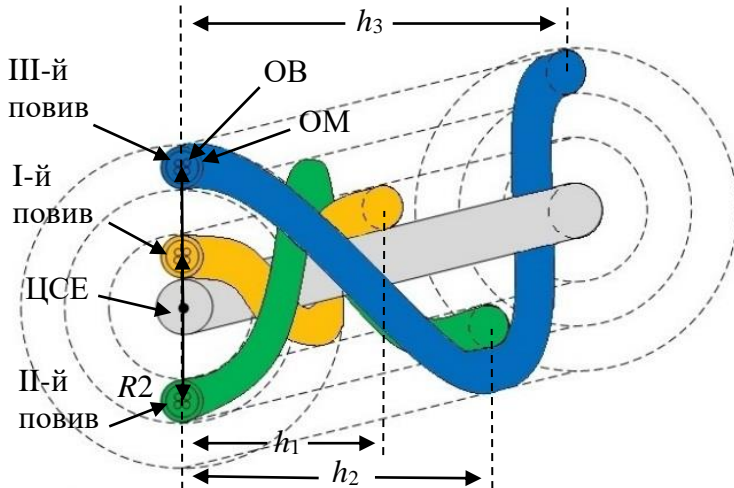


Рисунок 1 – Спіральне укладання ОМ навколо ЦСЕ в осерді багатоволоконних ОК

Проте, у даний час в Україні відсутні керівні нормативно-технічні документи з розробки конструкції ОК, а існуючі матеріали є інновацією фірм-виробників. Тому методики та методичні аспекти розрахунку параметрів, вибору елементів конструкції ОК та її модернізація є актуальними і необхідними.

Розробка конструкції осердя кабелю проводиться, виходячи з заданої кількості оптичних волокон (ОВ), потім вибирається модель кабелю за кількістю ОВ з певним числом оптичних модулів (ОМ) й заповнювальних елементів (ЗЕ), діаметром ОМ та центрального силового елемента (ЦСЕ) і розраховується допустиме розтягувальне навантаження (F_k), яке повинне відповідати очікуваному значенню, зазначеному в технічній умові (ТУ) [4].

В якості критерію для розрахунку допустимого розтягувального навантаження ОК застосовують допустиме відносне видовження кабелю (ϵ_{dk}) [2], за формулою (1):

$$\epsilon_{dk} = -1 + \sqrt{1 + \frac{4 \cdot \pi^2 \cdot R^2}{h^2} \cdot \left(\frac{2\Delta R}{R} - \frac{\Delta R^2}{R^2} \right)}, \quad (1)$$

де R радіус спірального укладання ОМ навколо ЦСЕ, мм; ΔR - відстань між ОВ (або пучком ОВ) і внутрішньою поверхнею стінки ОМ, мм; h - крок спірального укладання елементів (ОМ або ЗЕ) осердя навколо ЦСЕ, мм.

Виходячи з розрахунків, можна побачити, що допустиме відносне видовження ОК у першому повиві менше, ніж відносне видовження наступних повивів. Більше значення допустимого видовження наступних після першого повивів обумовлено великим радіусом спірального укладання оптичного модуля, що створює велику надлишкову довжину ОВ та ОМ й одночасно вимагає великих витрат їх матеріалів.

Таким чином, для розробки багатоповивної конструкції ОК пропонується наступна рекомендація щодо вибору конструктивних елементів осердя оптичного кабелю:

1. Вибрати кількість ОВ, що буде розміщуватися в кабелі $n_{ОВ}$.
2. Виходячи з загальної кількості ОВ $n_{ОВ}$ розробити передбачувані моделі ОК.
3. Вибрати конструктивні параметри чергової моделі ОК (тип і розміри силових елементів, кількість ОМ, кількість повивів).
4. Розрахувати кількість ОВ, які можна помістити в трубіці одного ОМ.
5. Розрахувати величину допустимого відносного видовження кабелів ϵ_{dk} , за укладанням першого повиву за формулою (1).
6. Виходячи зі значення відносного видовження ОК за укладанням ОМ першого повиву розрахувати крок спірального укладання елементів інших повивів за формулою (2)

$$7. h_{\text{іпов}} = \sqrt{\frac{4\pi^2}{(\varepsilon_1+1)^2-1} (2R_i \Delta R - \Delta R^2)}, \quad (2)$$

8. Розрахувати величину допустимого розтягувального навантаження кабелю та перевірити її відповідність очікуваним значенням.
9. У разі невідповідності допустимого розтягувального навантаження кабелю очікуваним значенням необхідно повернутися до пункту 3.

Висновки:

1. У даній роботі розроблені конструкції осердя оптичних кабелів на 144, 216 та 288 оптичних волокон, яким можна знайти застосування на оптичних мережах абонентського доступу.

2. У ході роботи встановлено, що розрахунок механічної міцності потрібно проводити за геометричними параметрами першого повиву з наступним перерахунком (збільшенням) кроку спіральної укладання елементів інших повивів для зменшення матеріалоемності оптичного кабелю.

3. Наведено рекомендацію щодо оптимізації розробки осердя багатоповивного оптичного кабелю модульної конструкції; ця рекомендація може бути використана в кабельній промисловості на етапі розробки оптичного кабелю з метою зменшення їх собівартості та матеріалозатрат.

Перелік посилань:

1. Захарченко М.В., Бондаренко О.В. «Вплив конструкції оптичного кабеля на стабільність параметрів передавання» Харків - Східно-європейський журнал передових технологій. Системи управління (Частина 111). Випуск 4/1 (40), 2009.

2. Бондаренко О.В. «Розробка методу розрахунку стійкості діелектричних оптичних кабелів до розтягуючого навантаження» Донецьк: Наукові праці Донецького національного технічного університету. Серія: (Обчислювальна техніка та автоматизація). Випуск 17, 2009.

3. Бондаренко О.В. Степанов Д.М. Боярова Г.А. «Метод оптимізації багатомодульної конструкції осердя оптичних кабелів» 99-105 с. – Україна: Наукові праці ОНАЗ ім. О.С. Попова, 2013.

4. Кабелі зв'язку оптичні для магістральних зонкових та міських мереж зв'язку. Технічні умови. ТУ-У 05758730.007-97: 1997. – [Чинні від 1997-12-10]. – Одеса.: УРУ Держстандарта Одеський центр стандартизації і метрології 1997. – 69 с.: табл. 12. – (Технічні умови ВАТ «Одескабель»).

ВИКОРИСТАННЯ ОПТИЧНИХ ПІДСИЛЮВАЧІВ В СИСТЕМАХ DWDM

Язаджи М.М., Кравцов К.В., студенти 4 курсу, група С-41, спеціальність 5.05090301 «Монтаж, обслуговування і ремонт станційного обладнання електровз'язку».

Науковий керівник: викладач першої категорії **Кокорєв В.В.**

Анотація. *Розглядається нелінійні спотворення в оптичному волокні при волновому мультиплексуванні. Величина нелінійних спотворень обмежує кількість оптичних підсилювачів у ВОЛЗ.*

При прокладанні нового кабелю потрібно скористатися вільними волокнами у вже наявних раніше прокладених кабелях. У цьому випадку виходом може стати високощільне хвильове мультиплексування (DWDM). Метод DWDM – метод ущільнення частот, що забезпечує одночасну передачу декількох різних сигналів по одному одномодовому волокну. Основними елементами DWDM системи передачі є оптичний передавач та оптичний фільтр.

Якщо на ранній стадії розвитку ВОЛЗ єдиними проблемами були погонні оптичні втрати і волоконно-оптична дисперсія, то зараз на перше місце стали виходити проблеми, пов'язані з нелійними ефектами, які особливо гостро проявляються в системах DWDM при передачі високошвидкісної цифрової інформації.

Існують наступні види оптичних підсилювачів: на волокні, що використовують бріллоєнське розсіювання (використовуються для посилення одного каналу); на волокні використовують раманівське розсіювання (використовується для посилення декількох каналів одночасно); напівпровідникові лазерні підсилювачі – ППЛУ (для посилення великого числа каналів в широкій області довжин хвиль одночасно); на домішковому волокні (для посилення великого числа каналів в широкій області довжин хвиль одночасно). Особливості роботи підсилювача залежать від типу домішок і від діапазону довжин хвиль, в межах якого він повинен підсилювати сигнал.

Для збільшення швидкостей інформаційних потоків раціональним є збільшення числа оптичних жил.

Спотворення в оптичних підсилювачах (EDFA – Erbium Doped Amplifier – оптичний підсилювач на волокні, легованому ербієм) за своєю величиною набагато менше аналогічних спотворень (CSO і CTB – спотворення другого і третього порядку відповідно), що виникають в оптичному передавачі або в оптичному приймачі. Для EDFA більш важливими параметрами є поляризаційна дисперсія, поляризаційна чутливість вихідної потужності і стабільність вихідної потужності, які у поєднанні з такими спотвореннями, як стимульоване Бріллоєнське розсіювання (SBS – Stimulated Brillouin Scattering), стимульоване Раманівське розсіювання (SRS –

Stimulated Raman Scattering), чотирьоххвильове змішання (FWM – Four Wave Mixily), фазова самомодуляція (SPM – Self-Phase Modulation) і перехресна фазова модуляція (XPM – Cross-Phase Modulation), створюють додаткові істотні спотворення в оптичних мережах, особливо небезпечні при трансляції цифрових сигналів.

Фазова самомодуляція (SPM – Self-Phase Modulation) виникає через нелінійний ефект Керра. Ефект Керра полягає в тому, що імпульси, починаючи з деякого рівня інтенсивності, поширюються з різними швидкостями, залежними від інтенсивності. ФСМ явище, яке веде до симетричного спектрального розширення оптичних імпульсів. Перехресна фазова модуляція (XPM – Cross-Phase Modulation) дуже схожа з SPM, але розглядається вже стосовно двох і більше оптичних каналів, тобто стосовно ВОСП зі спектральним мультиплексуванням (CWDM/DWDM систем). Інтермодуляція (IM – Inter Modulation) аналогічна SPM і XPM, але розглядається для декількох каналів.

Оптичний підсилювач дозволяє збільшити довжину регенераційної ділянки на відстань до 60-80 км.

Висновки:

1. Система WDM дозволяє передавати інформацію на двох частотах-1330 та 1550 нм, таким чином вдвічі збільшувати пропускну здатність оптичного волокна. Система DWDM дозволяє в одному волокні передавати 4, 8, 16, 32, 64 канали.

2. У сучасній техніці ВОЛЗ в даний час прийнято розглядати такі механізми нелінійності ОВ, пов'язаних із змінами рефракційного індексу і розсіюванням:

- стимульоване Бріллюенівське розсіювання;
- стимульоване Раманівське розсіювання.

3. Спотворення в оптичних приймачах (Optical Receiver) викликані двома складовими: спотворення, що виникають у фотодетекторі, і спотворення, що виникають у високочастотному (ВЧ) підсилювачі.

4. При великих рівнях вихідної напруги спотворення оптичного приймача не дуже залежать від рівня вхідної оптичної потужності.

Перелік посилань:

1. Иоргачев Д.В., Бодаренко О.В., Дащенко А.Ф., Усов А.В. Воконно-оптические кабели – Одесса, Астропринт, 2000 -535 с.: ил.
2. Убайдуллаев Р.Р. Волоконно оптические сети – Эко-Трейз, 2001-267 с.
3. Стерлинг Дж.Дональд. Техническое руководство по оптике – М., Лори, 1998-288 с.
4. Портнов Э.Л. Принципы построения первичных сетей и оптические кабельные линии связи. – М., Горячая линия-Телеком, 2009-544 с.

5. Корнейчук В.И., Лесовой И.П. Волоконно-оптические измерения – К., Научная мысль, 1993-323 с.

6. <http://www.telesputnik.ru/archive/120/article/62.html> – Нелінійні спотворення в волоконно-оптичних кабелях.

7. <http://www.telesputnik.ru/archive/116/article/58.html> – спотворення в підсилювачно-приймальних пристроях.

8. <http://xreferat.ru/102/1270-1-effekty-nelineynogo-prelomleniya.html> – Эффекты нелинейного преломления.

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ PON

Омельченко О.П., Зубенко М.Г., студенти 4 курсу, група С-41, спеціальність 5.05090301 «Монтаж, обслуговування і ремонт станційного обладнання електрозв'язку».

Науковий керівник: викладач другої категорії **Грачова Ю.М.**

***Анотація.** Розглядається впровадження пасивних оптичних мереж PON, архітектура, технології та різновиди пасивних оптичних мереж PON. Розглядається послідовність проектування PON, принципи вибору технології, формули розрахунку та приклад розрахунку втрат у розгалужувачах. Мета роботи – визначення доцільності впровадження пасивних оптичних мереж з урахуванням потреб абонентів на підставі аналізу переваг та недоліків цієї технології.*

В останні роки мережі доступу (МД) є найбільш динамічним сегментом телекомунікаційної галузі. Тут постійно вдосконалюються технології для задоволення нових потреб користувачів, з'являються нові, характерні лише для цих мереж, технічні рішення. На відміну від транспортних мереж (міжстанційних, міжміських тощо) в МД тільки починається перехід на оптичні технології в фіксованому зв'язку. Тому можна впевнено сказати, що МД знаходяться у фазі розвитку, що робить їх технічно та фінансово привабливими.

Наразі в операторських мережах різного рівня використовується технологія Active Ethernet, що добре зарекомендувала себе у локальних мережах. Однак технологія активних оптичних мереж Ethernet потребує великих затрат на активне обладнання, а можливість розширення мережі може бути проблематичною.

У нашій країні оптичний Ethernet найбільш поширений за схемою FTTB (Fiber to the Building, «волокно до будівлі»).

Ідея PON (Passive Optical Network, «пасивна оптична мережа») включає в себе побудову мережі доступу з великою пропускну здатністю при мінімальних

капітальних затратах. Це рішення передбачає створення розгалуженої мережі (переважно топології «Дерево») без активних компонентів – на пасивних оптичних розгалужувачах. Інформація для усіх користувачів передається з часовим розділенням каналів від головної станції OLT (Optical Line Terminal) до оптичних мережних блоків ONU (Optical Network Unit). Передача у різних напрямках здійснюється по одному оптичному волокну на різних довжинах хвилі: висхідний потік – 1490 нм, низхідний потік – 1310 нм. Також передбачена можливість передачі сигналу кабельного телебачення на довжині 1550 нм.

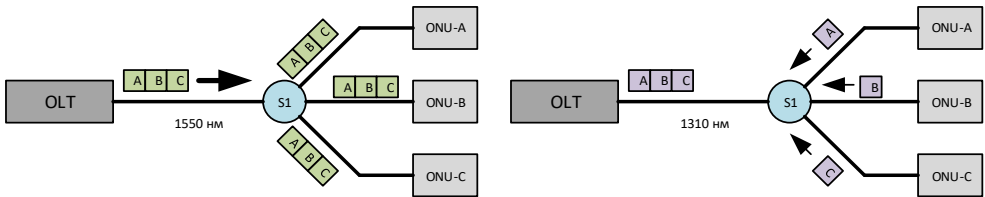


Рисунок 1 – Принцип організації зв'язку в мережі PON

В сімействі мереж PON існує декілька різновидів, що розрізняються в першу чергу базовим протоколом передачі: APON (ATM PON), BPON (Broadband PON), EPON (Ethernet PON), GPON (Gigabit PON)[1, 2]. Наступним кроком по збільшенню швидкості передачі побудованих систем PON є впровадження систем оптичного ущільнення WDM PON (близько 4-10 Гбіт/с по кожному каналу).

Основною особливістю пасивних оптичних мереж є використання оптичних розгалужувачів.[3] Розгалужувач являє собою багатополісник, задачею якого є перерозподіл енергії, що надходить у вхідні порти, між вихідними. Найчастіше використовують Y-подібні оптичні розгалужувачі, що називаються також ділянками потужності та розподіляються на симетричні та направлені (в залежності від коефіцієнту ділення потужності).

Задача проектування PON зводиться до послідовності наступних операцій: вибір місця встановлення ONU, вибір топології мережі, трас проходження кабелю та місць встановлення розгалужувачів, розрахунок бюджету втрат потужностей для кожної гілки мережі та визначення оптимальних коефіцієнтів ділення всіх розгалужувачів.

Побудова мереж PON передбачає такі основні варіанти топології: «Зірка», «Шина», «Дерево». Найбільш розповсюджена остання топологія, завдяки своїм широким можливостям в масштабуванні мережі та потенційного нарощування абонентської бази. Також ця топологія дозволяє значно економити на кількості прокладеного оптичного кабелю та оптичних випромінювачів у порівнянні з класичною технологією FTTH, де від головної станції до кожного абонента виділяється окремий кабель.

Найбільш відповідальна задача проектування – розрахунок бюджету втрат потужностей та визначення оптимальних коефіцієнтів ділення потужності всіх розгалужувачів [4].

Для прикладу приведені розрахунки бюджету втрат на сегменті мережі, що має наступний вид:

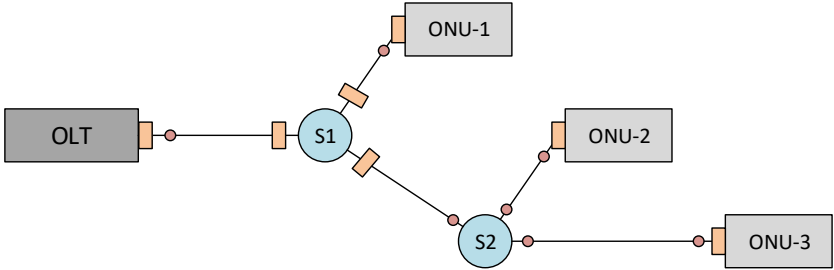


Рисунок 2 – Сегмент мережі, що проектується

Для кожної оптичної лінії представимо всі втрати як суму затухань всіх компонентів:

$$A_{\Sigma} = (l_1 + \dots + l_n) \cdot \alpha + N_p \cdot A_p + N_c \cdot A_c + (A_{\text{POЗ1}} + A_{\text{POЗm}}), \text{дБ}$$

де A_{Σ} – сумарні втрати в лінії (між OLT і ONU), дБ;

l_n – довжина n-ділянки, км;

α – коефіцієнт затухання оптичного кабелю, дБ/км;

N_p – кількість роз’ємних з’єднань;

A_p – середні втрати в роз’ємному з’єднанні, дБ;

N_c – кількість зварних з’єднань;

A_c – середні втрати в зварному з’єднанні, дБ;

$A_{\text{POЗm}}$ – втрати в m-оптичному розгалужувачі, дБ.

Визначивши загасання на кожній оптичній лінії, необхідно підібрати розгалужувачі з таким коефіцієнтом ділення, щоб сумарне затухання на кожному ONU було приблизно рівним.

Сучасні оптичні мережі вимагають високої якості їх тестування. Вимірювання в PON пов’язані з великими затратами часу та коштів та мають деякі особливості. На різних етапах прийнято розрізняти такі види вимірювань:[5]

- вхідний контроль;
- будівельно-монтажні;
- приймально-здавальні;

- експлуатаційні.

Основними факторами, що впливають на якість передачі в PON, є затухання, дисперсія та нелінійні ефекти. Основний пристрій, що використовується у вимірюваннях – оптичний рефлектометр. Принцип його дії базується на тому, що він відсилає світлові імпульси, що відбиваються від неоднорідностей в лінійному тракту. Та частина імпульсу, що відбивається, потрапляє на детектор пристрою. За допомогою рефлектометру можна визначити величину коефіцієнту загасання оптичного кабелю, а для зварних та роз'ємних з'єднань – внесені втрати та втрати на відбиття.

Висновки:

У даній роботі розглянута архітектура та принцип роботи пасивних оптичних мереж PON, а також основні параметри пасивного оптичного розгалужувача. Розглянуті основні пункти проектування мереж, наведено приклад розрахунків бюджету оптичної потужності. Наведені основні напрями вимірювань в PON, принцип роботи оптичного рефлектометру.

У ході роботи виявлено, що технологія PON дозволяє: значно економити використання оптичного кабелю за рахунок підключення до 32 абонентів до одного ОК; значно зменшити експлуатаційні затрати за рахунок використання пасивних елементів; можливе динамічне розширення полоси або збільшення швидкості передачі без заміни обладнання лінійного тракту. В той же час важливим недоліком PON є підвищена технічна складність робіт, пов'язаних із оптичним волокном, що потребують більш високого рівня кваліфікації технічного персоналу. Також необхідне значне посилення потужності на стороні OLT, щоб покрити всі втрати, що вносяться в сигнал на шляху до ONU пасивними оптичними розгалужувачами. Пасивні оптичні розгалужувачі не можуть передавати інформацію про несправності в центр управління мережею. Через це досить складно виявити несправність оптоволоконної лінії між розгалужувачем та ONU. Це значно ускладнює пошук та виправлення несправностей в мережах PON.

Зваживши всі «за» та «проти» технології PON, ми вважаємо, що її впровадження може виправдати себе в місцях щільного розташування абонентів – мікрорайонах, спальних районах та скупченнях багатоповерхових будівель, де більшу важливість має економія волокон і спрощуються задачі технічної експлуатації, оскільки всі елементи мережі територіально легкодоступні.

Перелік посилань:

1. Рекомендація ІТУ-Т G.983.1 Широкополосные оптические сети доступа на базе пассивных оптических сетей.
2. Рекомендація ІТУ-Т G.984.1. Gigabit-capable Passive Optical Networks (G-PON): General characteristics.

3. Алексеев Е.Б. Оптические сети доступа. Учебное пособие – М: ИПК при МТУ СИ, 2005 г. – 140 с.

4. <http://deps.ua/knowegable-base-ru/articles/item/465-praktika-proektirovanija-passivnyh-opticheskikh-setej-pon.html> – «Практика проектирования пассивных оптических сетей (PON)».

5. <http://deps.ua/knowegable-base-ru/articles/item/464-izmerenija-v-passivnyh-opticheskikh-setjah-pon.html> – «Измерения в пассивных оптических сетях (PON)».

6. <http://www.tehencom.com/Categories/OTDR/OTDR.htm> – «ОПТИЧЕСКИЕ РЕФЛЕКТОМЕТРЫ (OTDR): EXFO, ANRITSU, YOKOGAWA».

ВИКОРИСТАННЯ ВЕЙВЛЕТ-ФУНКЦІЙ ДЛЯ ВІДНОВЛЕННЯ БЕЗПЕРЕРВНИХ СИГНАЛІВ

Корвкіна К.В. студентка 3 курсу, група О-31, спеціальність 5.05090302 «Монтаж, обслуговування та ремонт апаратури зв'язку і оргтехніки».

Науковий керівник: викладач **Лісюк О.В.**

***Анотація.** Розглянуто вейвлет-функції та властивості вейвлет-перетворення. Виконано відновлення безперервного сигналу за допомогою вейвлет-функцій на базі вейвлета Хаара та вейвлета Котельникова-Шенона. Надано рекомендації щодо використання вейвлет-функцій для відновлення сигналів.*

Вейвлет-аналіз, на сьогоднішній день, є однією з перспективних технологій аналізу даних, що знаходить застосування для вирішення задач у різних сферах наукової та практичної діяльності. Вейвлети широко застосовуються при обробці і синтезі сигналів, для вирішення завдань стиснення і обробки зображень, для фільтрації і попередньої обробки даних, аналізу стану і прогнозування ситуації на фондових ринках, розпізнавання образів, при вивченні нейромереж і т.ін.

Вейвлети представляють собою особливі функції у вигляді коротких «хвиль» з нульовим інтегральним значенням і з локалізацією на осі часу. Ці маленькі «хвильки» здатні до зсуву та масштабуванню (стисненню чи розтягненню). Саме завдяки цьому вейвлети здатні виявляти локальні особливості досліджуваних функцій (наявність осциляцій, сплесків, розривів) [1].

В даній роботі досліджується використання апарату вейвлет-перетворень для відновлення неперервних сигналів.

Значний розвиток за останнє десятиріччя отримали вейвлет-функції, які обладують локальними властивостями як у часовій, так і у частотній областях.

Відомо, що до таких функцій відносяться вейвлет-функції Хаара, особливістю яких є простота реалізації у технічних пристроях.

Як показано в [2], у загальному випадку формула для відновлення сигналів з використанням вейвлет-перетворення має вигляд:

$$f(x) = \sum_k S_{m,k} \varphi_{m,k}(x) + \sum_{m,k} d_{m,k} \psi_{m,k}(x), \tag{1}$$

де $S_{m,k}, d_{m,k}$ – коефіцієнти вейвлет-перетворення;

$\psi_{m,k}(x)$ – базисна функція (материнський вейвлет);

$\varphi_{m,k}(x)$ – скейлінг-функція (батьківський вейвлет);

$m = \log_2 k$ – рівень масштабування;

$k = \overline{0, N-1}$ – кількість коефіцієнтів на кожному рівні масштабування;

N – кількість відліків вихідного сигналу.

Для системи Хаара аналітичний запис материнського вейвлета $\psi(x)$ та скейлінг-функції $\varphi(x)$ (батьківського вейвлета) має вигляд [2]:

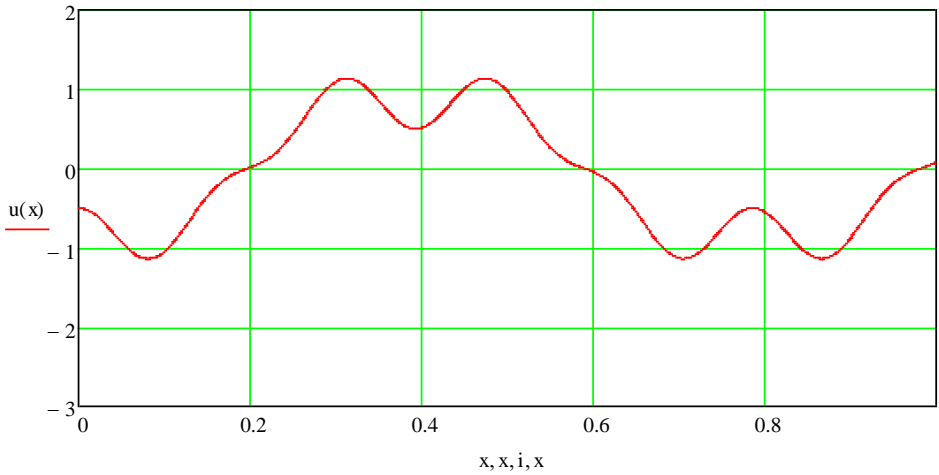
$$\varphi(x) = \begin{cases} 1, & 0 \leq x \leq 1, \\ 0 & x < 0, x \geq 1 \end{cases} \quad \psi(x) = \begin{cases} 1, & 0 \leq x < 1/2, \\ -1, & 1/2 \leq x < 1, \\ 0, & x < 0, x \geq 1 \end{cases}$$

Варто відзначити, що максимальна кількість коефіцієнтів розкладання у (1) дорівнює кількості відліків вихідного сигналу (N).

Розглянемо сигнал $f(x)$, заданий на інтервалі [0,1]:

$$f(x) = (1 + 0,5 \cos(32t + \pi)) \cos(32t + \pi) \tag{3}$$

Графік сигналу $f(x)$ зображено на рис. 1.



P

Рисунок 1 – Графік вихідного сигналу $f(x)$

Виконаємо відновлення сигналу $f(x)$ за допомогою вейвлета Хаара.

Приймаємо, що $m = 4$, тоді $N = k = 2^m = 16$.

Згідно [3] формула відновлення сигналу в базисі вейвлета Хаара має вигляд:

$$f(x) = S_{0,0}\varphi_{0,0}(x) + d_{0,0}\psi_{0,0}(x) + \sum_{k=0}^1 d_{1,k}\psi_{1,k}(x) + \sum_{k=0}^3 d_{2,k}\psi_{2,k}(x) + \sum_{k=0}^7 d_{3,k}\psi_{3,k}(x), \quad (4)$$

де $f(x)$ – функція вихідного сигналу виду (3);

$$\varphi_{m,k}(x) = 2^{m/2} \varphi(2^m x - k) \text{ – скейлінг-функція (батьківський вейвлет);}$$

$$S_{m,k} = f(k\Delta x) / 2^{m/2} \text{ – вейвлет-коефіцієнти;}$$

$$\Delta x = 1/N \text{ – крок дискретизації.}$$

Результати розрахунків за формулою (4) в середовищі *Mathcad 15* представлені на рис. 2 (крива 4).

Розглянемо відновлення сигналу $f(x)$ за допомогою вейвлета Котельникова-Шенона, для якого материнський вейвлет $\psi(x)$ та скейлінг-функція $\varphi(x)$ записуються у вигляді [4]:

$$\psi(x) = 2 \frac{\sin 2\pi(x-1/2) - \sin \pi(x-1/2)}{\pi(x-1/2)},$$

$$\varphi(x) = \begin{cases} \sin \pi x / x, & x \neq 0, \\ 1, & x = 0, \end{cases} \quad (5)$$

де материнський вейвлет $\psi(x)$ та скейлінг-функція $\varphi(x)$ пов'язані одна з одною наступними співвідношеннями:

$$\psi(x) = \sqrt{2} \sum_k g_k \varphi(2x-k),$$

$$\varphi(x) = \sqrt{2} \sum_k h_k \varphi(2x-k), \quad (6)$$

де h_k, g_k – коефіцієнти вейвлет-перетворення, які для вейвлета Котельникова-Шенона визначаються:

$$h_k = \begin{cases} 1/\sqrt{2}, & k = 0, \\ (-1)^{(k-1)/2} \sqrt{2} / \pi k, & k \neq 0, \\ 0, & k \text{ парне} \end{cases}$$

$$g_k = (-1)^k h_{N-1-k}, k = \overline{0, N-1} \quad (7)$$

Так як $f(x) \in L^2[0;1]$, то $f(x)$ можна представити у вигляді [3]:

$$f(x) = \sum_k S_{j,k} \varphi_{j,k}(x)$$

Враховуючи, що $N=16, k = \overline{0,15}, m = 4$. формула (3) приймає вигляд [5]:

$$f(x) = \sum_{k=0}^{15} S_{4,k} \varphi_{4,k}(x)$$

$$\text{де } S_{4,k} = \frac{1}{4} f\left(\frac{k}{16}\right), \varphi_{4,k}(x) = 4\varphi(16x - k)$$

Результати розрахунків наведені на рисунку 2 (крива 2).

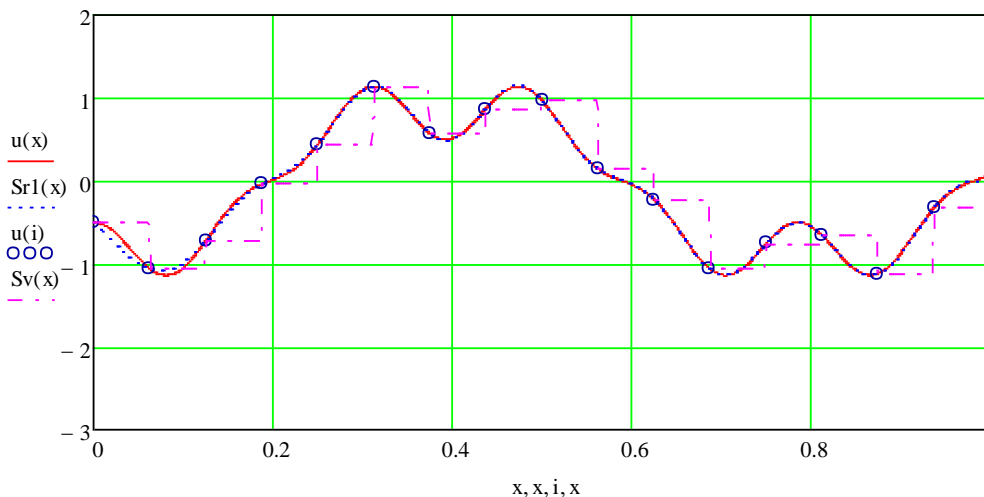


Рисунок 2 – Графік відновлення за допомогою вейвлета Котельникова-Шеннона

Як видно з рисунку 2, кращі результати відновлення отримані у випадку використання вейвлету Котельникова-Шеннона. Що стосується вейвлету Хаара, то його доцільно використовувати для відновлення імпульсних сигналів обмеженої тривалості, або для грубої апроксимації неперервних сигналів

Висновки:

1. Для відновлення неперервного сигналу виду (1) були використані вейвлет-функції на базі вейвлету Хаара та вейвлету Котельникова-Шеннона.
2. Дослідження показали, що для даного виду сигналу вейвлет Котельникова-Шеннона більш точно відновлює сигнал, ніж вейвлет Хаара. Проте можна стверджувати, що вейвлет Хаара ефективний для відновлення сигналів із локальними

особливостями (короткочасні сплески та коливання). Більш того, доцільним буде використання вейвлет-функцій Хаара для відновлення сигналів за відліками у випадках, коли відсутні аналітичні вирази досліджуваних функцій, чи навпаки – для вилучення певних складових сигналу, наприклад, шумів чи дрібних деталей, що не містять корисної інформації.

Перелік посилань:

1. Яковлев А.Н. Введение в вейвлет-преобразование: Учеб. пособие – Новосибирск: Изд-во НГТУ, 2003. – 104 с.
2. Сукачев Э.А. Введение в теорию сигналов с управляемой межсимвольной интерференцией: [монография] / Сукачев Э.А, Шкулипа П.А. – Одеса: ВМВ, 2011. – 200 с.
3. Дремин И.М. Вейвлеты и их использование / И.М. Дремин, О.В.Иванов, В.А.Нечитайло – Успехи физических наук, Том 171,№5 – 2001. С. 465-501.
4. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB / Н.К. Смоленцев. – М.: ДМК Пресс, 2005. – 304 с.
5. Стрелковская И.В. Различные виды аппроксимации в восстановлении сигналов/ И.В.Стрелковская, Е.В.Лысюк, Р.В. Золотухин // Інфокомунікації – сучасність та майбутнє,2013 – С. 169-172.

СЕКЦІЯ РАДІОЗВ'ЯЗКУ, РАДІОМОВЛЕННЯ ТА ТЕЛЕБАЧЕННЯ

ЗАСТОСУВАННЯ ЧИПІВ СЕРІЇ nRF24L У СУЧАСНІЙ ТЕХНІЦІ ЗВ'ЯЗКУ

Царев А.А., студент 4 курсу, група Р-41, спеціальність 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв'язку, радіомовлення та телебачення.

Науковий керівник: викладач **Шалімов С.М.**

***Анотація.** Розглядається практичне застосування радіочипу в сучасних пристроях радіозв'язку.*

У наш час інженери прагнуть мінімізувати розміри апаратури радіозв'язку, застосовуючи замість енергоємних електронних ламп, малогабаритні напівпровідникові елементи. Спочатку на їх основі створювалися схеми з окремих елементів, але потім ці схеми почали об'єднувати в структури на одному цілісному

кристалі – монокристалні чипи. Використовуючи малогабаритні мікросхеми, побудовані на монокристалах, ми економимо енерговитрати на виробництві та експлуатації техніки зв'язку. Застосувавши мікросхему фірми Nordic Semiconductor, серії nRF24L, в мобільному телефоні або в пристроях контролю ми отримуємо: мале енергоспоживання, мініатюрність блоку радіозв'язку і стійкість до факторів навколишнього середовища. У даній роботі я розглядаю використання мікрочипу замість приймально-передавального блоку на окремих елементах. Серія nRF24L це лінійка з п'яти радіочипів, які схожі за своєю будовою, тому я відібрав найбільш оптимальний чип – nRF24L01+. Для кращого дослідження даного чипу я розробив пристрій на його основі, провів ряд тестів і порівняльний аналіз.

Таблиця 1.1 – Характеристика мікрочипів.

Параметри	CC2511F32	nRF24L01+
Середній струм споживання	15мА	6,2мА
Напруга живлення	2,7-6,5В	1,9-3,6В
Зона покриття	15м	100м
Швидкість передачі даних	350кбит/с	0.25, 1, 2Мбит/с
Робочі частоти	2400 – 2483.5МГц	2400 – 2525МГц
Кількість радіоканалів	256	126
Розмір чипу, тип корпусу	6x6mm, QLP	4x4мм, QNF
Кількість виводів	36	20

Мета порівняльного аналізу полягає в порівнянні обраного чипу зі схожим чипом конкуруючої компанії, а саме чипа nRF24L01+ компанії Nordic Semiconductor з чипом CC2511F32 компанії Texas Instruments (табл. 1.1). Аналіз здійснювався за такими критеріями: напруга живлення, середній струм споживання, зона покриття, швидкість (або швидкості) передачі даних через радіоканал, частота роботи, кількість радіоканалів, розміри і кількість виводів. Порівнюючи вище перераховані параметри, я зробив висновок, що обраний чип значно перевершує свого конкурента.

Метою тестування параметрів чипу була перевірка номінальної зони покриття і з'ясування таких питань: які канали краще використовувати для роботи, як чип працює в умовах реального використання. Перевірка зони покриття здійснювалась на відкритій місцевості з дуже гладкою поверхнею при швидкості передачі в 250кбіт/с. Дані даного тесту доводять номінальне значення покриття - 100 метрів. Вибір каналів роботи проводився в два етапи:

- 1) зняття показань із всіх 126 каналів роботи в декількох місцях по місту;
- 2) За отриманими даними побудувати графік завантаженості каналів і виділити найбільш кращі канали роботи, а саме 96 – 126 канал.

Висновки:

У наслідок проведеної роботи, я можу сказати що даний чип має властивості , які затребувані в наш час, але його застосування досить вузьке (він ідеально підходить для недорогих, простих систем). Застосування однокристалного прийомопередавача nRF24L01+ доцільно в тих випадках, коли потрібно передавати дані в режимі «точка-точка» або створити просту бездротову мережу типу «зірка». Саме для цього призначений повністю апаратно реалізований у цьому прийомопередавачу протокол Enhanced ShockBurst. Надаючи зручний цифровий інтерфейс і здійснюючи повний апаратний контроль переданої інформації, трансивер nRF24L01 + дозволяє конструювати прості, компактні і недорогі пристрої.

Перелік посилань:

1. [http://ru.wikipedia.org/wiki/Texas Instruments](http://ru.wikipedia.org/wiki/Texas_Instruments) – опис компанії Texas Instruments;
2. [http://en.wikipedia.org/wiki/Nordic Semiconductor](http://en.wikipedia.org/wiki/Nordic_Semiconductor) – опис компанії Nordic Semiconductor;
3. <http://www.nordicsemi.com/eng/Products/2.4GHz-RF/nRF24L01P> - офіційний сайт чипа nRF24L01+;
4. <http://www.robototehnika.ru/e-store/catalog/248/1047/>– технічний опис чипа CC2511F32;
5. http://www.prochip.ru/news/2006/324369_mikroskhema-nrf24l01 - [odnokristalnyi-transiver-s-apparatnoy-podderzhkoy-protokola-peredachi.html](http://www.prochip.ru/news/2006/324369_mikroskhema-nrf24l01) – стаття «Микросхема nRF24L01 – однокристалний трансивер с апаратной поддержкой протокола передачи» з журналу «ПРОСОФТ»;
6. [http://ru.wikipedia.org/wiki/Serial_Peripheral_Interface SPI](http://ru.wikipedia.org/wiki/Serial_Peripheral_Interface_SPI) – jgbc iynthatqce

ГОЛОГРАМА ЯК ВИСОКОПЕРСПЕКТИВНИЙ НОСІЙ ІНФОРМАЦІЇ

Кислов Д.Ф., студент 3 курсу, група Р-31, спеціальність 5.05090306 «Монтаж, технічне обслуговування і ремонт обладнання радіозв'язку, радіомовлення та телебачення.

Науковий керівник: викладач **Матросова М.С.**

Анотація. *Розглядається розвиток голографічного запису інформації та можливість заміни голограмою існуючих носіїв інформації.*

Світ розвивається з фантастичною швидкістю! Величезні обсяги інформації, які ми пропускаємо крізь себе щодня, досягли колосальних розмірів. А з урахуванням

глобалізації й появи доступу до практично нескінченних ресурсів в усьому світі за допомогою мережі виникає питання: як, а головне, де зберігати всю цю інформацію?

Голографія дозволяє забезпечити дуже високу щільність запису при збереженні максимальної швидкості доступу до даних. Це досягається за рахунок того, що голографічний образ (голограма) кодується в один великий блок даних, який записується всього за одне обертання. А коли відбувається зчитування, цей блок цілком отримується з пам'яті. Для читання або запису блоків даних ("сторінок"), голографічно збережених на світлочутливому матеріалі, використовуються лазери.

Що ж таке голограма? Голографія (від грец. *holos* – увесь, повний і *grapho* – пишу) – спосіб запису і відновлення хвильового поля, заснований на реєстрації інтерференційної картини, що утворена хвилею, відбитою предметом, який освітлюється джерелом світла (предметна хвиля), і когерентною з нею хвилею, яке розповсюджується від джерела світла.

Ідея голографічних носіїв полягає в записі інформації за допомогою лазерного променя на трьохмірну підложку. Замість декількох гігабайтів таке середовище може зберігати терабайти даних на носії не більшому, ніж компакт-диск. Голографічні дані можуть зчитуватися на дуже високих швидкостях.

На перших стадіях розробки головною проблемою було створення просторових модуляторів світла (*spatial light modulator*). На сьогоднішній час технологія цих пристроїв на достатньому рівні відпрацьована, а найбільш складним завданням став підбір речовини-носія інформації. За даними Imation перші голографічні диски можуть зберігати близько 125 Гб інформації, а швидкість передачі даних складає до 30 Мб/с.

Голографія стрімко розвивається в багатьох сферах науки, медицини, зв'язку та комп'ютерних технологій. Розробкою японського національного інституту ІКТ є кольорова електронна голограма. Технологія кольорової електронної голографії дозволяє продукувати 3D-зображення рухомих об'єктів в умовах звичайного освітлення без використання лазерного променя.

Microsoft розробляє технологію 3D-телеприсутності, яка згодом буде впроваджена в комунікаційні сервіси компанії, повідомляє Neowin. Технологія буде забезпечувати «реалістичну присутність» віртуального двійника користувача в іншому місці — наприклад, на нараді в офісі. Віддалений робітник зможе «по-справжньому зайняти місце за столом, оглянутися навкруг, повернутися до колеги та поговорити з ним, сидячи пліч-о-пліч».

Що стосується медицини, то на сьогоднішній час в одному з великих дослідних центрів Ізраїлю розроблена методика, яка дозволяє бачити голограму такого органу, як серце, в форматі 3D безпосередньо під час проведення хірургічного втручання. Необхідні відомості комп'ютер, який транслює, що відбувається, отримує з аналізу, що проводиться або за допомогою ультразвукових хвиль, або за допомогою томографа. З врахуванням даних складається голограма, використовуючи спеціальне

програмне забезпечення, після чого вона за допомогою проектора передається на носій. Як затверджують практикуючі хірурги, подібна методика допоможе поліпшити якість операцій.

Також голографія використовується у створенні топографічних карт. Завдяки голографії можливо створювати більш точні карти, передавати всі нерівності земної поверхні, що є дуже корисним у даній області.

Висновки:

1. Голограма є вкрай перспективним носієм інформації. При правильному виборі носія запису голограма зможе на порядки випередити сучасні носії.
2. За допомогою голограми буде можливо передавати будь-яку інформацію у великих кількостях при малих розмірах носіїв.
3. Голографія починає знаходити широке використання в ЗМІ.
4. Голографічні технології впроваджуються в різноманітних галузях, зокрема в медицині, телебаченні, зв'язку.
5. Головною проблемою розробки голографічного запису є підбір необхідного носія.

Перелік посилань:

1. Физический энциклопедический словарь. Главный редактор А. М. Прохоров – М.: Советская энциклопедия, 1983.
2. Ахизер А. И., Берестецкий В. Б. Квантовая электродинамика, 4 изд. – М., 1981.
3. Феофилов П. П., Поляризованная люминесценция атомов, молекул и кристаллов – М., 1959.
4. Шерклифф У., Поляризованный свет, пер. с англ. – М., 1965.
5. Борн М., Вольф Э., Основы оптики, пер. с англ., 2 изд. – М., 1973.
6. Джеррард А., Бегч Д. ж. М., Введение в матричную оптику, пер. с англ., М., 1978.
7. Аззам Р., Башара Н., Эллипсометрия и поляризованный свет, пер. с англ. В. С. Запасский – М., 1981.
8. <http://ru.euronews.com/2014/01/20/holographic-heart-for-better-surgery/> Голограма на службе медицины.
9. <http://holography.by/infocenter/news/2009/150/> Голографическая индустрия. [Закрытое](http://holography.by/infocenter/news/2013/520/) акционерное общество. Голографическое телевидение.
10. <http://holography.by/infocenter/news/2013/520/> Голографическая индустрия. [Закрытое](http://holography.by/infocenter/news/2013/520/) акционерное общество. Ученые создали голографический дисплей для планшетов.

11. <http://holography.by/infocenter/news/2013/503/> Голографическая индустрия. Закрытое акционерное общество. Через Skype разрешат проводить совещания голограмм.
12. <http://www.leiadisplay.com/>Technology of holographic display.

СЕКЦІЯ ІНФОРМАЦІЙНИХ МЕРЕЖ ТА КОМП'ЮТЕРНИХ НАУК

СТЕГАНОГРАФІЯ В СУЧАСНОМУ СВІТІ

Вешкін Д. С., студент 4 курсу, група О-412, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки»
Науковий керівник: викладач другої категорії **Орлова Л. Б.**

Анотація. *Виконано аналіз основних методів стеганографії зображень та приведено їх порівняння на основі потрібного рівня безпеки та оцінки зображень. Визначено основні способи використання методів стеганографії в сучасному світі. Приведені приклади їх використання та рекомендації щодо цього.*

Триваючий розвиток комп'ютерних технологій і повсюдне впровадження глобальної мережі Інтернет докорінно змінює установлені способи захисту інформації. Системи інформаційної безпеки, щоб забезпечити свою якісну роботу, також розвивають свої системи та впроваджують нові.

Метою даної роботи є:

- дослідження основних методів стеганографії;
- аналіз головних методів стеганографії зображень та їх зрівняння по оцінкам якості зображень;
- наведення прикладів для використання методів стеганографії в сучасному світі.

Нині, наприклад, електронна пошта використовується як спілкування для людей чи передачі контрактів і конфіденційної фінансової інформації. Та із засобів сьогодні повсюдно використовується криптографічний, але він лише доводить, що ця інформація дуже важлива для користувача. Тому ще до комп'ютерної ери був придуманий метод стеганографія.

Стеганографія – це метод організації зв'язку, який приховує саму наявність зв'язку. На відміну від криптографії, де ворог точно може визначити чи є передане

повідомлення зашифрованим текстом, методи стеганографії дозволяють вмонтовувати секретні повідомлення в звичайні послання так, щоб неможливо було запідозрити існування вмонтованого таємного послання.[1]

Слово "стеганографія" в перекладі з грецької буквально означає "тайнопис" (steganos – секрет, таємниця; graphy – запис). До неї відноситься величезна безліч секретних засобів зв'язку, таких як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні канали та засоби зв'язку на плаваючих частотах і т. д. [2].

Вона займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту [5].

Стеганографічна система – сукупність засобів і методів, які використовуються для формування прихованого каналу передачі інформації.

При побудові стегосистеми повинні враховуватися наступні положення:

- противник має повне уявлення про стеганографічну систему у її деталях реалізації. Єдиною інформацією, яка залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення;

- якщо противник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому витягти подібні повідомлення в інших даних до тих пір, поки ключ зберігається в таємниці;

- потенційний противник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Всі методи стеганографії вимагають певного співвідношення між стійкістю вбудованого повідомлення до зовнішніх впливів (в тому числі і стегоаналізу) і розміром самого вбудованого повідомлення. [3]

Для більшості сучасних методів, використовуваних для приховання повідомлення в цифрових контейнерах, має місце наступна залежність надійності системи від обсягу вбудовуваних даних.

Дана залежність показує, що при збільшенні обсягу вбудованих даних знижується надійність системи (при незмінності розміру контейнера). Таким чином, використовуваний в стегосистемі контейнер накладає обмеження на розмір вбудованих даних.

Висновки:

Сьогодні інтерес до комп'ютерної стеганографії швидко зростає. Причин для цього достатньо багато. Однією з основних є те, що стеганографія надає принципово новий спосіб захисту інформації і не має аналогів. На відміну від криптографії, стеганографія приховує факт передачі інформації, який сам по собі може мати вирішальне значення. З іншого боку, комп'ютерна стеганографія, як впливає з її визначення, для приховування інформації використовує файли, що містять інформацію мультимедіа. Приголомшливе зростання обсягів такого роду інформації та її повсюдне проникнення роблять стеганографію універсальною і ще більш привабливою, як інструмент. Одним із значущих чинників є і те, що стосовно стеганографії, на відміну від криптографії, на даний момент не розроблено відповідної нормативно-правової бази, що регулює її використання. Всі перераховані вище фактори більшою мірою характерні для цифрових зображень, що робить їх одним з найбільш ефективних носіїв інформації, що приховується.[4]

Під час народження комп'ютерної стеганографії відбувалося створення і становлення нових високоефективних мультимедійних форматів. Тому спочатку стеганографія зображень розвивалася в бік залучення вирішення своїх завдань нових стандартів зберігання графіки. В даний час є досить усталений набір графічних форматів, що набули широкого поширення, а вдосконалення алгоритмів вбудовування відбувається в основному за рахунок збільшення ефективності використання цих форматів.

Тема «Стеганографія» актуальна, тому що може дати змогу захищати свою інформацію новими методами, що в комбінації з іншими дають високий рівень безпеки інформації. А саме ця тема є одною із найважливіших в сучасному суспільстві, бо кожній людині, чи організації важливо зберігати свою інформацію конфіденційно.

Перелік посилань:

1. Швидченко И.В. Анализ криптостеганографических алгоритмов/ Проблемы управления и информатики, 2007. - № 4. - С. 149-155.
2. Барсуков В.С., Романцов А.П. Компьютерная стеганография: вчера, сегодня, завтра. / <http://st.ess.ru/>
3. «Стеганография» / <https://ru.wikipedia.org/wiki/стеганография>
4. Генне О.В. Основные положения стеганографии/ Журнал "Защита информации. Конфидент", 2000. - №3.
5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография/ М.: Солон-Пресс, 2002. - 272 с.

6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография Теория и практика / К: МК-Пресс, 2006. - 288 с.
7. Грибунин В.Г. Критерии оценки надёжности паролей/ М.: РУСКАРД, 2003.
8. Игнатов В.А. Теория информации и передачи сигналов/ М.: Радио и связь, 1991. - 280с.
9. Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений / Журнал "Защита информации. Конфидент", 2000. - №3. - С.34.
10. Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. Основы компьютерной стеганографии/ М.: Радио и связь, 2003. - 152 с.
11. «Основные положения стеганографии»/ <http://citforum.ru/internet/securities/stegano.shtml>
12. «Стеганографический метод Кутгера-Джордана-Боссена»/ <http://habrahabr.ru/post/115287/>
13. «DarkJPEG: стеганография для всех» / <http://habrahabr.ru/post/187402/>.
14. «Прикладные методы защиты информации» / <http://crypto-blog.ru/>.

ДОСЛІДЖЕННЯ ПОКРИТТЯ WLAN AP NANO STATION LOCO M2

Палій О. Г., студент 4 курсу, група О-412, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки»
Науковий керівник – викладач другої категорії **Малюта С. О.**

Анотація. Розглянуто технології бездротових локальних комп'ютерних мереж IEEE 802.11 «Wi-Fi». Проведено дослідження діючої мережі «Wi-Fi» на базі AP Ubiquiti NanoStation Loco M2. Проаналізовані можливості виконання та достовірність провісного інспектування бездротових локальних комп'ютерних мереж «Wi-Fi» для різних груп користувачів.

Безперечною особливістю сучасності є високий рівень інформатизації суспільства. Широка комп'ютеризація та впровадження нових телекомунікаційних технологій призвели до того, що вони сприймаються вже не тільки як утилітарні засоби комунікації та доступу до інформації, але й є невід'ємною часткою життя та культури людства.

Метою даної роботи є:

- загальне дослідження технології бездротових локальних комп'ютерних мереж стандартів IEEE 802.11 «Wi-Fi»;

– дослідження діючої бездротової локальної мережі головного корпусу КЗІ ОНАЗ ім. О. С. Попова, розгорнутої на базі використання точок доступу (access point, AP) Ubiquiti NanoStation Loco M2;

– розглядання способів провісного інспектування (predictive inspection) Wi-Fi мережі, їх оцінка, порівняння результатів провісного інспектування з результатами вимірювань в існуючій мережі.

Бездротові комп'ютерні мережі дозволяють розгортання в умовах, коли принципово неможливе, або є економічно не вигідним прокладання кабелю; за наявності потреби швидкого розгортання мережі, оперативного об'єднання віддалених мереж у разі відсутності між ними кабельних, чи волоконно-оптичних каналів зв'язку, за необхідності їх резервування [1, с. 17; 2]; для забезпечення обслуговування рухомих абонентів чи обслуговування зон з інтенсивним обігом клієнтів. Персональні бездротові мережі дозволяють налагоджувати оперативний зв'язок у безпосередній близькості до користувача, локальні – використовуються для забезпечення зв'язку у межах будівлі, частини будівлі, міські – населеного пункту чи його частини, глобальні – у масштабах, більших за регіон. Порівняно з дротовими мережами, бездротові історично мають нижчі показники швидкості, надійності та захищеності передачі інформації, однак можуть досягати рівня, порівнюваного з дротовими, за умови використання відповідних технологій.

Бездротові локальні мережі досягли поширення як у корпоративному, так і домашньому використанні. Розрізняють мережі з незалежною базовою зоною обслуговування та мережі з базовою станцією [1, с. 23-30]. При плануванні мережі розрізняють ті, що застосовуються на відкритому просторі (зовнішні), та у приміщенні (внутрішні) - оскільки ефективність таких мереж має високу залежність від умов навколишнього середовища, в якому поширюється сигнал [1, с. 66]. Так середні швидкості та радіуси дії найбільш поширених AP зі штатними антенами оцінюються як: IEEE 802.11b (2.4ГГц) – максимальна швидкість 11 Мбіт/с, середня практична швидкість 3.2 Мбіт/с, за радіусами дії – у приміщенні 38, на відкритому просторі – 140 метрів; 802.11a (5 ГГц) – 54 / 18.4 Мбіт/с та 35 / 120 метрів відповідно; 802.11g (2.4 ГГц) – 54 / 15.2 Мбіт/с та 38 / 140 метрів; 802.11n (2.4 / 5 ГГц) – 600 / 59.2 Мбіт/с та 70 / 250 метрів [3]. Значний вплив має конфігурація навколишнього середовища (наявність та параметри фізичних перешкод у напрямку між клієнтом та AP, а також навколо них) та характеристики використаного мережевого обладнання. Досліджувана у даній роботі мережа є внутрішньою мережею з використанням базової станції Ubiquiti.

Ubiquiti NanoStation Loco M2 має характеристики: процесор - Atheros MIPS 24 КС (400 МГц); RAM – 32 Мб SDRAM; Flash – 8 Мб; роз'єми – 1x10/100 Base-TX (Cat. 5, RJ-45) Ethernet; стандарти – 802.11b/g/n/AirMax; ОС – AirOS v5. Вбудована 2x2 MIMO антена з малим розміром зворотного сектора діаграми направленості, посилення – 8 dBi. Має змінну ширину каналу. Розміри корпусу – 163x31x80 мм; вага

– 0,18 кг, пластиковий корпус; максимальне споживання – 5,5 Вт; електроживлення 24В/0,5А, спосіб живлення – «Passive power over Ethernet»; робоча температура - 30..+80°C; вологість 5..95% [4]. Виробник заявляє можливу площу «впевненого покриття» мережі 300 квадратних метрів у приміщенні та високий рівень ізоляції радіочастини пристрою від навколишнього середовища [5].

Отримання даних з існуючої мережі було виконано з використанням програмного забезпечення InSSIDer Home, CommView for WiFi, HeatMapper, для провісного інспектування було застосовано TamoGraph Site Survey. Усі використані версії програм є безкоштовними, або умовно-безкоштовними, програми працюють у середовищі Windows.

Висновки:

Незважаючи на велику кількість існуючих моделей, поширення радіохвиль [6, 2, 1, с. 212], прогнозування динаміки покриття бездротових локальних комп'ютерних мереж є важким завданням: навіть при використанні спеціалізованих програм провісного інспектування бездротових мереж, розрахунок може гарантувати лише приблизний рівень точності прогнозу, адже достовірне прогнозування покриття мережі потребує врахування величезної кількості факторів (складна конфігурація приміщення, великі адитивні перешкоди від інтерференції сигналів, висока залежність проникаючої здатності радіохвиль діапазону надвисоких частот від матеріалу та конфігурації фізичних перешкод, електромагнітний вплив сусідніх мереж схожої технології, різноманітні динамічні показники навколишнього середовища). Через це є необхідними додаткові дослідження покриття розгорнутої мережі, що може мати значно нижчі за прогнозовані показники ефективності (через вплив неврахованих факторів), а отже – потребувати реконфігурації. Існуючі на ринку програми здатні здійснювати ефективно провісне інспектування мережі, однак можуть виявитися економічно нерентабельними для корпоративних та приватних абонентів. Спроби ж розрахунку оптимальної конфігурації мережі без застосування спеціалізованих програм відносно успішно замінюються методами реконфігурації на підставі результатів її тестування безпосередньо під час роботи мережі.

Перелік посилань:

1. Безпроводні локальні комп'ютерні мережі / В. Чернега, Б. Платтнер. – Київ, «Кондор», 2013.
2. Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 900 MHz to 100 GHz, ITU-R Recommendations – Geneva, 2001 – http://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1238-7-201202-I!!PDF-E.pdf.

3. НИКС: FAQ WiFi: беспроводные сети – http://www.nix.ru/support/faq/show_articles.php?number=596&faq_topics=WiFi-802.11 (Перегляд: 11/01/2014).
4. ТехноТрейд: Ubiquiti NanoStation Loco M2 (00294) – <http://www.technotrade.com.ua/Products/ubiquiti-nanostation-loco-m2.php> (Перегляд: 11/01/2014).
5. Ubiquiti NanoStation LocoM2 – <http://ubnt.su/ubiquiti/LocoM2.htm> (Перегляд: 11/01/2014).
6. Wikipedia.org: Radio Propagation model – http://en.wikipedia.org/wiki/Radio_propagation_model (Перегляд: 11/01/2014).
7. Wikipedia.org: IEEE 802.11 – <http://en.wikipedia.org/wiki/802> (Перегляд: 09/02/2014).
8. Magazilla: Ubiquiti NanoStation Loco M2 – <http://m.ua/pric/ubiquiti-nanostation-loco-m2/> (Перегляд: 09/02/2014).
9. Wikipedia.org: Comparison of wireless site survey applications – http://en.wikipedia.org/wiki/Comparison_of_wireless_site_survey_applications (Перегляд: 12/02/2014).

АСИМЕТРИЧНА КРИПТОСИСТЕМА RSA ТА ЦИФРОВИЙ ПІДПИС НА ЇЇ ОСНОВІ

Міненко В.А. студент 3 курсу, група О-31, спеціальність 5.05090302 «Технічне обслуговування і ремонт апаратури зв'язку та оргтехніки»

Науковий керівник: викладач другої категорії **Фіньковська М. С.**

Анотація. *Розглядаються криптографія, шифрування та ЕЦП як методи захисту інформації. В основі роботи дослідження криптосистеми RSA як методу шифрування та ЕЦП.*

Головна мета дослідницької роботи – провести аналіз алгоритму шифрування RSA та цифрового підпису на її основі. Для цього був здійснений алгоритм RSA в середовищі програмування Delphi 7.0.

Криптографія – це спосіб так замаскувати повідомлення, щоб його міг зрозуміти тільки адресат.

Процедура шифрування складається з двох етапів. Перший етап – маскування відкритого тексту. Така процедура називається кодуванням, а закодоване повідомлення – шифротекстом. Адресату повинна бути відома зворотна процедура декодування шифротексту в початкове повідомлення. Ця процедура називається декодуванням або дешифрувкою.

Шифрування застосовується для зберігання важливої інформації в ненадійних джерелах та її передачі по незахищеним каналам зв'язку. Зараз шифрування допомагає уникнути необхідності зберігати файли у фізично захищеному сховищі.

Є два основних методи шифрування: симетричне та асиметричне.

У симетричних криптосистемах для шифрування і розшифрування використовується один і той же ключ. Звідси назва - симетричні. Алгоритм і ключ вибирається заздалегідь і відомий обом сторонам. Збереження ключа в секретності є важливим завданням для встановлення і підтримки захищеного каналу зв'язку. У зв'язку з цим, виникає проблема початкової передачі ключа (синхронізації ключів).

У системах з відкритим ключем або асиметричних використовуються два ключі – відкритий і закритий, пов'язані певним математичним чином один з одним. Відкритий ключ передається по відкритому (тобто незахищеному, доступному для спостереження) каналу і використовується для шифрування повідомлення і для перевірки ЕЦП. Для розшифровки повідомлення і для генерації ЕЦП використовується таємний ключ.

Електронний цифровий підпис (ЕЦП) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Із систем кодування з відкритим ключем більш відомою і широко поширеною є система RSA. RSA стала першою криптографічною системою яка придатна і для шифрування і для цифрового підпису.

Безпека алгоритму RSA побудована на принципі складності факторизації. Алгоритм використовує два ключі – відкритий і закритий (секретний), разом відповідні ключі утворюють пари ключів.

Система RSA використовується для захисту програмного забезпечення й у схемах цифрового підпису. Також вона використовується у відкритій системі шифрування PGP.

Через низьку швидкість шифрування (близько 30 кбіт/сек при 512 бітному ключі на процесорі 2 ГГц), повідомлення звичайно шифрують за допомогою продуктивніших симетричних алгоритмів з випадковим ключем (сеансовий ключ), а за допомогою RSA шифрують лише цей ключ.

Висновки:

У роботі докладно описана реалізація алгоритму RSA як для шифрування, так і для цифрового підпису. Реалізована програма для оцінки алгоритму у середовищі Delphi 7. Побудовано графік залежності модуля простих чисел p і q від

часу. За результатами досліджень можна зробити висновок, що чим більша довжина простих чисел p і q , тим більший час і потужність техніки потрібні на розрахування секретного ключа. Але чим більший і складніший ключ, тим більш криптостійким буде алгоритм.

Перелік посилань:

1. Нильс Фергюсон, Брюс Шнайер Практическая криптография.
2. Венбо Мао Современная криптография. Теория и практика.
3. Коутинхо С. Введение в теорию чисел. Алгоритм RSA.
4. Бернет С., Пэйн С. – Криптография. Официальное руководство RSA Security.
5. <http://www.e-nigma.ru/stat/rsa>. Алгоритм шифрования RSA.
6. <http://ru.wikipedia.org/wiki/Криптоанализ> RSA Криптоанализ RSA.

Технічний редактор – *Горлінська О. Ю.*, заступник директора з НР
Комп'ютерне макетування – *Орлова Л. Б.*

Здано в набір 14.02.2014 р. Підписано до друку 17.02.2014 р.

Тираж 25 прим. обсяг 1,32 друк. арк.

Віддруковано в коледжі зв'язку та інформатизації ОНАЗ ім. О.С. Попова

© КЗІ ОНАЗ, 2014