І МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ НАУКИ І ТЕХНІКИ»

22 жовтня 2015 року

УДК 621.387:681.327

Актуальніпроблеми розвитку науки і техніки: Матеріали першої міжнародної науково-технічної конференції.Збірник тез. — Київ :ДУТ, 2015. — 263 с.

Даний збірник містить тези учасників конференції, представлених на
І Науково-технічній конференції "Актуальні проблеми розвитку науки і техніки", яка проводилась 22 жовтня 2015 р. в Державному університеті телекомунікацій, м. Київ.

Робочі мови конференції - українська, російська, англійська.

Вчені секретарі конференції:
Невдачина О.В. к.т.н., доцент каф. КС, ДУТ
Складаний П.М. ст.викладач каф. ІКБ, ДУТ
Полоневич А.П. к.т.н. доцент каф. КС, ДУТ

Державний університет телекомунікацій
Київський національний університет імені Тараса Шевченка
Національний авіаційний університет
Військовий інститут телекомунікацій та інформатизації
Національний університет “Львівська політехніка”
Вінницький Національний університет
Національна академія оборони України
Академія Служби безпеки України
Інститут спеціального зв’язку та захисту інформації
Університет Бульсько-Бяла
Одеська національна академія зв'язку ім.О.С.Попова
Український державний університет залізничного транспорту
Інститут газу Національної Академії Наук України
Львівський національний університет імені Івана Франка
Білоруський державний університет транспорту
Санкт-Петербурзький державний університет телекомунікацій ім. проф. М.А.Бонч-Бруєвича

I МІЖНАРОДНАНАУКОВО-ТЕХНІЧНАКОНФЕРЕНЦІЯ «АКТУАЛЬНІПРОБЛЕМИРОЗВИТКУНАУКИІТЕХНІКИ»

ЗБІРНИК ТЕЗ

22 жовтня 2015 року

м. Київ

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Програмний комітет:

ШЕВЧЕНКО Віктор Леонідович*(д.т.н., проф., Київ, Україна);*
БУРЯЧОК Володимир Леонідович*(д.т.н., с.н.с., Київ, Україна);*
РОЗОРІНОВ Георгій Миколайович*(д.т.н., проф., Київ, Україна);*
НАКОНЕЧНИЙ Володимир Сергійович *(д.т.н., с.н.с., Київ, Україна);*
СКЛАДАННИЙ Павло Миколайович (*ст. викладач, Київ, Україна);*
КОЗЕЛКОВ Сергій Вікторович *(д.т.н.,проф., Київ, Україна);*
ПОЛОНЕВИЧ Андрій Петрович *(к.т.н., Київ, Україна);*
НЕВДАЧИНА Ольга Володимирівна *(к.т.н.,Київ, Україна);*
ЖУРАКОВСЬКИЙ Богдан Юрійович *(д.т.н. проф, .Київ, Україна);*
ДРУЖИНІН Володимир Анатолійович*(д.т.н.,проф., Київ, Україна);*
ТУПКАЛО Віталій Миколайович *(д.т.н., проф., Київ, Україна);*
ОКСІЮК Олекесандр Глебович*(д.т.н., доцент, Київ, Україна);*
ТОЛЮПА Сергій Васильович *(д.т.н.,проф., Київ, Україна);*
САМОХВАЛОВ Юрій Якович*(д.т.н.,проф., Київ, Україна);*
ЮДІН Олександр Констянтинович*(д.т.н.,проф., Київ, Україна);*
КОРЧЕНКО Олександр Григорович *(д.т.н.,проф., Київ, Україна);*
ЯРЕМЧУК Юрій Євгенович*(д.т.н.,проф., Вінниця, Україна);*
КОЗЛОВСЬКИЙ Валерій Валерійович*(д.т.н.,проф., Київ, Україна);*
СУБАЧ Ігор Юрійович*(д.т.н.,доцент, Київ, Україна);*
ГОРБЕНКО Іван Дмитрович *(д.т.н.,проф., Харків, Україна);*
ПАРКУЦЬ Любомир Тодорович *(д.т.н.,проф., Львів, Україна);*
ДУДИКЕВИЧ Валерій Богданович *(д.т.н.,проф., Львів, Україна);*
НАЗАРКЕВИЧ Марія Андріївна *(д.т.н.,проф., Львів, Україна);*
ГРИЩУК Руслан Валентинович *(д.т.н., с.н.с., .Житомир, Україна);*
БАЙЕР Анджей *(д.т.н.,проф., Польща);*
ТУРМАНІДЗЕ Рауль Сергійович*(д.т.н.,проф., Грузія);*
КАРПІНСЬКИЙ Микола *(д.т.н.,проф., Польща).*
СТЕПУТІН Антон Миколайович (*к.т.н. доц. СПбДУТ*, *Росія*)

ЗМІСТ

ParkhomeiI.R.
Doctor of technical Sciences,associate professor
State University of Telecommunications
Kiev, Ukraine

MODERN METHODSOFINCREASINGTOEFFICIENCYRADIOLOCATION

Was considered that such phenomena as excitement, breakdown of insulators, formation of standing waves in the coverings have the accompanying mean character and therefore purposefully weren't reproduced in vitro and weren't investigated from the point of view of technical realization as an element of defeat of arms. Possible ways of obtaining information of objects from nonmetallic substances are given.

The modern equipment is created with use of nonmetallic materials in a design. It clearly for a number of reasons, basic of which is the best characteristics of substances. The existing approaches concerning obtaining radar information on such objects is improper as they are based on use of the effects proceeding in metals at their radiation by the electromagnetic microwave oven we weed. Therefore the problem of creation of conditions on remote temporary change of the leading properties for use of the caused effects in the existing ways of a radar-location is actual.

Research objective is search of approaches in creation of artificial conductivity in nonmetallic materials means of resonant impact of electric field on elements of crystal structure of dielectric.

Scientific task which is considered in work, devoted calculation of the quantitative indices characterizing possibility of change of electroconductive properties of dielectric of carbon type at distance of practical use of the existing radar-tracking systems.

Important circumstance which promotes creation of local conductivity, existence at atoms in a zone of conductivity of electrons that is characteristic for conductors is. At semiconductors and dielectrics the zone of conductivity and a valent zone are divided by the forbidden zones. So at carbon which is widely applied in radio engineering, width of the forbidden zone makes 5,4 eV [1]. If to assume that under certain conditions electrons from a valent zone of atom of carbon will be moved to a conductivity zone, the specified substance will show properties of the conductor.

It will allow to change views of use of carbon, its connections and other dielectric and semiconductor materials in radar equipment.

Transition of electrons to a zone of conductivity happens in wild spirits atom [2]. It is possible to carry out excitement of atom on condition of impact on it of an external electromagnetic field of big power. Power of a field of radiation of for the translation of one electron from a valent zone in a zone of conductivity is necessary is defined by dependence [3].

$$P = \frac{w}{\tau}, (1)$$

where w – width of the forbidden zone.

Considering Avogadro's law, creation of a local zone of conductivity demands the big power of the irradiated field that doesn't make practical sense from dielectrics and semiconductors. But, if to weigh on that transmission of energy of excitement of atom will occur on condition of achievement of a frequency and phase resonance (fluctuations) of an external source of electromagnetic radiation and own fluctuations of atom, then power expenses significantly decrease. As practice [4] shows, the typical survey lokats_yna station possesses radiation parameters: Ri=0,5 MWT (power), =12 HHz (frequency) =0,5 мcs (impulse duration) creates amplitude of fluctuations at a frequency of resonant interaction with dielectric like soot =0,975 V). Amplitude of fluctuations of a signal of radiation at a frequency of resonant interaction decides on atom of carbon by powerful dependence

$$U_к = 2U_н \omega_н \tau_u \left| \frac{\sin\left(\frac{\varpi_к}{2}\tau_u\right)}{\frac{\varpi_к}{2}\tau_u} \right|, (2)$$

where $U_н$ – radiation signal amplitude at the bearing frequency; $\varpi_к$ – frequency of a range of amplitudes of a signal of radiation.

Respectively a power of a signal of radiation at working range of D=100 station of km which is defined by dependence (2), will make P=2,5 10-16 Wt at a reference value of G=0,94 of Wt.

$$P = \frac{2P_1 G\sigma}{\left(4\pi D^2\right)^2}, (3)$$

where G – coefficient of connection of the antenna; σ – dielectric surface area.

If to assume that at some distance there is a coincidence on a phase and frequency or their difference is the whole constant of a signal of radiation and fluctuations of atoms of dielectric, such interaction should be considered as coherent. Thus there is an excitement of atom at the expense of transmission of energy of a field of radiation of an external source. In this case electrons from a valent zone pass into a conductivity zone that is followed by radio wave radiation. Duration of radiation is defined by time of receipt of electrons in the forbidden zone after an atom conclusion from an equilibrium state and is equal 0,5 – 1 mcs [4]. The resultant of energy of an electromagnetic field of radiation is defined by dependence:

$$E_p = \sqrt{E_e^2 + E_{U_к} + 2E_e E_{U_к} \cos\Delta\varphi}, (4)$$

where E_e – energy of an electron; $E_{U_к}$ – energy of a signal of radiation at a frequency of resonant interaction; $\Delta\varphi$ – a difference of phases of the interacting

fluctuations.

Not difficult calculations show that at range of 100 km at radiation of a sample of dielectric on a carbon basis an electromagnetic field with characteristics which are indicated the begun power of the return wave will make 1,602·10-7 Wt.

Except the specified effect under the influence of resonant radiation the local area of conductivity with existence time to 1 mcs will be formed. Existence of this area is explained by the East of electrons in a conductivity zone, that is there is an electric breakdown of dielectric. That is during breakdown possibly aiming at surface areas of dielectric of a secondary electromagnetic field and the accompanying reflection of a radio wave with any frequency.

Practical interest causes possibility of determination of the area of area of local conductivity of dielectric at radiation resonant the electromagnetic we weed. For this purpose it is necessary to determine intensity resonant material by a formula [4]

$$I = \frac{\rho V U^2}{2}, \quad (5)$$

where ρ - material density; V - radio wave speed; U - amplitude of fluctuations of atom.

In the case under consideration intensity dielectric of carbon type in wild spirits makes 16,2·10-15 Wt·m3.If to use a known formula [3],

$$S = \frac{E}{I}, \quad (6)$$

where S - the area of a sample of material; I - intensity; E - energy радіовипромінення,

it is possible to claim that that at practical range of work of 100 km it is possible to create local area of conductivity of 0,101 m on a surface of a dielectric covering of carbon type.

The specified approach on remote control of a condition of dielectric and semiconductor materials has the practical importance as expands possibilities of a location of aircraft, sea and land objects in which design all are more widely used nonmetals.

Literature:

1. ПархомейІ.Р. Дослідження явища ентальпії/ І.Р. Пархомей// Збірник тез доповідей на ІІ Всеукраїнської науково-практичної конференції ВІКНУім. Т.Г. Шевченка, 2006 р. - Київ, 2006. С. 60 - 62.

2. ПархомейІ.Р. Методика розрахунку радіопоглинаючих покриттів аеродинамічних літальних апаратів / І.Р. Пархомей // Зб. наук.пр. ВІТІНУТУ «КПІ». - К., 2002.-№1.- С. 146-151.

3. ПархомейІ.Р. Моделювання умов бажаного процесу керування складною технічною системою/ І.Р. Пархомей // Міжвід. наук.-техн. зб. «Прикладна геометрія та інженерна графіка», КНУБА. - К., 2006. - №76. - С. 94-98.

4. ПархомейІ.Р. Обґрунтування процесу взаємодії НВЧ сигналу з кристалічною структурою діелектрика/ І.Р. Пархомей, І.А. Кравець // Всеукраїнський науково-технічний журнал «Вібрації в техніці та технологіях». - 2005. - №2(40). - С. 38-43.

Срочинська Г.С.
Аспірант,ст.викладач кафедри Інфокомунікацій
Довженко Н.М.
Аспірант, ст.викладач кафедри Інфокомунікацій
Державний університет телекомунікацій
м. Київ, Україна

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ QR-КОДУВАННЯ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ УКРАЇНИ

Міжнародні інтеграційні процеси і, перш за все, процеси науково-технологічного і економічного розвитку держави неможливі без впровадження в телекомунікаційну мережу тих технологій та процесів, що зможуть активізувати та підняти рівень послуг на більш вагомий щабель.

Україна не може конкурувати, а тим паче еволюціонувати, не використовуючи досвід світових телекомунікаційних лідерів; влада не може забезпечити стійкий розвиток держави, якщо не будуть введені механізми достовірного інформування користувачів, контролю та управління ресурсами життєдіяльності і бюджетом на всіх рівнях.

Інформація - цеособливий вид капіталу країни, а тому, вона повинна бути насамперед доступною, коректнорегульованою і вміло керованою. Збір, обробка, зберігання, використання та передача інформації забезпечують нормальну роботу ринку телекомунікацій. Головними вимогами до цього ринку являються: використання інформаційних технологій великої швидкодії, високої точності і надійності, автоматизації та системності.

В умовах конкурентного середовища, значна частина інформації повинна бути оперативною, а також недоступною для її використання нерегламентованими користувачами.

Тому більшість інформаційних технологій базуються на зберіганні і передаванні інформації в закодованому вигляді. Одним із кращих, сучасних рішень для інтегрованих телекомунікаційних мереж, є технологія QR-кодування.

На сьогоднішній день, ця технологія використовується банківському секторі економіки, в рекламі, торгівлі, логістиці, туризмі, інтернет-магазинах з метою максимальної економії часу клієнтів та онлайн-покупців. Однак поява вУкраїні нових технологій опрацювання інформації не означає, що вони відразу отримають широкого впровадження.

QR-код (QuickResponseCode, 2D Code) –двовимірний (матричний) штрих-код, розроблений японською компанією Denso-Wawe у 1994 році. Абревіатура

QR перекладається як “швидка відповідь”. Основна перевага QR-коду – це легке його розпізнавання сканувальним обладнанням, що дає можливість використання коду в багатьох сферах. Для зчитування інформації з QR-коду потрібен мобільний телефон, смартфон чи планшет з камерою і спеціальне програмне забезпечення, яке розповсюджується безкоштовно через мережу Інтернет. Вибір програми диктується типом операційної системи, встановленої на мобільному пристрої. Для Android – це I-Nigma, GoogleGoggles, QuickMark, BarcodeScanner, Barcode2file, QR Droid, NeoReader, ixMATScanner, 2D-код, Elinext UPC; для Java –KaywaReader, I-Nigma, UpCode; для Symbian OS – QuickMark, Kaywareader, Nokiabarcodereader, I-Nigma, UpCode, NeoReader, BeeTag; для Windows Mobile –QuickMark, I-Nigma; для Bada – BeeTagg, Quick QR Reader та ін. Для деяких операційних систем програми зчитування QR-кодів є вбудовані в магазини додатків для портативних пристроїв [1].

QR-коди не прив’язані до конкретного формату даних, тобто до усталеного стандарту запису інформації у файлі. Програми перегляду QR- кодів розпізнають текст, графічні зображення, інформацію веб-сторінок, E-mail, SMS, номери телефонів, географічні координати та іншу інформацію. Тип інформації вказується при генеруванні QR-коду. Щоб отримати інформацію безпосередньо на екран мобільного телефона, достатньо запустити програму для сканування коду і навести об’єктив камери на код. Програма-декодер розпізнає тип інформації і виконає потрібні дії, наприклад відкриє веб-сторінку (в цьому випадку потрібне ще з’єднання з інтернет).

Для максимального комфорту та швидкості отриманні інформації, QR-код розміщується на: web-сайтах, сторінках блогів, в періодичних виданнях, на туристичних об’єктах, плакатах, на одязі, в музеях,на сувенірах, і т.д. QR-код виконуєдві функції: вміщує велику кількість інформаціїу невеликій картинці (більше двох друкованихсторінок) і дозволяє автоматично зчитувати закодовані дані. Даний код є унікальним в своєму вигляді. Будучи дуже простим, зручним у використанні, а також допомагаючи оперативно отримувати і розповсюджувати інформацію інтерактивним шляхом, саме цей код набув широкого застосування.

Сучасні мобільнітелефони, смартфони і планшети мають вбудоване програмне забезпечення для зчитування і розпізнавання QR-коду. Після сканування камероюмобільного пристрою програма, встановлена на ньому, розпізнає вид інформації, що зберігається в QR-коді. Якщо це адреса сайту – відкриває його браузером, якщо електронна візитна картка – додає нову контактну особу в телефонну книгу, якщо звичайний текст – виводить його на екран.

Але враховуючи всі переваги використання, важливо також відмітити і загальні проблеми із якими зіштовхуються користувачі.

Особливості функціонування

QR-код завжди має форму квадрата (матриці)і відрізняється від звичайних штрих-кодів розміщенням інформації в двох напрямах – вертикальному і горизонтальному. Менші квадрати ічорні лінії містять інформацію, яка зберігаєтьсяв модулях. Кількість модулів залежить від об’ємузакодованих даних.

Перша версія QR-коду (найменший код) має розмір 21×21 піксель і 441модуль, версія 40 (найбільший код) – 177×177пікселів і 31 329 модулів. Завдяки цьому збільшується максимальна кількість інформації, якувміщає один QR-код: цифри – 7089, цифри і літери (включно з кирилицею) – 4296, двійковийкод – 2953 байт, ієрогліфи – 1817 [2].

Існує мікроQR-код ємністю до 35 цифр, його використовують для розміщення коду на невеликій площі, наприклад на запальничці чи сувенірному брелку.Кількість інформації, яку вміщує мікро QR-коднevелика, але в ньому можна закодувати номертелефону чи коротку URL-адресу. Також використовується псевдо-кодування – задання методукодування даних або розбиття довгого повідомлення на кілька кодів тощо. Розмір QR-коду може бути будь-яким, але длязручності читання і розпізнавання довжина кожної сторони повинна бути не меншою за 2,5 см.

Для зчитування кодів меншого розміру потрібнібільш високоточні скануючі пристрої, ніж сучасні смартфони і планшети.На відміну від одновимірного штрих-коду,який сканують тонким променем, QR-код визначається сенсором як двовимірне зображення,але зчитувати його можна в будь-якому напрямку. Три великі квадрати в кутах зображення таконтрольна точка поблизу четвертого кута дозволяють при зчитуванні нормалізувати розмірзображення і його орієнтацію, а також кут, підяким камера –зчитувач розташована до поверхнізображення.

QR код можна прочитати і “вручну” без смартфона, для цього слід знати особливості QR-кодів іалгоритм дешифрування інформації [1]. Оскільки є багато готових і безкоштовних програм длягенерування QR-кодів та їх розпізнавання, необхідності в цьому немає.

Алгоритмом декодування може бути будь-який відомий та прийнятий, адже QR-код використовує двійкове кодування інформації: чорні квадратики кодуються одиницями, білі – нулями. Крім того,для виявлення і виправлення помилок при декодуванні виконується перевірка контрольних сум з використанням операції XOR (додавання бітів коду за модулем два до спеціальної восьми бітової двійкової маскою, наприклад 10101010). Завдяки виправленню помилок на код можна нанести рисунок, зробити його кольоровим та різнокольоровим – він залишиться читабельним. Розрізняють статичні та динамічні QR-коди.

Статичний QR-код містить інформацію, яку вказали при його генеруванні. Динамічний QR-код є багатофункціональним: до нього можна підключати додаткові функції, які будуть виконуватися одночасно чи змінити їх. Різновидами QR-кодів є Data Matrix та AztecCode. QR-коди можуть легко генеруватись з використанням вільно розповсюджуваного програмного забезпечення [3].Альтернативними QR-кодуванню технологіями є SonicNotify, RFID-мітки та NFC.

Література

1.Вячеслав Логачев. Что несет QR-код -http://www. ridcom.ru/ publications/131/.

2. Anna Skryabina. 20 способов использования QR-кодов.—http://computers-the.ru/?p=211/.

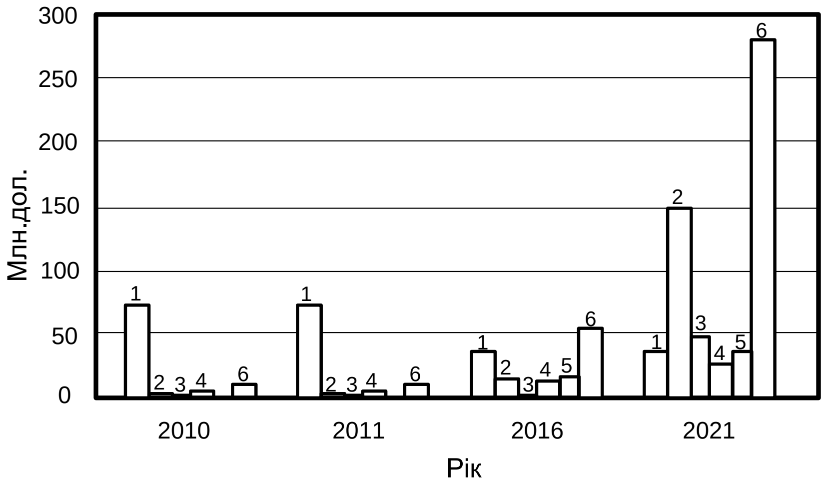
3.Читаем QR код - : http://habrahabr.ru /post/127197/.

Кременецька Я.А.
Доцент кафедри фізики
Морозова С.В.
Ст. викладачкафедри фізики
Державнийуніверситет телекомунікацій
м. Київ, Україна

РАДІОСИСТЕМИ СУБМІЛІМЕТРОВОГО ДІАПАЗОНА: ОСОБЛИВОСТІ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ

Особливість субміліметрового діапазону(300 ГГц – 3 ТГц). полягає в тому, що відповідні йому хвилі мають дуже велику довжину для застосування у добре розвинутій оптичній техніці і в той же час дуже коротку для перенесення в неї радіометодів. Протягом багатьох років субміліметровий діапазон в літературі називали «білою плямою», «спектроскопічним провалом». Зараз його прийнято називати «терагерцевою щілиною». Вчені здійснювали спроби створення альтернативних тепловим генераторів субміліметрового діапазону з кінця XIX століття. Ще у 1895 році П.М.Лебедєв за допомогою іскрового генератора, створеного ним же, отримав хвилі короткого міліметрового діапазону (до λ >3 мм). Однак через немонохроматичність та малу спектральну густину випромінювання метод не отримав широкого застосування. У 1902 році П.М.Лебедєв у доповіді «Шкала электромагнитных волн в эфире» відмічав, що субміліметровий діапазон, що відповідає «молекулярним коливанням матерії», при освоєнні зустріне суттєві труднощі: «Сейчас мы не имеем возможности предвидеть, как удастся разрешить это затруднение; во всяком случае способ получения еще более коротких волн будет очень крупным шагом вперед в области экспериментальной физики»[1].Терагерцевий діапазон хвиль був практично недосяжним до 2002 року, до створення першого терагерцевого квантово-каскадного лазеру, який працює на частоті 1,4 ТГц і має потужність 2 мВт. Відтоді проводяться інтенсивні дослідження з метою розв'язання фізичних та технологічних обмежень для створення пристроїв генерації, приймання, обробки та введення-виведення випромінювання терагерцевих сигналів.

Терагерцевий діапазон маєт аку чудову властивость, як іскробезпека, не спричиняє іонізуючу та руйнуючу дію. Саме тому він представляє значний інтерес для радіотехнічних застосувань, таких, як транспортна безпека, засоби зв'язку, медичне діагностичне обладнання, системи неруйнівних випробувань для військового використання та аерокосмічної апаратури. Згідно звіту «Системи терагерцевого випромінювання» (TerahertzRadiationSystems), опублікованого компанією BCCResearch (США), яка досліджує розвиток різноманітних технологій, ринок терагерцевих пристроїв у 2016 році становитиме 127 млн. долл., а у 2021 досягне 570 млн. [2] Найбільше застосування терагерцеві системи мають зараз у астрономічних дослідженнях (обсяг продажів у 2011 році становив 70 млн. долл.). Проте очікується, що до 2016 року продажі у цьому сегменті ринку зменшаться вдвічі (до 35 млн. долл.) і залишаться на цьому рівні до 2021 року (рис.1).



1- астрономічні дослідження
2- біомедичні дослідження
3- військові системи зв'язку
4- неруйнівні випробування
5- безпека передачі інформації
6- інші

Рисунок 1. Динаміка світового ринку за галузями застосування ТГц-приладів.

Основні особливості, переваги та області застосування терагерцевого діапазону

Хвилі терагерцевого діапазону мають здатність проникати у різноманітні непровідні непрозорі для світла у видимій частині спектру матеріали, такі як тканини, папір, пластмаса тощо, а також у велику кількість органічних сполук, в тому числі у тканини людського тіла. А оскільки енергія фотонів при терагерцевому випромінюванні невелика, то вона не спричиняє такого негативного шкідливого для людини впливу, яким є іонізуюче рентгенівське випромінювання. Більше того, багато хімічних та біологічних речовин у терагерцевому діапазоні мають унікальну структуру спектру, за якою можна проводити їх ідентифікацію.

У хвилях терагерцевого діапазону відсутні інтерференційні явища та завмирання сигналу, вони характеризуються хорошою відбивальною здатністю, швидкість передачі даних цих хвиль не менша 10 Гбіт/с, що сприяє розвитку засобів бездротового зв’язку ближнього радіусу дії, а також дозволяє створювати сотові системи радіусу до одного кілометра.

Характерна особливість цих хвиль така:

– великі обсяги інформації: розумний телевізор з терагерцевим трансівером зможе передавати і приймати зображення високої чіткості, а цифрова фотокамера з терагерцевим блоком – практично миттєво пересилати знімки портативному комп’ютеру;

– у межах нульової видимості здійснювати навігацію, застосовувати хвилі цього діапазону для автотранспортної безпеки;

– проводити відеозйомку за несприятливих погодних умов (під час дощу, сильного туману тощо), використовувати ці хвилі для систем зв’язку військового призначення у радіоелектронних засобах розвідки. Так, керівник програми «Терагерцева електроніка» Джон Альбретч відзначив, що здатність синхронно обробляти сигнали на частоті 0,85 ТГц дозволить створювати апаратуру, необхідну для реалізації програми DARPA «Відеолокатор з синтезуванням апертури» (Video Synthetic Aperture Radar, ViSAR) [3]. Мета цієї програми – розробка та демонстрація можливостей інформаційного датчика надзвичайно високої частоти (Extremely High Frequency, EHF), який в умовах щільної хмарності (природної, на зразок пісчаної бурі, або штучної димової завіси) зможе здійснювати таку ж ефективну роботу засобів систем виявлення, прицілювання та наведення, як і сучасні інфрачервоні системи у безхмарну погоду;

– будувати системи зв’язку на основі гібридного з’єднання оптоволокно-радіоканал (ГЗОР) [4], основні положення якого визначені у Рек. МСЭ-Р F.1332. Основними перевагами ГЗОР є, насамперед, надання системам широкосмугового радіозв’язку простого та ефективного інтерфейсу з ВОЛЗ, а також використання ряду переваг, притаманних оптоволоконним технологіям, таких, як висока завадостійкість, забезпечення великих розв’язок між оптичними каналами, безконтактна комутація;

– широкий спектр сигналу і перестроювання за частотою та амплітудою дає можливість моделювання різноманітних сигналів складних форм з різними властивостями за прохідністю, відбиваючою здатністю тощо, складних комбінованих способів кодування та модулювання інформаційних сигналів;

Проведений аналіз особливостей поширення радіохвиль показує, що в ТГц діапазоні (для хвиль 1,3 мм; 0,96 мм і 0,88 мм), для якого ослаблення не досить велике, і для малих дальностей дії радіотехнічних систем (до 500 м) цілком придатне. При цьому середні значення загасання з ймовірністю 0,8, зазначеною у «вікнах прозорості», не перевищують значення відповідно: 3 дБ/км; 8,5 дБ/км і 10 дБ/км [3]. Субміліметрові хвилі мають велику проникаючу здатність з теоретичною швидкістю передачі інформації більше 10 Гбіт/с.

Література:

1.Субмиллиметровая спектроскопия /Физика/ Е. М. Гершензон// Соросовский образовательный журнал . – 15/04/1998 . – N 4 . – 78-85 .

2.Майская В. На пути к достижению субмиллиметрового диапазона длин волн/В. Майская // Электроника: наука, технология, бизнес, 2013, № 6.-С.44-58.

3.Направления создания телекоммуникационных радиосистем миллиметрового и субмиллиметрового диапазонов волн / Б. М. Булгаков, С. А. Кравчук, Т. Н. Нарытник// "СВЧ-техника и телекоммуникационные технологии", международ. Крым.конф. (КрыМиКо'2003): материалы конф./ Севастополь : Вебер, 2003. - С. 305-308.

4.http://www. newelectronics.co.uk.

КамранХасілзаде
Магістр ФТ
Турал Мамедов
Магістр ФТ
ІлгинЕркан
Магістр ФТ
Державний університет телекомунікацій
м.Київ, Україна

ОЦІНКА ТОЧНОСТІ ПОЗИЦІОНУВАННЯ АБОНЕНТСЬКОЇ СТАНЦІЇЗ ВИКОРИСТАННЯМ МЕТОДУ CELL-ID

Як показує оцінка особливостей позиціонування [1], в даний час в операторів мобільного зв'язку найбільш популярним є метод позиціонування на основі ідентифікатора стільника Cell-ID. Оскільки на точність позиціонування можуть впливати різні фактори, такі як поширення радіохвиль до АС, що виконують АС хендовери й інше, то у зв'язку з цим необхідно оцінити достовірність даних, одержуваних від мережі мобільного зв'язку на першому етапі позиціонування АС. За результатами оцінки необхідно виробити ряд рекомендацій, що дозволяють зменшити ймовірність неточного позиціонування АС за допомогою методу Cell-ID.

Досліди проводилися на базідіючого оператора мобільногозв'язку в м.Київ. У дослідженні за допомогою методу Cell-ID здійснювалосяпозиціонування АС в декількохконтрольних точках, коли АС працювала в одному з стандарті взв'язку (GSM або UMTS). Потім проводилася перевірка точності позиціонування за допомогою навігаційної системи GPS.

У досліді АС рухалася з точки А до точки Б (з вул. Солом'янська 3 до вул.Солом'янська11). При цьому вона виконала декілька зупинок, в яких проводилося позиціонування АС по черзі в двох режимах:

- GSM;
- UMTS.

З метою позиціонування АС відправлялося смс-повідомленняіз запитом на позиціонування АС спочатку для випадку, коли АС працювала в стандарті GSM, потім АС переключалася на стандарт зв'язку UMTS.

Потім у всіх 18 контрольних точках було вироблено позиціонування АС за допомогою навігаційної системи GPS з метою визначеннядійсних координат місце знаходження АС.

На наступному етапі здійснювалася оцінка похибки позиціонування АС шляхом зіставленняданих з Web-інтерфейсу послуги позиціонування оператора мобільного зв'язку і даних про точне місцезнаходження АС, отриманих за допомогою навігаційної системи GPS (рис. 1, 2).

Потім на підставі DBBS Plan (комплексу клієнт - серверних додатків, що працюють під управлінням MS SQL Server) вироблялося порівняння отриманих даних з чинним покриттям мережі мобільного зв'язку.

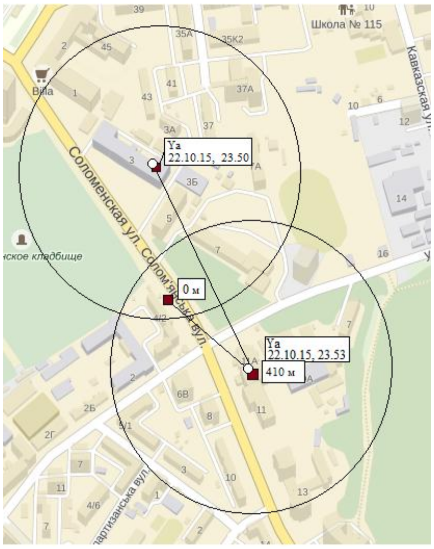


Рисунок1 Приклад позиціонування АС за допомогою методу Cell-ID в стандарті GSM

Таблиця1ОцінкадостовірностівизначенняCell-ID, в якомузнаходиться АС

№ онтрольна точка	Режи м роботи АС	Радіусз они,м	Попад ння в зону (дані з GPS)	Відста ньвід центра зони, м	Пох ибка, м
1	GSM	600	Так	600	-
	UMT S	300	Так	300	-
2	GSM	600	Так	600	-
	UMT S	300	Так	300	-
3	GSM	600	Так	300	-
	UMT S	500	Так	287	-
	GSM	600	Так	410	-

4	UMTS	700	Так	468	-
5	GSM	900	Так	216	-
	UMTS	800	Так	257	-
6	GSM	900	Так	400	-
	UMTS	750	Ні	-	150
7	GSM	800	Так	688	-
	UMTS	700	Так	530	-
8	GSM	850	Так	305	-
	UMTS	700	Так	320	-
9	GSM	900	Так	238	-
	UMTS	800	Так	281	-
10	GSM	1000	Так	600	-
	UMTS	1100	Так	500	-
11	GSM	1100	Так	440	-
	UMTS	900	Так	448	-
12	GSM	1300	Так	673	-
	UMTS	1000	Так	590	-
13	GSM	1200	Так	678	-
	UMTS	1000	Так	780	-
14	GSM	1400	Так	620	-
	UMTS	1300	Так	580	-
15	GSM	2000	Так	400	-
	UMTS	1100	Ні		928
16	GSM	1500	Так	642	-
	UMTS	1500	Так	761	-
17	GSM	3400	Так	656	-
	UMTS	3400	Так	764	-
18	GSM	1500	Так	642	-
	UMTS	1500	Так	761	-

У табл. 1 наведені результати оцінки достовірності визначення Cell-ID, в якому знаходиться АС. Вказанідані для різних контрольних точок і режимів роботи АС (GSM/UMTS). Під радіусом зони похибки розуміється значення радіуса кола, в який потрапляє АС при проведенні вимірювань. Розмір окружності знаходиться з Web- інтерфейсі програми позиціонування оператора мобільного зв'язку і відповідає зоні обслуговування сектора базової станції, в якому знаходиться АС. Попадання в зазначену зону оцінюєтьсяза допомогою GPS приймача, вбудованогов АС.

Параметр «Відстаньвід центру зони» є допоміжним і оцінюєвідстань, на якому опинилася АС від центру сектора, вякому вона була позиціонована засобами мережі мобільного зв'язку.

Похибка позиціонування методом Cell-ID показує відстаньвід кола (або зони обслуговування сектора), в яку повинна була потрапити АС, до справжнього стану АС (рис. 2).

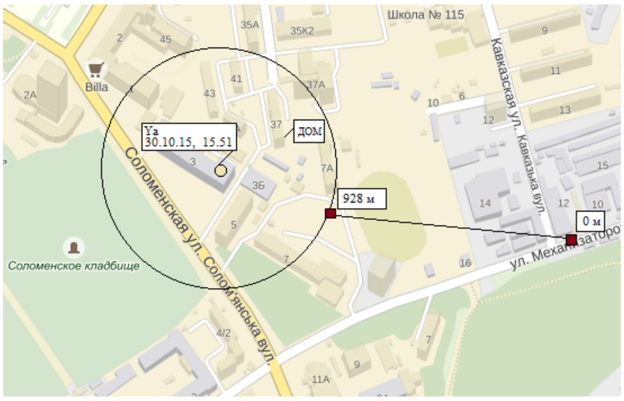


Рисунок 2 Позиціонування АС за допомогою методу Cell-ID в стандарті UMTS,обраний примусово

Рисунок 3 Територіальне розташування сайтів мереж стільникового зв'язку стандартів GSM і UMTS

Незважаючи на те, що зона дії стандарту UMTS менше, ніж у GSM, в місті похибка позиціонування АС для стандартів GSM-900, GSM-1800 і UMTS відрізняється незначно. Це можна пояснити частим розташуванням БС стандартів GSM і UMTS в місті.

У разі примусової прив'язки АС до частоти, що відрізняється від частоти, яку видає мережу, в більшості випадків спостерігається погіршення точності позиціонування. Значення похибки позиціонування тим вище, чим далі знаходиться обрана частота в списку «сусідів», що в більшості випадків аналогічно найбільшою віддаленості БС від АС. Функція вибору частоти може використовуватися абонентами при наявності встановленого на АС спеціалізованого програмного забезпечення (нетмонітора) і служить, наприклад, для виборучастоти, на якійприсутній EDGE, абочастоти з найменшими перешкодами, чи меншою завантаженістю (зайнятістю TS).

Для більш точного позиціонування оператор повинен мати якомога точнішу цифрову карту із зазначенням території зони обслуговування кожної з сот, що можливо лише при проведенні значного числа вимірів за рівнем сигналу в різних зонах обслуговування, а також визначення географічного місця розташування точок естафетної передачі обслуговування між сотами.

Література:

1.Горелик, АЛ. Некоторые вопросы построения систем распознавания/ А.Л. Горелик, В.А. Скрипкин. - М.: Советскоерадио, 1974. - 224 с.

2.Parsons J.D. The Mobile Radio Propagation Channel. - London, Pentech Press Publisher, 1992. — 316 p.

3.Котоусов, Л. С. Теоретические основы радиосистем/ А.С. Котоусов.- М.: Радиосвязь, радиолокация, радионавигация, 2002.

4.Позиционирование в сетях мобильной связи, новые услуги//www.mobile-review.com

Сєрих С.О.

Доцент каф. Інформаційних технологій

Державний університет телекомунікацій

м. Київ, Україна

АНАЛІЗ ДОСЛІДЖЕННЯ СПЕКТРІВ СКЛАДЕНИХ СИГНАЛІВ ДЛЯ ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Аналіз довгостроковихдослідженьза напрямком підвищення надійності обміну повідомленнями безпроводових засобів зв'язку переконує, що стрімке збільшення кількості кінцевих засобів, швидка змінність їх просторового зосередження, об'єктивне зростання об'єму повідомлень, а відповідно і часу надання телекомунікаційної послуги суттєво впливають на вірність приймання сигналів. Погіршення електромагнітної сумісності (ЕМС) об’єктів систем радіозв’язку, а тим більш навмисне їх пригніченняпротидіючими засобами чи сумісно діючими системами вказують на неможливість розв’язання проблеми у енергетичний спосіб.

Тому системи радіозв'язку, особливо мобільні, нового покоління повинні будуватися на основі використання [1] складних сигналів (СС), які забезпечують вирішення проблеми за рахунок оптимізації структури сигналів [2] і при застосуванні передових цифрових технологій мінімізацію ускладнення пристроїв формування та обробки сигналів з базою $Б_с = T_с\Delta F >> 1$. Але підвищення завадозахищеності сигналів тільки за рахунок значного збільшення $Б_с$мають наслідки непропорційного ускладнення обладнання, що вказує на необхідність дослідження і пошуку раціональних структур сигналів та вибору ефективних для досягнення конкретної мети видів сигналів, які визначаються типом модуляції СС чи їх комбінацією.

Виходячи з того, що в широкосмугових радіосистемах з підвищеними вимогами до завадостійкості [3] частіше знаходять застосування фазоманіпульовані сигнали (ФМ) з прямим розширенням спектра або шумоподібні сигнали (ШПС) завдання вибору ефективного виду СС не розглядається. Але в разі коли пристрої обробки ФМ ШПС за значенням $Б_с$ наближаються до межі, що пов’язана із раціональністю витрат на реалізацію, дієвим напрямком стає використання додаткового ступеню поширення сигналу за рахунок використання псевдовипадкової перебудови робочої частоти (ППРЧ). Разом з тим затрати на реалізацію попереднього ступеня можливо скоротити, якщо застосувати складені структури СС. Доцільність застосування такого підходу до розв’язання проблем базується на аналізі взаємокореляційних властивостей сигналів та потребує поглибленого аналізу спектру складених СС.

Для спрощення аналізу спектрів складених ФМ ШПС сигнал можливо представити як послідовність позитивних і негативних прямокутних імпульсів [1], що чергуються за законом кодової формуючої послідовності $A=(a_1.a_2,...a_n\ldots a_{Ne})$, тобто двох амплітуд імпульсів відповідних значенням 1 і -1, що співпадають із значеннями – 0 і π для ФМ ШПС маючи однакову кодову відстань. Загальний ансамбль - Q таких сигналів позначається як - $\{a_n\}^{Ne}$, де N_e це кількість елементів сигналу.

Спектр ФМ ШПС (точніше спектр комплексної огинаючої) $G(\omega)$ визначається добутком спектра імпульсу $S_0(\omega)$ і спектру кодової послідовності $H(\omega)$. Нерівномірність $G(\omega)$ цілком визначається спектром кодової послідовності, що залежить від вибору структури $\{a_n\}^{Ne}$. При цьому кількість послідовностей із якісними ВКФ і АКФ в загальному ансамблі Q дуже мало, що в часи найбільшого навантаження не задовольняє вимогі до кількості одночасно працюючих в системі абонентів із індивідуальними ПВП.

Екстенсивний напрямок їх збільшення [4] потребує підвищення значення $Б_с$, яке для системи кінцеве та обмежене смугою ΔF, щовідведено їй для роботи. Саме тому застосування складених СС при незначному погіршені властивостей ВКФ і АКФ але спрощенні реалізації пристроїв обробки (ПО) із досягненням не тільки номінального значення $Б_с$ а і адаптації її значення до завадових умов стає доцільним.

Обробка складених ФМ ШПС [1, 4] здійснюється поетапно у спосіб накопичення несучих послідовностей, наприклад, в узгоджених фільтрах (УФ) першого ступеня із кількістю елементів $N_н$,рішенням для яких стають елементи модулюючої послідовності із кількістю $N_м$ у другому ступені, що накопичуються в УФ для прийняття рішення про елемент сигналу. Тоді вираз для бази складеного сигналу зазначається як $Б_с=Б_н \cdot Б_м$, а тривалість сигналу через тривалість елементу та їх кількості у відповідних послідовностях як $T_с=\tau_е \cdot N_н \cdot N_м$. Загальний ансамбль такого складеного ФМ ШПС також зростає пропорційно добутку $Q_н \cdot Q_м$ – ансамблів несучої і модулюючої ПВП відповідно. Тоді вибором раціональної структури $\{a_п\}^{Nе}$ на формуючих поліномах якісних властивостей можливо зменшити зазначений раніш недолік.

При аналізі спектра складеного СС доцільно зазначити, що найбільша частина його енергії -$E_с$ зосереджена в частотно–часовому прямокутнику зі сторонами ΔF і $\tau_е \times Б_с$.Значення її можна отримати через квадрат модуля огинаючої, змінною величиною якого є квадрат модуля амплітудного спектра - $H(\omega)$. Для складеного ФМ ШПС він має вигляд [3, 5]:

$$
|H(\omega)|^2 = \Bigg[N_м N_н + 2N_м \sum_{n=1}^{N_н-1} (\cos n\omega_э) \sum_{k=1}^{N_н-n} a_k a_{k+n} + 2N_н \sum_{m=1}^{N_м-1} (\cos m\omega\tau_э) \sum_{l=1}^{N_м-m} a_l a_{m+l} + 4 \sum_{m=1}^{N_м-1} (\cos m\omega\tau_э) \times
$$

$$
\times \sum_{n=1}^{N_н-1} (\cos n\omega\tau_э) \sum_{l=1}^{N_н-m} a_l a_{m+l} \sum_{k=1}^{N_н-n} a_k a_{n+k} \Bigg]^2 \qquad (1)
$$

Аналіз $|H(\omega)|^2$ показує:

-додаткові сплески елементів спектру кодових послідовностей реальних ФМ ШПС гуртуються біля значення - $\sqrt{Б_с}$, що відповідає першому доданку в (1) і для формуючих поліномів із ідеальною АКФ, тобто без бокових піків, їх не буде зовсім;

- чим більше рівень бічних піків АКФ, тим більше флуктує амплітудний спектр і з більшою нерівномірністю розподілена $E_с$;

- наявність істотних максимумів спектральної щільності сигналу визначаються значеннями наступних трьох доданків в (1), які навіть при зразковій рівності кількості 1 та-1 структури $\{a_п\}^{Nе}$, досягають значення $Б_с/2$ і більше.

Висновки. Для використання в системах що розгортуються на задане значення Q потрібен додатковий підбір структур кодових послідовностей без узагальнюючої усередненої оцінки їх ВКФ і АКФ [1], за реальними$H(\omega)$.

За результатами попереднього аналізу [1, 5] на відміну від спектрів довільних послідовностей, що мають значні нерівномірності, М–послідовності (також сегменти послідовностей Гоулда, Насами [1]) більш рівномірні, особливо коли в складених структурах$N_н \approx N_м$.

Для систем з підвищеними вимогами до скритності наявність відчутних максимумів у спектрах кодових послідовностей збільшує ймовірність постановки в них навмисних завад, що небажано.

Завада або багаточастотні завади в максимумі або максимумах енергетичного спектру сигналу після їх режекції[2]зменшує енергію корисного сигналу, що призводить до збільшення – імовірності помилкового приймання сигналу, тобто зниження завадостійкості.

Таким чином функціонування радіосистем в умовах дії завад (імпульсних або багаточастотних) в загальному випадку навмисних вимагає ретельного вибору структури $H(\omega)$ і застосування СС з найбільш рівномірним спектром з метою підвищення завадозахищеності телекомунікаційних систем.

Література:

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985.–384с.

2.Сєрих С.О. Проблеми завадостійкості радіоліній з складними сигналами в умовах активних завад. // ЗВ'ЯЗОК.—2013.-- № 4.- С. 32-37.

3.Серых С.А. Анализ спектров составных фазоманипулированных сигналов и условия их применения в телекоммуникационных системах/ С.А. Серых, В.Р. Соловьев, О.В. Кокотов, П.М. Скачков // ЗВ'ЯЗОК.- 2002.- № 6.- С. 48-51.

4.Серых С.А. Составной согласованный фильтр для обработки сложных сигналов с большой базой -- К.: КВАИУ, НТЗ № 1.- 1986. – С. 133-134.

5.Серых С.А. Методика выбора составных широкополосных сигналов для мобильных систем CDMA/ С.А. Серых, В. Р. Соловьев, О.В. Кокотов // Вісник ДУІКТ.- 2009. --№ 2.- С.112-117.

Полоневич А.П.
К.т.н., доцент каф. Комутаційних систем
Невдачина О.В.
К.т.н., доцент каф. Комутаційних систем
Ярошенко С.О.
Магістр ФТ
Державний університет телекомунікацій
м.Київ, Україна

ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ В МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Ряд експертів характеризують поточну ситуацію в мережевій галузі як «критичну і революційну». Домінуючі на ринкузакриті рішення являють для додатків «чорніящики», а сумісність рішень різних вендорів забезпечується в кращому разі на рівні інтерфейсів. Мережі є надто складними, що ускладнює їх масштабування і управління ними, знижує їх надійність. Очевидно, що це гальмує подальший розвиток мережі функціонуючих в них додатків.

Основними передумовамидо появиконцепцій«програмно обумовлених» (або «програмно конфігурованих») мереж (Software-DefinedNetworking, SDN) і віртуалізації мережевих функцій (Функція мереживіртуалізації, NFV) є, насамперед, швидке зростання трафікуданих ікількостіпідключених до мережі пристроїв.

В операторів виникла реальна потреба в динамічній пріоритетності трафіку. Наприклад, в деяких випадках пріоритет повинен бути зроблений для FTP-протоколу, в інших - для SIP і навпаки.

У галузі стільникового зв'язку установка додаткових макростільниками (базових станцій) після досягнення певного порогу щільності їх розміщення вже не дає істотного приросту пропускної здатності та ємності мереж радіодоступу (RAN), тому наступним етапом стає використання малих сот (фемто- і пікосоти). В результаті конфігурування великомасштабних мереж перетворюється на складне завдання і вимагає серйозних змін принципів побудови, експлуатації та управління мереж та управління ними.

За результатами дослідження IHS iSuppli, до 2017 року кількість користувачів хмарних сервісів досягне 1,3 млрд. чоловік. Дослідження Microsoft показало, що в Європі хмарна платформа в 40 разів економить бюджет компанії, при цьому 59% опитаних говорять про продуктивності бізнесу, 57% заявляють про реальну економію грошей і 24% відзначають появу інновацій в їхніх компаніях.

Модель мережі мобільного зв’язку, реалізована на базі хмарних технологій

Загальна модель мережі стільникового зв’язку на основі хмарних технологій представлена на рисунку 1

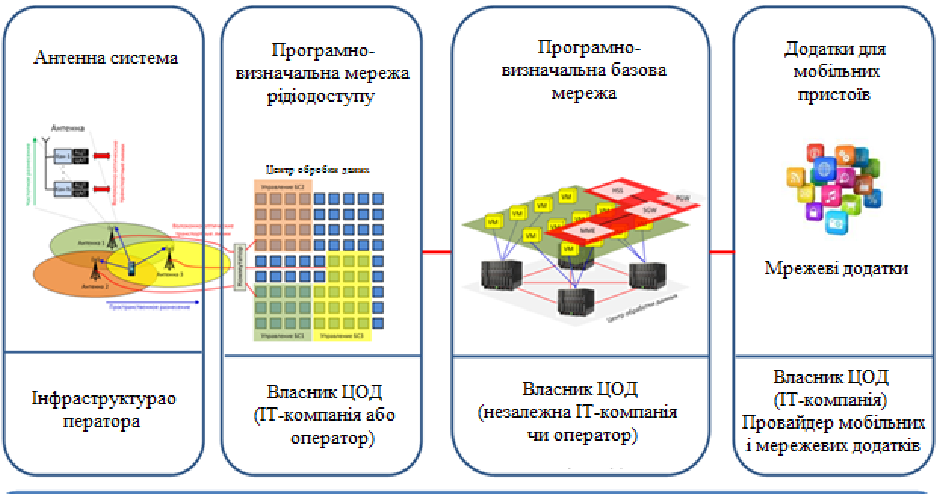


Рисунок 1 - Загальна модель мережі стільникового зв’язку на основі хмарних технологій

Функціонал розподілу радіоресурсів в стандартах LTE, UMTS, GSM здійснюється у віртуальній програмної мережі RAN на базі центру обслуговування даних (ЦОД).

Всі елементи ядра мережі LTE (EPC) реалізуються у вигляді програм на основі високонадійних ЦОД. Управління мережею виробляє єдиний контролер, де зберігається інформація про стан всієї мережі.

Всі елементи базової мережі LTE (EPC), реалізуються у вигляді програм на базі високонадійних ЦОД. Управління мережею здійснює єдиний контролер в якому зберігаться інформація про стан всієї мережі.

Мережеві і мобільні додатки будуються на ЦОДах операторів, IT або сервіс-провайдерів і здійснюють взаємодію з стільниковою мережею за допомогою стандартних програмних інтерфейсів.

Три постачальника послуг працюють над планами розгортання хмарної мережі радіодоступу (C-RAN), концепція якої передбачає використання серверів x86 для обробки дзвінків стільникових телефонів, на відміну від підходу з традиційними бездротовими базовими станціями.

Компанія ChinaMobile, найбільший стільниковий оператор в світі (700 мільйонів абонентів), була ініціатором випробувань і планів розгортання системи вже в 2015 році. Японська NTT Docomo заявила, що піде за нею в 2016 році, а третій, поки невідомий оператор, зараз теж готує плани на C-RAN, як стверджує ГіладГарон (GiladGaron), виконавчий директор AsocsLtd, постачальника процесорів для модемів.

За оцінками експертів, за рахунок перенесення в «хмару» окремих елементів мережі радіодоступу оператори стільникового зв'язку зможуть скоротити свої капітальні витрати на 30-60%. Використання принципів програмованого управління мережею і віртуалізації мережевих сервісів входить в урядовий «Перелік пріоритетних наукових завдань».

Компанія J'son&PartnersConsulting представляє основні результати дослідження нових трендів в стільниковому зв'язку: віртуалізації мережевих функцій (NFV) та програмно-конфігуруються мереж (SDN).

Передумови для появи SDN і NFV

Ряд експертів характеризують поточну ситуацію в мережевий галузі «критичну і революційну». Домінуючі на ринку закриті (пропрієтарні) рішення являють для додатків «чорні ящики», а сумісність рішень різних вендорів забезпечується в кращому разі на рівні інтерфейсів. Мережі є надто складними, що ускладнює їх масштабування і управління ними, знижує їх надійність. Очевидно, що це гальмує подальший розвиток мереж і функціонуючих в них додатків.

Основними передумовами до появи концепцій «програмно визначаються» (або «програмно конфігуруються») мереж (Software-DefinedNetworking, SDN) і віртуалізації мережевих функцій (NetworkFunctionVirtualization, NFV) є, насамперед, швидке зростання трафіку даних і кількості підключених до мережі пристроїв.

При цьому сам трафік стає різнорідним - якщо в кінці 1990-х рр. його основу становила пересилання даних і файлів без особливих вимог до каналу, за винятком швидкості передачі даних, то вже до середини 2000-х на перше місце вийшли питання забезпечення якості сервісу (QoS), мінімальної затримки в каналі (latency) і ін. Це, в першу чергу, пов'язано зі зміною структури користувача трафіку, в якому стали переважати комунікації в реальному часі (RealTime Communications, RTC) - VoIP, відеосервіси тощо. В операторів виникла реальна потреба в динамічній пріоритетності трафіку. Наприклад, в деяких випадках пріоритет повинен бути зроблений для FTP-протоколу, в інших - для SIP і навпаки.

У галузі стыльникового зв'язку установка додаткових макростільників (базових станцій) після досягнення певного порогу щільності їх розміщення вже не дає істотного приросту пропускної здатності та ємності мереж радіодоступу (RAN), тому наступним етапом стає використання малих сот (фемто- і пікосоти). В результаті конфігурування великомасштабних мереж перетворюється на складне завдання і вимагає серйозних змін принципів побудови, експлуатації та управління мереж та управління ними.

Концепції SDN і NFV

Основна суть SDN складається у фізичному поділі рівня управління мережею (networkcontrolplane) від рівня передачі даних (forwardingfunctions) за рахунок перенесення функцій управління (маршрутизаторами, комутаторами і т. п.) в програми, що працюють на окремому сервері (контролері).

У результаті повинна вийти гнучка, керована, адаптивна і економічна архітектура, яка здатна ефективно адаптуватися під передачу великих потоків різнорідного трафіку.

Основні ідеї SDN включають:

- поділ проходження трафіку (dataplane) і сигналізацію/управління (controlplane);
- істотне спрощення мережевих елементів рівня dataplane;
- єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем управління і рівнем передачі даних;
- логічно централізоване управління мережею, здійснюване за допомогою контролера з встановленою мережевою операційною системою і реалізованими поверх мережевими додатками;
- віртуалізація фізичних ресурсів мережі.

Базові ідеї SDN були сформульовані фахівцями університетів Стенфорда і Берклі ще в 2006 р, і ініційовані ними дослідження знайшли підтримку у великих операторів та інтернет компаній (Google, DeutscheTelekom, Facebook, Microsoft, Verizon і Yahoo). В результаті в березні 2011 р був утворений консорціум OpenNetworkingFoundation (ONF), склад якого швидко розширюється, в 2013 р до нього увійшли понад 100 компаній, включаючи Brocade, Citrix, Oracle, Dell, Ericsson, HP, IBM, Marvell, NEC, VMware та ін.

ONF розвиває, насамперед, протокол OpenFlow, який реалізує взаємодію контролера з мережевими пристроями, однак ряд членів цієї організації зацікавлений у більш універсальних специфікаціях.

Ідея OpenFlow проста і заснована на спостереженні, що незважаючи на істотні відмінності між сотнями моделей комутаторів і маршрутизаторів, всі вони містять таблицю передачі, визначальну базову функцію передачі даних - для кожного, хто входить пакету переправити його якнайшвидше на певний вихідний інтерфейс. Більше того, хоча формат цих таблиць різний, можна ідентифікувати стандартний набір функцій даного рівня.

Кожен запис абстрактної таблиці передачі OpenFlow є "правилом" і пов'язана з так званим «потоком» даних (потік). Потік визначається заголовком пакету - наприклад, комбінацією адрес MAC, IP номерів портів джерела і одержувача даних, хоча в принципі потік може складатися з пакетів з певним (нестандартним) заголовком - наприклад, для підтримки нових нестандартних протоколів. Не всі елементи цієї комбінації повинні бути визначені - наприклад, потік може бути визначений як весь трафік до деякого хосту. У цьому випадку визначеним є тільки один елемент - ІС адреса одержувача даних.

Іншим елементом записи таблиці є «дія», що визначає необхідну обробку пакетів потоку. Основних дій яких є:

Передати пакет на певний порт (або певні порти) комутатора.

Передати пакет контролеру через «захищений» канал. Контролер - це керуючий центр мережі, що включає центральну мережеву операційну систему і керуючі додатки, що розраховує топологію і маршрути, а також здійснює інші функції управління. Тому, як правило, перший пакет невідомого потоку відправляється контролеру для визначення правила і створення нового запису таблиці передачі.

Відкинути пакет. Ця дія може бути необхідним, наприклад, у боротьбі з комп'ютерними атаками.

Нарешті, пакет може бути направлений на «стандартну» обробку, наприклад якщо OpenFlow-комутатор також є стандартним комутатори, маршрутизатори і т.п. Дана функціональність дозволяє розділити потоки даних на потоки, керовані OpenFlow, і потоки, керовані іншими механізмами, наприклад, за допомогою існуючих протоколів маршрутизації. Завдяки цьому, наприклад, дослідники можуть ізолювати експериментальний трафік від нормального, використовуючи загальну інфраструктуру.

У квітні 2013 компанії Cisco, Citrix і IBM сформували структуру OpenDaylight.org, мета якої - випуск відкритого загальнодоступного стандарту SDN, заснованого на вільному ПЗ.

Таким чином, SDN намагається розділити дві площини - управління мережею і транспорт, і в підсумку забезпечити централізацію управління розподіленої мережі з метою більш ефективного використання ресурсів та автоматизації управління мережевими сервісами. NFV же зосереджена на оптимізації мережевих сервісів всередині мережі за рахунок поділу мережевих функцій (наприклад, DNS, кешування та ін.), Від власне реалізації апаратного забезпечення. Вважається, що NFV дозволяє універсалізувати програмне забезпечення, прискорити впровадження нових функцій мережі та служб і при цьому не вимагає відмови від уже розгорнутої мережевої інфраструктури.

Стосовно до мереж стільникового зв'язку віртуалізація виражається, зокрема, в концепції C RAN - хмарної (Cloud) або централізованої (Centralized) мережі радіодоступу. У цьому випадку радіопідсистеми (remoteradioheads, RRHs) і антени відокремлюються від основних блоків (модулів управління) базової станції (basebandunits, BBUs), які розташовуються в так званому basestationhotel і з'єднуються через оптоволоконний кабель з блоками RRHs (рис. 2). Таким чином, оператори можуть будувати хмарні мережі радіодоступу за принципом NFV, розміщуючи в хмарі основний функціонал базової станції, відповідальний за цифрову обробку сигналу, синхронізацію, управління, збір статистики та ін. Не виключено, що такий тип хмарних і віртуальних мереж радіодоступу може істотно змінити розстановку сил на користь IT вендорів.

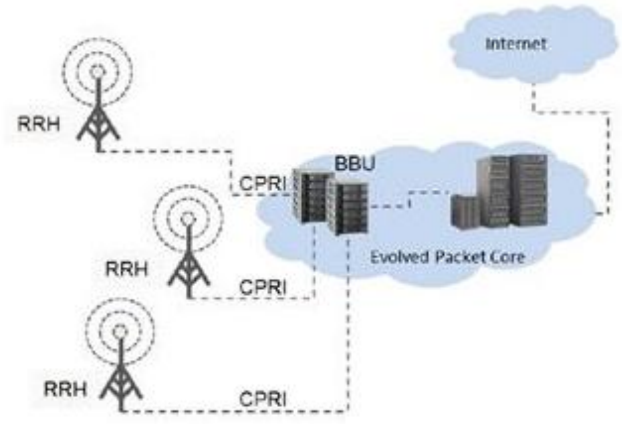


Рисунок 2 Архітектура хмарної мережі радіодоступу (C-RAN)

Основні драйвери та стримуючі чинники впровадження з погляду операторів, інтерес в SDN пов'язаний з підвищенням ефективності мережевого обладнання, зниженням витрат, підвищенням мережевої безпеки і наданням можливості програмно створювати нові сервіси та оперативно завантажувати їх в мережеве обладнання.

Література:

1.Співаковський О. В. Теорія і практика використання інформаційних технологій у процесі підготовки студентів математичних спеціальностей: монографія / Олександр Володимирович Співаковсккий - Херсон: Айлант, 2003. - 250 с.

2.Колеров Ю. Облачныйрынок в цифрах и фактах: взглядParallels. Докладна CLOUD ComputingSummit 2013

3. Leung, J. Y. Handbook of Scheduling. Algorithms, Models and Performance Analysis / Y-T. Joseph. - Leung: CRC Press, 2004. - 622 p.

ГринкевичГ.О.
К.т.н, доценткаф.Телекомунікаційнихсистем
Перепелиця Н.Л.
Зав. лаб. каф. Телекомунікаційних систем
Державний університет телекомунікацій
м. Київ, Україна

ІМІТАЦІЙНА МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНОСТІ МЕТОДУ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ПЕРЕДАЧІ ДАНИХ І ОБҐРУНТУВАННЯ ДОСТОВІРНОСТІ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Сучасний рівень інформатизації і комп'ютеризації українського суспільства, впровадження безлічі інтерактивних мультимедійних інфо-комунікаційних послуг практично в усі сфери громадської діяльності, вдосконалення засобів зв'язку і обробки даних, цифровізація радіо і телевізійного мовлення обумовлюють інтеграцію ряду телекомунікаційних послуг в єдину багатофункціональну інтерактивну мультимедійну підсистему і диференціацію завдань обробки даних і додатків по пріоритетності окремих показників якості передачі інформації [1]. Розробка імітаційної моделі систем ідентифікації трафіку.В якості основного інструментарію імітаційного моделювання використовуємо середовище символьної математики MathCAD - 14 [2]. У імітаційній моделі підсистеми параметричної ідентифікації трафіку реалізована процедура n- мірного шкалування на основі, якій приймається рішення про розбиття інформаційного трафіку по категоріях і напрям його на різні мережеві облаштування(порти) багато-протокольного вузла зв'язку. Використовуючи методи і прийоми математичного і імітаційного моделювання оцінено ефективність розробленого методу підвищення оперативності передачі даних в телекомунікаційній мережі, проведено порівняльні дослідження з відомими методами(побудованими на принципах статичного управління чергами і "справедливого" розподілу ресурсів у багатопротокольних вузлах зв'язку)

Проведений аналіз і дослідження показали, що основою системи управління чергами у багато-протокольному вузлі зв'язку є підсистеми установки первинних параметрів і динамічного розподілу ресурсів. Для підтвердження ефективності розробленого методу в порівнянні з методом, ґрунтованим на принципах статичного управління(алгоритмах обслуговування черг без пріоритетів) с обліком, знайдемо відношення J_{cy}/J варіацій часу доставки інформаційного пакету(джиттер затримки) в ТКС при використанні методу статичного управління і розробленого методу.

Вхідними даними для вказаних підсистем є в першу чергу імовірнісно-тимчасові характеристики інформаційного потоку, такі як інтенсивність інформаційного потоку, час очікування інформаційних пакетів в черги, джиттерзатримки, а також статистичні дані про поведінку інформаційного потоку різних служб прикладного рівня.

Функціонування усіх приведених підсистем має на меті реалізацію принципу справедливого розподілу мережевих ресурсів з урахуванням пріоритетного обслуговування трафіку мультимедійних служб.

Для оцінки ефективності методу підвищення оперативності передачі даних і обґрунтування достовірності отриманих результатів проведено імітаційне моделювання систем ідентифікації трафіку і управління чергами у багатопротокольних вузлах зв'язку телекомунікаційної мережі.

Дослідження структурних і функціональних властивостей багатопротокольних вузлів зв'язку проводилося з використанням теорії графів і теорії масового обслуговування. Дослідження характеру зміни інтенсивності інформаційних потоків між окремими елементами телекомунікаційної мережі спиралося на основні положення теорії вірогідності, теорії зв'язку і теорії телетрафіку. Оцінка коректності і достовірності теоретичних і практичних результатів проводилася за допомогою методів математичного і імітаційного моделювання.

Отже, показали доцільність використання розробленого методу підвищення оперативності передачі даних, особливо в умовах підвищеного завантаження багатопротокольних вузлів зв'язку мультимедійним трафіком.

Література:

1 С.В. Толюпа, Р.В. Хращевський, Г.О. Гринкевич, А.О. Макаренко, О.В. В'юннік Начальний посібник "Управління та якість послуг інформаційних мереж зв'язку" Київ: ДУТ, 2014. [176, 361 с.]

2 Кучерявий Е.А. Управління трафіком і якість обслуговування в мережі Інтернет / Євгеній Андрійович Кучерявий. - Спб.: Наука і техніка, 2011. –[244, 336 с.]

Ткаленко О.М.
К.т.н., доцент каф. Комутаційних систем
Державний університет телекмунікацій
м.Київ, Україна

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЕЗПРОВОДОВОГО ВИСОКОЧАСТОТНОГО ЗВ`ЯЗКУ МАЛОГО РАДІУСУ ДІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В наш час спостерігається впровадження безпроводових технологій у різні області застосування. Вони заміняють проводові технології і роблять комунікацію між пристроями зручнішою і простішою для користувача. Сьогодні стандарт NFC (NearFiledCommunication) розвивається разом з такими технологіями, як Wi-Fi, Wi-Max. Технологія NFC, перед усім, призначена для використання у мобільних пристроях. Вона є логічним продовженням технологій RFID [1, 4]. Технологія NFC отримала максимальне поширення в якості технології для здійснення безконтактних платежів. Але, останнім часом все частіше можна побачити як можна використовувати NFC в різних галузях. Наприклад, смарт-карту з вбудованим NFC чіпом як проїзний у громадському транспорті, як платіжну карту в установах роздрібної торгівлі, як «розумну» візитку, як безконтактну картку-ключ та багато іншого. З поширенням технології в певних галузях стане можливим більш простішийдоступ до певних функцій. Тому її впровадження на даний момент є дуже актуальним.

NFC в Україні знаходиться в початковій стадії, незважаючи на те, що в інших країнах вже було накопичено достатній досвід практичного використання цієї технології. Основною проблемою впровадження повсюдного використання NFC платежів в Україні як і в решті світу, є мала кількість NFC-сумісних смартфонів, а також відсутність єдиного підтримуваного усіма виробниками стандарту оплати для уніфікації всіх пристроїв, які можуть здійснювати безконтактну оплату. Але, за прогнозами аналітиків кількість NFC-сучасних пристроїв значно виросте до 2017року.Основні фактори, які стримують розвиток NFC в Україні, це: побоювання користувачів з приводу безпеки проведення таких платежів, недостатньо розвинута інфраструктура і відсутність інформації.

Для активного розвитку технології NFC в Україні необхідно, щоб користувач мав телефон/ SIM-карту, що підтримує NFC; технологія повинна бути зрозумілою, доступною для користувача, бути простішою, ніж інші і мотивувати її використання; вартість щоб була розумною; вирішилося питання безпеки (потрібно враховувати, що при втраті мобільного, доступ до засобів буде відкритий новому власникові нашого телефону).

Безсумнівна перевага NFC - простота використання. Для обміну необхідно піднести пристрої близько один до одного. Пропонуються наступні способи впровадження технології NFC та її актуальність.

Таблиця 1 - Способи впровадження технології NFC

Область	Приклад
Оплата за допомогою мобільного телефону	Купівля квитків або оплата таксі бота з безконтактними терміналами продажів (платіжні системи) берігання чеків в пам'яті телефону
Телефон як електронний ключ	Для проходу в будівлю (контроль доступу) Для доступу до ПК Для автомобіля Для створення офісу будинку

Передача даних	Обмін електронними візитками Друк фотографій безпосередньо з фотоапарата
Електронне блокування	Доступ до глобальних мереж або Bluetooth
Доступ до даних	Завантаження розкладів з електронного табло на телефон Завантаження карт на телефон читування навігаційних Координат
Зберігання електронних квитків на мобільному телефоні	В театр, на атракціон або на який-небудь захід

Одним з найбільш перспективних варіантів використання технології NFC – це оплата за допомогою мобільного телефону. Телефон з чіпом встановлює з'єднання з платіжним терміналом, який зчитує необхідну інформацію. В результаті з'єднання з рахунку абонента списується вартість послуги. Переваги технології мобільних NFC платежів: простий персоналізований інтерфейс для управління NFC додатками; швидкість проведення транзакцій; «картковий» рівень безпеки платежу; можливість реалізації декількох додатків в одному пристрої; віддалена установка і управління додатками; номер телефону - засіб ідентифікації платника.

Чіп NFC виконує роль електронного ключа, відмикає машину, квартиру, офіс або номер готелю. Що особливо важливо, у випадку втрати може бути легко заблокований віддалено (і не прийдеться спішно міняти купу дорогих замків). З рідерів (і замків) можна буде прибрати весь логічний функціонал. Перевірка ідентифікаційних даних переміститься в сам телефон, який на підставі певних правил буде приймати рішення про те, чи має власник доступ до приміщення, після чого буде відправляти зашифроване повідомлення рідеру. Це і буде єдиною функцією рідера - інтерпретувати повідомлення, прийшло з телефону, і або відкривати замок, або не робити цього.

Документи з NFC містять як відкриту, так і закриту інформацію. Закрита область даних може бути доступна тільки для міліції та інших відомств, а відкрита область даних може бути зчитана телефоном з NFC модулем і використана третьою стороною, наприклад, для зберігання інформації про страховку і розміщення віртуальних ключів.

За допомогою смартфона з’явиться можливість використати мітку вбудовану в автомобіль, як ключ для доступу. Також стане легше витягати з автомобіля сервісну інформацію та інформацію про пробіг авто, витрати палива, ремонт та діагностику, а також використовувати різноманітні мультимедійні можливості в середині автомобіля.

NFC-клавіатура для смартфонів і планшетів: корпус клавіатури еластичний, а також водонепроникний. Його можна спокійно згортати, що дуже зручно. Для того, щоб підключити наш смартфон або планшет до клавіатури, потрібно встановити спеціальні драйвера, які незабаром з'являться в каталозі Android Market і App Store.

Впровадження NFC на транспорті. Багато жителів, незалежно від того, користуються вони громадським транспортом або ні, стають очевидцями довгих черг. За допомогою NFC абонент отримує додатковий додаток у свій телефон, використовуючи свій банківський рахунок він може здійснювати покупку транспортних квитків, минаючи черги і каси. Також можна завантажувати розклад, карти і схеми маршрутів.

Візитні картки можуть використовуватися для зберігання і передачі відомостей про компанію, посилання на її сайт, онлайнові ресурси партнерів та ін. При цьому власники «розумних» карток зможуть оновлювати інформацію, яка зберігається на них, за допомогою спеціального додатку.

Рисунок 1 – Візитка з вбудованим NFC

NFC в супермаркетах. Поруч з кожним продуктом буде розміщена NFC мітка, що містить інформацію про сам продукт і записує інформацію про нього на телефон покупця за допомогою спеціального додатку. Додаток дозволяє покупцеві отримати не тільки інформацію про вартість продукту, але і харчової цінності, отримати інформацію про найближчі магазини, в яких також є цей товар, розмістити своє замовлення в режимі онлайн. Така система дозволяє покупцям своєчасно оцінювати і контролювати власні витрати, а також виключає ймовірність помилок на касі, таких як, наприклад, повторне сканування продукту. До інших переваг належить можливість зв'язати карту лояльності клієнта з додатком - тепер покупцеві не доведеться турбуватися про отримання всіх знижок. Щоб стимулювати покупців користуватися NFC і інтерактивними додатками, магазин повинен мати безкоштовний Wi-Fi.

Технологію NFC доцільно впроваджувати в різних галузях телекомунікаційних систем. Вже на даному етапі розвитку технології має зміст її використовувати, удосконалюючи і шукаючи нові сфери застосування.

В майбутньому при збільшені практичного застосування NFC може проникнути в усі сфери нашого життя, часом навіть зовсім несподівані і можна буде швидше знайти способи усунення недоліків які існують зараз.

Література

1.Tesa. Технология NFC в электронных замках TESA. http://www.tesa.ru/news/132.

2.Мобильная лавка. Голышко, Александр. 07, 2011 г., Мобильные Телекоммуникации, стр. 26-31.

3.Потресов, Сергей. Билайн: Мобильный проездной. http://www.mobile-review.com/articles/2012/bee-nfc-metro.shtml.

4.Liou J.C. et al. A Sophisticated RFID Application on Multi-Factor Authentication //Information Technology: New Generations (ITNG), 2011 Eighth International Conference on. – IEEE, 2011. – С. 180–185.

Яскевич В.О.

Доцент кафедри Прикладнгого програмування

Державний університет телекомунікацій

м. Київ, Україна

АЛГОРИТМ ПРИСКОРЕНОГО МЕТОДУ МНОЖЕННЯ

Проведений аналіз завантаження ядер мультиядерного мікропроцесора (МП) побудований на основі використання теорії систем масового обслуговування (СМО) [1], а також аналіз взаємодії мультиядерних МП з пам'яттю [2] показав, що найприйнятніші імовірнісні співвідношення мають місце, коли інтенсивності узгоджені, тобто приблизно рівні. Це можна досягти, якщо всі команди по тривалості виконання будуть однаковими (тобто довгі операції типу множення і ділення матимуть тимчасові характеристики такі як і типові короткі – додавання і віднімання). Особливо це актуально при використанні мультиядеярності в процесорах цифрової обробки сигналів. Що вимагає використання операції «множення з накопиченням» (Multiply-Accumulate, MAC) (Y:=A*B+X).

Аналіз розглянутих алгоритмів множення показав, що:

Класичні методи множення найбільш тривалі;

Прискорені методи покращуюсь час виконання операції, але несуттєво;

Табличні методи є найбільш швидкими, але потребують надто великий обсяг табличної пам'яті.

Очевидно, що існують компромісні методи, які дають прийнятний час виконання при порівняно невеликому обсязі табличної пам'яті.

Пропонований метод заснований на використанні відомої формули, (1)

$$R = a \cdot b = \frac{1}{4}[(a+b)^2 - (a-b)^2], \quad (1)$$

де a, b - співмножники розрядності n,

R - результат множення

При цьому способі використовується таблиця квадратів чисел розрядності n + 1, що дає зменшення обсягу в порівнянні з попереднім (чисто табличним). Зменшення обсягу табличної пам'яті оцінюється значенням.

$$\frac{2^{2n}}{2^{n+1}} = 2^{n-1}, \qquad (2)$$

Таблиця 1 демонструє обсяг табличної пам’яті при множенні цілих чисел різного порядку.

Таблиця 1 Обсяг пам’яті

Метод	Формат			
	Тетрада	Байт	Слово	Подвійне слово
Табличний	2^8	2^{16}	2^{32}	2^{64}
За формулою	2^5	2^9	2^{17}	2^{33}

Якщо при цьому способі використовувати для додавання і віднімання зворотні коди, то вираз (1) перетвориться в наступний:

$$D = \frac{1}{4}\overline{\left[\overline{(a+b)^2} + \overline{(a+\bar{b})}^2\right]}, \quad (3)$$

де риса означає, що використовується зворотний код.

Необхідно відзначити, що при виконанні умови

$$a < b, \qquad (4)$$

Операція додавання виконується без появи одиниці циклічного переносу, що спрощує апаратну реалізацію помножувача. Якщо умова (4) не виконується, співмножники міняються місцями, що можна виконати легко. На рис. 1 представлена схема помножувача. Поділ на 4 можна здійснити зрушенням результату на 2 розряду вправо за один такт.

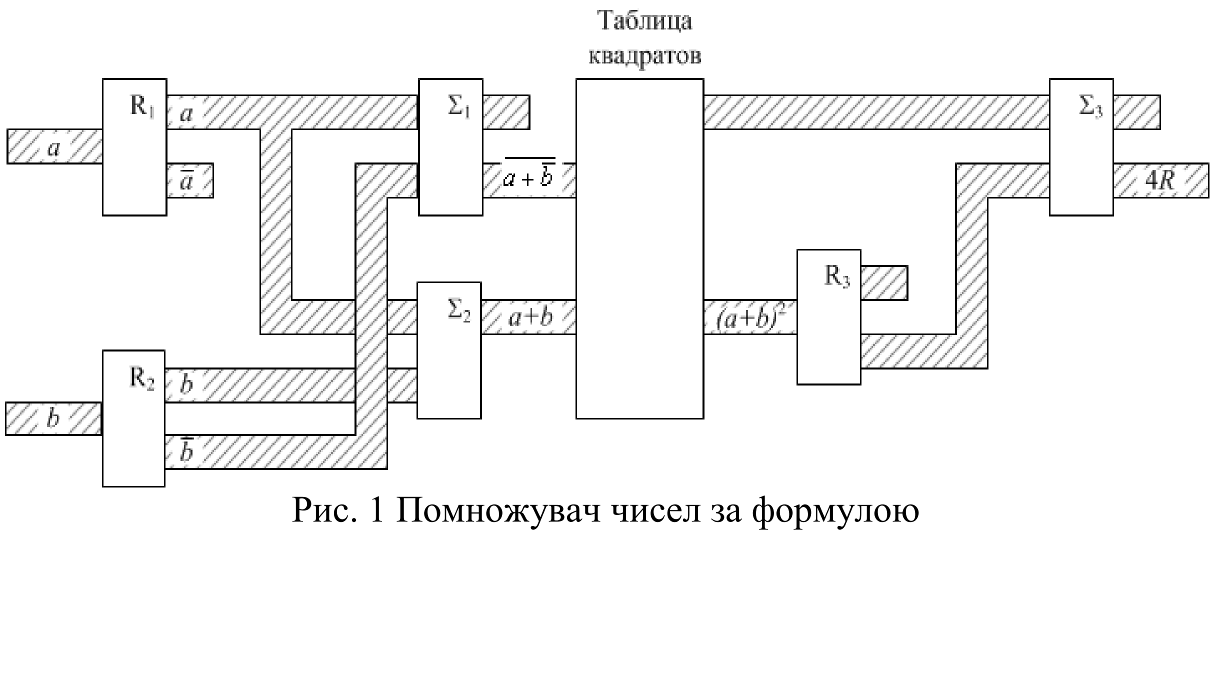


Рис. 1 Помножувач чисел за формулою

Література

1. Дробик О.В., Лобанов Л.П., Яскевич В.О. Распараллеливание потока команд в мультиядерных микропроцессорах // Системи управління, навігації та зв'язку, № 3 (27), 2013.

2. Яскевич В.О. Математические модели взаимодействия мультиядерных микропроцессоров с памятью // Системи управління, навігації та зв'язку, № 4 (28), 2013.

3. Дробик О.В., Лобанов Л.П., Яскевич В.О. Побудова цифрових схем на мультиплексорах // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк № 8 2012.

Зариленко Е.С.
Студент ІМДМ-51
Катков Ю. И.
доцент каф. Информационных технологий
Государственный университет телекоммуникаций
г. Киев, Украина

ОБЗОР СХЕМ УПРАВЛЕНИЯ МОЩНОСТЬЮ В LTE ДЛЯ ВОСХОДЯЩЕГО ПОТОКА

Целью этой статьи является описание новых способов управления мощности системы сотовой связи EUTRAN LTE, что является актуальной задачей построения безпроводових сетей.

Управление мощностью является важнейшей функцией радиосетей в системах сотовой связи. Эта статья, описывает управление мощностью в системе LTE для физического восходящего канала (Physical Uplink Shared Channel). Реализация LTE основана на схеме множественного доступа OFDM (Orthogonal Frequency Division Multiple Access) для нисходящего потока, и SC-FDMA (SingleCarrierFrequencyDivisionMultipleAccess) для восходящего. Исходя из того, что 3GPP LTE разработана с учетом коэффициента пере использования частот 1, существованием помех между сотами нельзя пренебречь. Каналы данных и управляющие каналы очень чувствительны к интерференции, поэтому должен быть обеспечен контроль управления мощностью в восходящем канале для минимизации этого эффекта.

В LTE для формулы контроля мощности восходящего канала стандартизировано два компонента: открытая петля (openloop) и закрытая петля (closedloop). В openlooppowercontrol (OLPC), мощность передачи устанавливается на пользовательском оборудовании (UE) используя параметры полученные от базовой станции. Closed loop предназначен улучшить производительность FPC, компенсируя быстрые вариации в канале. В closed loop power control (CLPC) базовая станция отправляет информацию для дальнейшей корректировки мощности передачи UE. Предполагается, что CLPC потребует высокую нагрузку при передаче, но в то же время обеспечит быстрый механизм компенсации интерференции. С другой стороны, OLPC обеспечивает более простую реализацию, но невозможность корректировать UE индивидуально.

Openloop предназначен для компенсации низких вариаций получаемого сигнала таких как затухание и ослабление сигнала за пределами прямой видимости. Closedloopпредназначен для дальнейшей корректировки мощности с целью оптимизировать производительность системы.

Различают:

1. Схему управления мощностью LTE UL, в которой устанавливается в UE мощность передачи P_{tx} для восходящегопотока. Затухание, измеряемое в UE основано на среднем значении принятых пилотных сигналов (RSRP). Этой информации достаточно чтобы позволить UE изначально установить мощность передачи. RSRP может измеряться как для одной антенны, так и для двух антенн. Это является конфигурационным параметром и передается в блоке системной информации.

2. Частичное управление мощностью (Fractional Power Control). Пороговое отношение сигнал/шум меняется для пользователей в зависимости от их положения внутри соты: чем ближе абонент к базовой станции, тем выше порог отношения сигнал/шум как критерий регулировки мощности. Следовательно, вблизи базовой станции абонентский терминал работает с более высоким отношением сигнал/шум, с более высокой скоростью кодирования и кратностью модуляции, а значит, с более высокой спектральной эффективностью.

Следует заметить, что работая с повышенной мощностью, UE справляется с внутрисистемной интерференцией – подавляет соканальные помехи, что критично в сетях с коэффициентом переиспользования частот 1. Кроме того, каждая базовая станция LTE контролирует уровень помех от соседних сот. Периодически, базовые станции обмениваются индикаторами перегрузки OI (OverloadIndicator), указывающем, в каком ресурсном блоке уровень помех превышает пороговое значение. Индикатор OI формируется по результатам измерения базовой станцией уровней помех и фонового шума для каждого частотного блока в соте. Параметры управления мощностью устанавливаются в зависимости от принятого OI: если для какого-либо блока указывается высокий уровень помех, то базовая станция передает команду снизить мощность UE, излучающего в данном ресурсном блоке (рис 1)

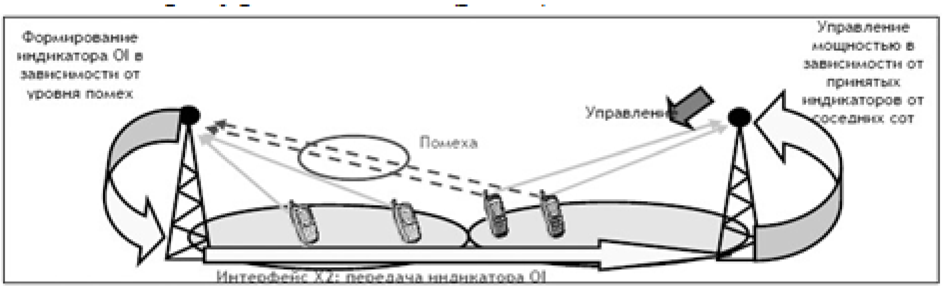


Рисунок 1 Управление мощностью соседней

CLOSED LOOP POWER CONTROL

1. Closed Loop PC Concept. В системе CLPC приемник оценивает соотношение сигнал/шум (SINR) принятого сигнала и сравнивает его с требуемым значением. Если полученный сигнал ниже заданного значения SINR, то Transmit Power Control (TPC) передает команду пользовательскому оборудованию увеличить мощность передатчика. Или наоборот уменьшить мощность передатчика.

В спецификации 3GPP определено два типа команд TPC:

Absolute: абонент применяет значение изменения полученное командой PC, используя начальную мощность OLPC как эталон.

Comulative: абонент использует последнее (недавнее) значение мощности.

2. CLPC постоянным SINR. Для того чтобы понять поведение CLPC, в принятом SINR исследуются closedloop и частичное управление мощностью. В традиционном CLPC значение SINR остается неизменным для всех абонентов. На рис. 3 показано отношение SINR при двух разных схемах управления мощностью. На графике видно, что не все абоненты способны достичь требуемого значения SINR из за максимального предела мощности. Эти абоненты передают сигнал уже на максимальной мощности и поэтому не могут ее увеличить.

Частичное управление мощностью позволяет пользователям с хорошими радио условиями (абоненты находятся близко к Базовой Станции) достичь высокого значения получаемого SINR. Результатом этого является высокая пропускная способность для пользователя, сохраняя при этом достаточную пропускную способность на краях соты. Тогда как CLPC устанавливает для всех абонентов равное значение получаемого SINR; это приводит к тому что абоненты с хорошими радио условиями, не могут получить высокий коэффициент SINR, что приводит к низкой средней пропускной способности. Следует отметить что CLPC, позволяет абонентам, находящимся на границах соты, получить более высокий SINR (рис 2)

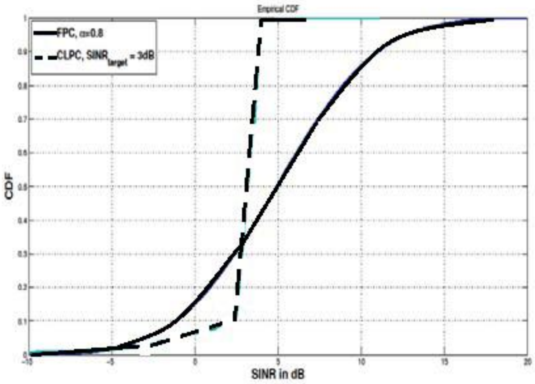


Рисунок 2. График принятого SINR для FPC используяа = 0.8 и CLPC используя $SINR_{target}$= 3 dB

Установки высокого значения SINR означает, что пользовательское устройство должно передавать сигнал с более высокой мощностью. В связи с ограничением мощности, некоторые пользователи не смогут достичь высокого коэффициента, что приведет к падению скорости на краях соты. Таким образом установки closedloop SINR это компромисс между средней пропускной способностью и границами соты.

Управление мощностью сигнала на восходящей линии в системе LTE является гибким, простым и надежным. Оно включает множество реализаций с различными целями, поддерживающими различные сценарии развертывания и сервисы.

Управление мощности функционирует с помощью двух механизмов – openloop и closedloop. Работа openloop основана на технике частичного управления мощности, которая предназначена для полной или частичной компенсации потерь при затухании сигнала.

Функция увеличения мощности частично компенсирует затухания в openloop. Это дает возможность сделать компромисс между пользователями, находящимися на краю соты с теми, кто находится непосредственно около базовой станции. Это имеет явные преимущества по сравнению с традиционной полной компенсацией в open и closedloop.

Алгоритмы, используемые для реализации closedloop, специфичны для каждого поставщика оборудования и все еще находятся в разработке.

Литература:

1.http://www.3gpp.org/Highlights/LTE/LTE.html.

2.3GPP TS 36.213 V9.1.0 , "E-UTRA Physicallayerprocedures".

3.3GPP TS 36.211 V8.8.0, "Evolved Universal Terrestrial Radio Access(EUTRA); Physical Channelsand Modulation".

4.R1-073036, "IntracellUplinkPowerControlfor E-UTRA - Evaluation of Fractiona lPath Loss Compensation"

5. A. Simonssonand A. Furuskar, "UplinkPowerControlin LTE Â– Overview and Performance", IEEE Transactionson communications,2008

6. StefanParkvallandDavidAstely, "The Evolutionof LTE towards IMT-Advanced"

Онищенко В.В.

Завідувач каф. Прикладного програмування

Шевченко С.М.

Доцент каф. Вищої математики

Державнийуніверситеттелекомунікацій

м. Київ, Україна

ОСВІТА В СУЧАСНОМУ СВІТІ-ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Сучасний світ сьогодні-світ інформаційних технологій, які стрімко змінюється. Обсяг інформації щороку зростає, з'являються нові технології та професії. Щоб бути успішним у сучасному динамічному середовищі, треба ефективно взаємодіяти з іншими людьми та постійно навчатися. Навчання впродовж всього життя—це гасло сьогодення.

Отже система освіти також має змінюватись. Завдання сучасної вищої освіти — сформувати навички успішної, соціальної адаптованоїлюдини, здатної до самоосвіти. На зміну традиційним методикам приходить концепція електронної освіти — процесу навчання і виховання за допомогою сучасних інформаційних технології.

Сучасна людина вже не уявляє свого життя без сучасних електронних пристроїв: телефону, смартфону, планшету, ноутбуку, компьютеру. Зрозуміло, що традиційні методи освіту не можуть забезпечити потреби часу. І тут постає проблема оновлення матеріально-технічної бази навчального закладу: як встигнути за змінами часу? Відомо, що апаратне та програмне забезпечення удосконалюється та оновлюється практично щодня. І тут на допомогу приходять такі технології як веб, віртуальні та хмарні. Вони радикальним чином змінюють навчальні заклади, навчально-виховний процес, природу освіти та її доступність. Як показує досвід розвинених зарубіжних країн, відмінним рішенням вищеописаних проблем є розбудова інноваційної освіти на засадах впровадження «хмарних технологій» у навчально-виховний процес.

У поєднанні можливостей новітніх гаджетів та ресурсів мережі Інтернет створюються умови для розробки доступного навчального середовища, при цьому доступ не обмежується до потрібних даних.

Використання такого навчального середовища, яке було б насичене різноманітними електронними ресурсами, значно підвищить інтерес студентів до навчання в цілому, створить умови для розвитку, а також активізує пізнавальну діяльність студентів. Все це можливо за умови використання сучасних хмарних технологій.

Єдиний інформаційний простір в освіті планується побудувати, з використанням хмарних технології, які надає компанія Microsoft Україна. Загальноосвітні навчальні заклади для впровадження нових форм навчального процесу, безпечного зберігання даних і електронного обміну даними будуть застосовувати хмарний сервіс Office 365.

Хмарний сервіс Office 365, базовий тарифний план якого доступний для освітніх установ безкоштовно, вже використовується в українських школах - всього відкрито понад 237 тис. облікових записів.

Хмарні технології мають ряд переваг: не потрібні потужні комп'ютери, менше витрат на закупівлю програмного забезпечення і його систематичне оновлення, оскільки все знаходиться у хмарі; відсутність піратства, необмежений обсяг збереження даних, доступність з різних пристроїв і відсутня прив'язка до робочого місця, забезпечення захисту даних від втрат та виконання багатьох видів навчальної діяльності, контролю і оцінювання, тестування он-лайн, відкритості освітнього середовища, економія коштів на утримання технічних фахівців.

При всіх перевагах сучасних засобів навчання вони не повинні замінити викладача з його емоціями, жартами, вмінням пояснити. Потрібне розумне поєднання сучасних та традеційних методик освіти. Тільки за таких умов можна створити якісну та професійну освіту.

Література:

1. Литвинова С. Г. Методика використання технологій віртуального класу вчителем в організації індивідуального навчання учнів : автореф. дис. на здобуття наук. ступеня канд. пед. наук : спец. 13.00.10 "Інформаційно-комунікаційні технології в освіті" / С. Г. Литвинова. - К, 2011. - 22 с.
2. Морзе Н.В. Як навчати вчителів, щоб комп’ютерні технології перестали бути дивом у навчанні/ Н.В. Морзе// Комп’ютер у школі та сім’ї. - №6 (86). - 2010. - С. 10-14.
3. Морозов А. Школьники уходят в облака/ А Морозов/ [Електронний ресурс]. -http://www.ng.ru/education/2011-09-06/8_shkolniki.html. - Назва з екрану.
4. Облачные вычисления. [Електронний ресурс]. - Режим доступу: http://habrahabr.ru/blogs/cloud_computing/111274 . - Назва з екрану.
5. Рождественська Л.В. Дневник конференции. 10 шагов информатизации: призрак виртуальной учитель ской [Електронний ресурс]. http:// edugalaxy.intel.ru/index.php?automodule=blog&blogid=8&showentry=3664- Назва з екрану.

Даков С.Ю.
Аспирант кафедры Телекоммуникаций
Национальный Авиационный Университет
г. Киев, Украина

УВИЛИЧЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ РАДИОКАНАЛА ДЛЯ СЕТЕЙ LTE ПРИ ПОМОЩИ АРХИВАЦИИ ДАННЫХ

С момента развития мобильных сетей LTE 4 поколения, мы имеем большое количества технологий, способных сделать работу радиоканалов, максимально функциональной. В теории так оно и есть, более 100 мб. [3] пропускной способности, методы пространственного кодирования, мультиплексирования с ортогональным частотным разделением.

Но на практике все по-другому, не учитывается 25% накладных расходов канала, условия максимальной загрузки (Например, большого скопления людей, автомобильные пробки, выставки, учебные заведения…), к тому же нужно принимать во внимание такие нюансы, как плохие условия покрытия, плохие погодные условия…

Постоянные обрывы и замедление приема съделают работу с сетью невыносимой и сложной. В таких условиях возникнет, «негативная ассоциация». Которая приведет к торможению развития и увеличения пользователей в таких условия будет невозможно, из за чего оператор задумается, стоит увеличивать зону покрытия или расходы на развития структуры. Для этого нужно сделать так чтобы для оператора и пользователя, пропускная способность была максимально эффективна.

К тому же основное направления развития интернета это безлимитный вариант, что касается проводного интернета, эта вершина уже взята и путь развития ведет в сторону увеличения скорости скачивания. Именно такой сценарий должны иметь и беспроводные технологии.

В условиях работы пропускного канала мы можем обозначить два основных номинала: максимальная пропускная способность радиоволны и трафика пройденного по этому радиоканалу. Что касается радиоволны, этот номинал является статическим и его увеличения возможно только при внедрении нового оборудования или модернизации старого. Трафик – эта величина динамическая и при помощи различных методов объем информации пропущенной через радиоканал, можно увеличить.

Для расширения трафика можно использовать метод сжатия

При использовании сжатия нужно понимать, что метод имеет преимущества, так и недостатки.

Под преимуществом подразумеваем, что объем информации пропущенный через компрессор будет в большем объеме. Это значит, что пользователь получит файл первоначального объема, но нагрузка на радиоканал будет меньше на процент который компрессор смог сжать.

$$k = \frac{S_o}{S_c}$$

k – Коэффициент сжатия

S_o – Объем исходных данных

S_c – Объем сжатых данных

Если So>Sc тогда процедура имеет смысл и сжатие можно производить перед отправкой. В других случаях файл будет передан по радиоканалу в исходном виде, возможно файл уже архивирован или его компрессия невозможна.

Рисунок 1 Применения компрессора, для передачи данных по сети

Так же нужно понимать, что сжатия зависит от типа данных, если мы берем контент, то степень сжатия будет велика, к тому его можно сжимать методом сжатия с потерями, а это значит что коэффициент коэффициент сжатия будет довольно большой [1 ст.246]. Если объект сжатия документ, в котором содержится в основном текст, такова типа объект имеет так же большую степень сжатия [1 ст.246]. Если архивируется изображения, метод архивации будет другой и коэффициент сжатия будет значительно меньше [1 ст.272], нужно учитывать что изображения отличаются сами по себе и метод сжатия для них другой [1 ст.273]. Ну для сжатия видеоданных имеется третий вид компрессора [1 ст.338] к тому же архивация видео – данных имеет особое значения, т.к. это самые тяжелые файлы и сжатия таких файлов самая значительная [2].

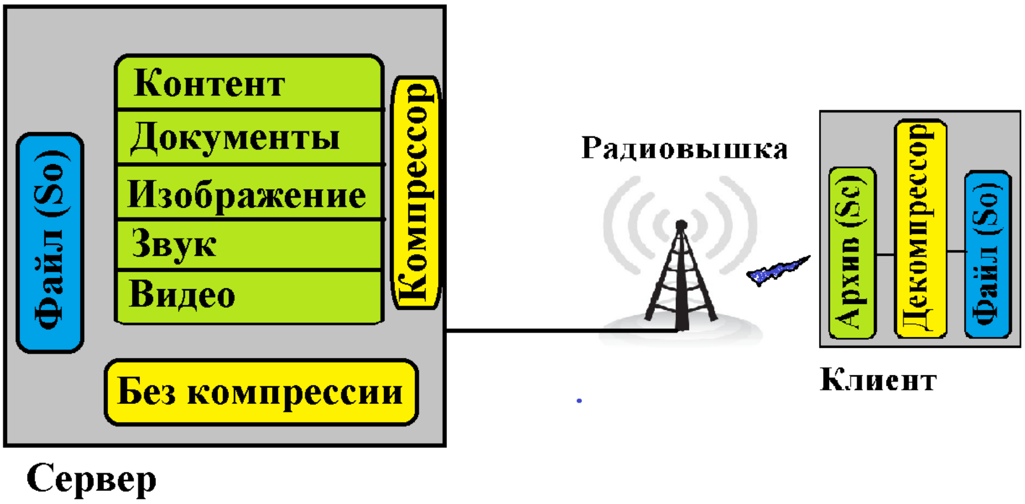


Рисунок 2 Сортировка файлов по типу, для определения необходимого компрессора

Ну и в зависимости от типа файла, после сортировки, мы пропускаем через соответствующий тип кодека после чего передаем конечному пользователю по радиоканалу и после декомпрессии пользователь работает над полученным файлом который отображается ему в исходном виде, что касается контента, пользователь получает информацию в зависимости от настроек браузера.

Что касается упаковки и распаковки архива, все манипуляции проводятся на сервере и непосредственно на устройстве клиента, по радиоканалу будет передаваться только архив. И благодаря архивации мы получим возможность передать большее количество информации для пользователей по выделенному радиоканалу.

Имеются недостатки компрессии, нужно учитывать, что компрессия и декомпрессия файла займет определенное время, и во многих случаях архивировать данные не будет смысла. Например, если файл слишком маленький и время на его упаковку и распаковку займет больше чем передать его в исходном виде, некоторые файлы вообще не поддаются архивации, и передача их осуществляется в исходном виде.

Литература:

1. Д. Сэломон. Сжатие данных, изображения и звука. — М.: Техносфера, 2004. — С. 368.

2. Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. — Диалог-МИФИ, 2002. — С. 384

3. А.Л.Гельгор, Е.А.Попов. Технология LTE мобильной передачи данных. — Издательство политехнического университета, 2011 — С 205

Савченко А.І.
Студентка каф.Телекомунікаційних систем
Корольов В.І.
Студент каф.Телекомунікаційних систем
Національний авіаційний університет
м. Київ, Україна

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ЯДРА МЕРЕЖІ LTE

Мережа LTE включає в себе мережу радіодоступу (Evolved Universal Terrestrial Radio Access Network, E-UTRAN) та вдосконалене пакетне ядро (EvolvedPacketCore, EPC) (рис. 1).Ядро мережі об'єднує окремі мережі доступу (E-UTRAN) та виконує функції транзиту трафіка між ними по високошвидкісним каналам. Також до ядра мережі під'єднані магістральні канали зв'язку. EvolvedPacketCore – це еволюція пакетно-канальної архітектури мереж GPRS/UMTS.

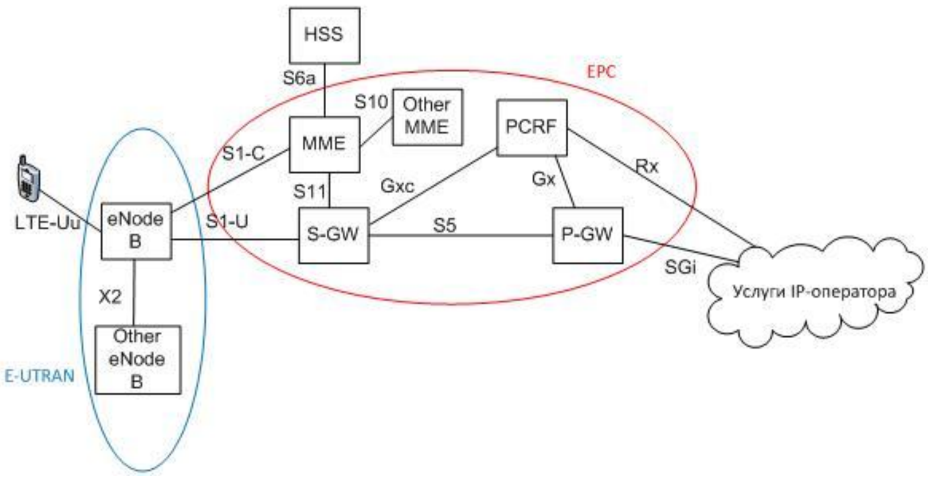


Рисунок 1. Структурамережі LTE

Evolved Packet Core складається з таких компонентів: HSS (Home Subscriber Server), MME (Mobility Management Entity), S-GW (Serving Gateway), P-GW (PDN Gateway), PCRF (Policyand Charging Rules Function).

HSS (Home Subscriber Server) – цебазаданих, в якій зберігається абонентська інформація. Також HSS забезпечує підтримку в мобільному управлінні, налаштування дзвінків та сесій, автентифікацію користувача та авторизацію доступу. HSS базуєтьсянаpre-3GPP (3rd Generation Partnership Project) Release 4 - Home Location Register (HLR) та Authentication Centre (AuC).

MME (Mobility Management Entity) – модуль, який взаємодіє з системою управління та забезпечує мобільність і захист доступу до E-UTRAN. Модуль MME відповідає затрекінг та пейджинг абонента.

S-GW (Serving Gateway) – шлюз, який служить для транспорту IP-трафіка між мобільною станцією (UE – User Equipment) та мережею пакетних даних. Serving Gateway є точкою взаємодії між мережею радіодоступу (E-UTRAN) та пакетним ядром (Evolved Packet Core). Із назви шлюза видно, що S-GW обслуговує мобільну станцію, виконуючи маршрутизацію вхідних та вихідних IP-пакетів.

P-GW (PDN Gateway) – шлюз, який є точкою взаємодії між EPC та мережами пакетних даних, які називаються PDN (Packet Data Network). PDN шлюз виконує маршрутизацію пакетів від /до мереж пакетних даних.

PCRF (Policyand Charging Rules Function) – пристрої, які висліджують потік наданих послуг й забезпечують тарифну політику.

Література:

1. The Evolved Packet Core [Електронний ресурс]. – Режим доступу: URL: http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

2. Принципыпостроения и функционированиясетей LTE [Електронний ресурс]. – Режим доступу: URL: http://1234g.ru/4g/lte/printsip-raboty-seti-lte/printsipy-postroeniya-i-funktsionirovaniya-setej-lte

3. Introductionto LTE [Електронний ресурс]. – Режим доступу: URL: http://www.3glteinfo.com/introduction-to-lte/#disqus_thread

Домрачева Е.А.
Аспирант каф. Телекоммуникационных систем
Краснянский М.С.
Студент ФТК группа ТСД-41
Государственный университет телекоммуникаций
г. Киев, Украина

ИССЛЕДОВАНИЕ ПОМЕХОЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХСИСТЕМ

Помехозащищенность характеризуется потерей информации под влиянием помех. Из теории связи известно, что существуют две основные причины снижения достоверности передачи. Этоснижение отношениясигнал/шум (S/N) и искажениесигнала.

Из теории передачи аналоговых сигналов известно, что одним из критериев качества сигнала является отношение средней мощности сигнала (S) к средней мощности шума (N). В цифровых системах связи чаще используется нормированная версия S/N, обозначается как E_b/N_0 [1]

где E_b-энергия, расходуемая для передачи одного бита информационного потока.

N_0 - это спектральная плотность мощности шума.

Гауссово распределение часто используется как модель шума в системе, даже если отдельны еслучайные процессы будут иметь негауссово распределение, распределение вероятностей совокупности многих таких процессов будет стремиться к гауссовому распределению. [2]

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(x-\mu)^2/2\sigma^2} \qquad (1)$$

где x -случайный сигнал;

μ-сигнал вканалесвязи;

$\sigma^2 = \frac{N_0}{2}$-дисперсия.

Вероятность$P(x > x_0) = \int_{x_0}^{\infty} f_X(x) = Q(\frac{x_0 - \mu}{\sigma}) = \frac{1}{2} \mathrm{erfc}(\frac{x_0 - \mu}{\sqrt{2\pi}\sigma})$

где$Q(x) = \int_{x}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right)$ du-гауссов интеграл ошибки.

Для BASK, где два сигнала являются одномерными и их геометрическое представление определяется одномерными векторами $S_1 = \sqrt{E_b}$,$S_2 = -\sqrt{E_b}$, то

вероятность ошибки можно выразить через расстояние между двумя сигнальными точками.

Два сигналанаходятсяна расстоянии$d_{12} = 2\sqrt{E_b}$, откуда $E_b = \frac{1}{4} d_{12}^2$.

Получим

$$P_b = Q\left(\sqrt{\frac{d_{12}^2}{2N_0}}\right) = Q(\sqrt{\frac{2E_b}{N_0}}). \qquad (2)$$

В системес двоичной фазовой манипуляцией (BPSK) расстоянием между сигналами $d_{12} = 2\sqrt{E_b}$, следовательно вероятность ошибки будет:

$$P(0/1) = P(1/0) = P\left(x > \sqrt{E_b}\right) = Q\left(\frac{\sqrt{E_b}}{\sigma}\right) = Q\left(\frac{\sqrt{E_b}}{\sqrt{\frac{N_0}{2}}}\right) = Q\left(\sqrt{{}^{2E_b}/_{N_0}}\right) (3)$$

DPSK (некогерентное детектирование)[3]

$$P_{DPSK\,n} = \frac{1}{2} e^{-E_b/N_0} \qquad (4)$$

DPSK(когерентное детектирование)

$$P_{DPSKk} = 2Q\left(\sqrt{{}^{2E_b}/_{N_0}}\right)[1 - Q(\sqrt{{}^{2E_b}/_{N_0}})] \qquad (5)$$

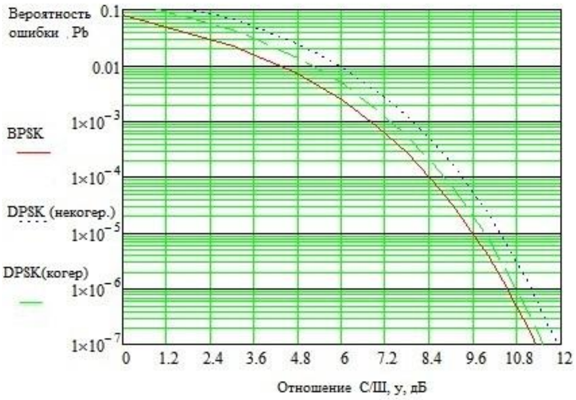


Рисунок 1 Вероятность ошибки BPSK и DPSK

Вслучае PSK модуляции, вероятность ошибки преимущественн случайный выбор одной из двух сигнальных точек, примыкающих к передаваемой сигнальной точке. Для M>2 ($M = 2^k$) с когерентным обнаружением можно выразить (для больших отношений $\frac{E_b}{N_0}$) [1]

$$P_{MPSK} = 2Q\left(\sqrt{\frac{2E_s}{N_0}}\sin\frac{\pi}{M}\right) \qquad (6)$$

где $E_s = E_b(\log_2 M)$- энергия, приходящаяся на символ.

Для $DMPSK$ (некогерентного детектирования) используется следующаяформула

$$P_{DMPSK} = 2Q\left(\sqrt{\frac{2E_s}{N_0}}\sin\frac{\pi}{\sqrt{2}M}\right) \qquad (7)$$

При ортогональной частотной модуляции FSK, в которой расстояние между сигналами $d = \sqrt{2E_b}$ используются формула для когерентного детектирования [2]

$$P_{FSKk} = Q\left(\sqrt{d^2/2N_0}\right) = Q\left(\sqrt{\left(\sqrt{2E_b}\right)^2/2N_0}\right) = Q\left(\sqrt{E_b/N_0}\right) \qquad (8)$$

и некогерентного детектирования

$$P_{FSKn} = \frac{1}{2}\exp\left(-\frac{1}{2}\frac{E_b}{N_0}\right) \qquad (9)$$

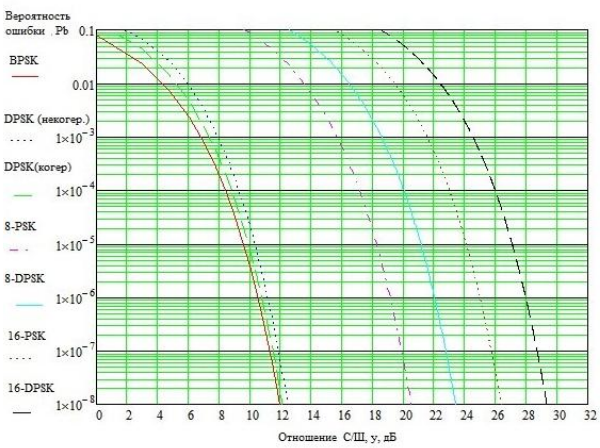


Рисунок 2 Сравнение помехоустойчивости приема MPSK и DMPSK

Ортогональная MFSK (когерентное детектирование)

$$P_s(M) \le (M-1)Q\left(\sqrt{E_s/N_0}\right) \qquad (10)$$

ОртогональнаяMFSK(некогерентного детектирования)

$$P_s = \frac{1}{M}\exp(-E_s/N_0)\sum_{j=2}^{M}(-1)^j\frac{M!}{j!(V-j)!}exp\left(E_s/jN_0\right) \qquad (11)$$

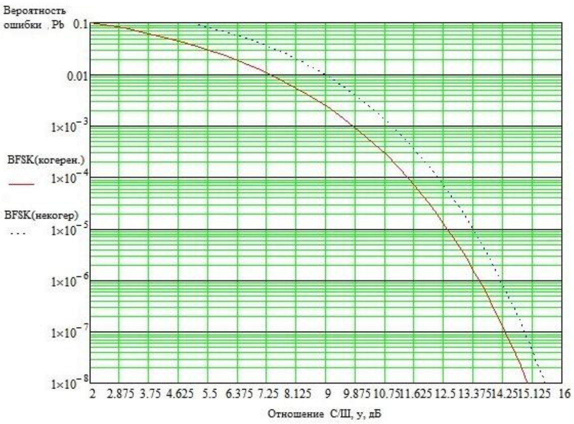


Рисунок 3 Зависимость вероятности ошибки от E_b/N_0 для BFSK для когерентного и некогерентногодетектирования

Для QAM с использованием кода Грея (два последовательных кода отличаются значением только одного бита) применяют формулу(результат точный при $M = 2^k$,когда k-парное.) [4]

$$P_{QAM} \le 1 - \left[1 - 2Q\left(\sqrt{\left(\frac{3E_{cp}}{(M-1)N_0}\right)}\right)\right]^2 \le 4Q\left(\sqrt{\frac{3kE_{bcp}}{(M-1)N_0}}\right) \qquad (12)$$

где $E_{cp} = \frac{1}{6}(M^2-1)d^2E_b$-средняя энергия сигнала.

$\frac{E_{bcp}}{N_0}$- средней отношение сигнал /шум набит.

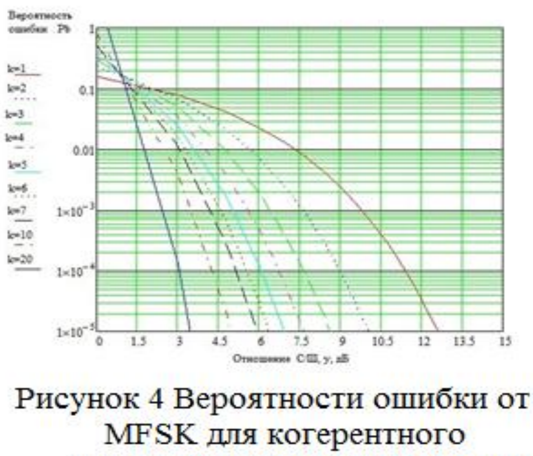


Рисунок 4 Вероятности ошибки от для MFSK для когерентного детектирования при различных значения $M=2^k$

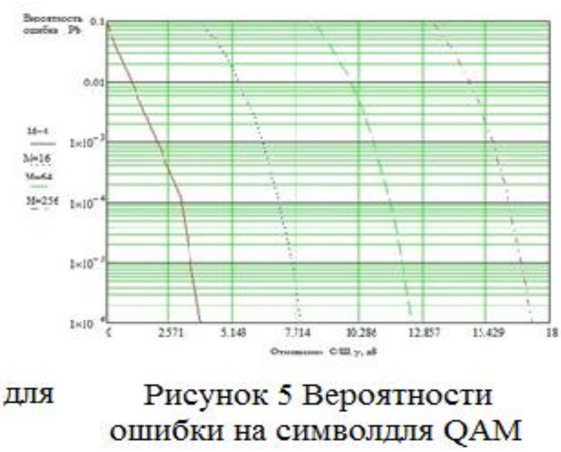


Рисунок 5 Вероятности ошибки на символдля QAM

Из сравнительного анализа можно сделать вывод, что при передаче сигналов наиболее перспективным видом модуляции является квадратура-амплитудная манипуляция QAM-4 и многочастотная манипуляция MFSK (для k> 20). При одинаковой величине ошибки этим модуляциям нужно меньшее значение отношения E_b/N_0. Единственный недостаток MFSK - высокая точность настройки и стабильность частоты, которые требуются от аппаратуры, в MFSK могут работать только современные радиостанции.

Если сравнить MPSK и MFSK, видно что с увеличением равновероятных символов M в MPSK помехозащищенность падает, а в MFSK наоборот увеличивается.

Литература:

1.Банкет В.Л.,Дорофеев В.М. Цифровые методы в спутниковой связи.– М.:Радио и связь, 1988.

2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. / Б Скляр. Изд.2-е, испр. :Пер. с англ.-М.: Издательский дом «Вильямс», 2007.- 1104 с.

3.Сотовые сети радиосвязи с подвижными объектами: учеб. пособ. /Сукачев Э.А. – [3-е изд., перераб. и дополн.]. – Одесса: ОНАС им. А.С. Попова, 2013.

4. Прокис, Дж. Цифровая связь. / Дж Прокис . - М.: Радио и связь, 2000. - 800 с.

Коник Р. С.
Аспірант каф. Прикладного програмування
Тихонов Є. С.
Аспірант каф.Прикладного програмування
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ХМАРНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Впровадження хмарних сервісів в український малий і середній бізнес дозволить не тільки модернізувати його діяльність, але і підвищити конкурентоспроможність з іноземними компаніями. Що в умовах вступу до ЄС є актуальним завданням.

Український ринок «хмар» стартував відносно недавно - в 2005-2006 роках. Тому Україна у світовому контексті - ще займає досить малу частку ринку. При цьому аналітики прогнозують на найближчі 3-4 роки - виключно позитивне зростання даного ринку. Прогноз на 2016 рік - 0,2 - 0,5 млрд. доларів. При цьому частка України у світі не перевищить 0,4 - 1%.

Ринок віртуалізації продовжує розширюватися, росте число замовників. Віртуалізація допомагає багатьом компаніям зробити перший крок у бік інноваційних хмарних обчислень, які не тільки здешевлюють вартість використання інформаційних технологій, але і роблять їх доступними практично в будь-якому місці і в будь-який час, підвищуючи тим самим мобільність.

В українській підприємницькій практиці на аутсорсинг найчастіше передаються такі функції, як ведення бухгалтерського обліку, забезпечення функціонування офісу, перекладацькі послуги, підтримка роботи комп'ютерної мережі та інформаційної інфраструктури, рекламні послуги, забезпечення безпеки.

Перед великою частиною організацій малого та середнього бізнесу, що активно розвиваються і швидко зростають сьогодні стоїть завдання управління своїм розвитком. Керівники усвідомлюють, що їм вкрай необхідна корпоративна пошта і свій сайт, загальні календарі і довідник співробітників і доступ до всього цього повинен бути з будь-якого мобільного пристрою в будь-якій точці світу. Так на допомогу їм приходять хмарні технології.

Дані переваги економічно вигідні для підприємств, так як дозволяють скоротити витрати, вивільнити грошові кошти для використання їх в інших сферах діяльності. Основні переваги даної технології полягають у наступному для впровадження в організації:доступність - «хмари» доступні всім, з будь-якої точки, де є інтернет, з будь-якого комп'ютера, де є браузер; низька вартість - основні фактори, які знизили вартість використання хмар, наступні:

- зниження витрат на обслуговування віртуальної інфраструктури;
- оплата фактичного використання ресурсів;

гнучкість - необмеженість обчислювальних ресурсів (пам'ять, процесор, диски), за рахунок використання систем віртуалізації, процес масштабування; надійність - надійність «хмар», особливо що знаходяться в спеціально обладнаних ЦОД;

безпека;

швидке впровадження, оскільки не потрібно чекати поки встановлять все необхідне обладнання і ПЗ на комп'ютери підприємства.

На жаль, як і всі технології ця теж недосконала. У неї теж є ряд недоліків:необхідність постійного стабільного з'єднання з мережею;

програмне забезпечення - є обмеження по ПЗ, яке можна розгортати на «хмарах» і надавати його користувачеві;

конфіденційність - конфіденційність даних які зберігаються на публічних «хмарах» в даний час викликає багато суперечок, але в більшості випадків експерти сходяться на тому, що не рекомендується зберігати найбільш цінні для компанії документи в публічній «хмарі», так як в даний час немає технології, яка б гарантувала 100% конфіденційність збережених даних.

неможливість відновлення інформації яка знаходиться в «хмарі»;

інші проблеми, які в найближчій перспективі, швидше за все, будуть усунуті або зведені до мінімуму.

Крім недоліків властивих самій технології існує ряд причин, які заважають розвитку «хмар» на українському ринку. Їх можна поділити на дві логічні групи: об'єктивні і суб'єктивні. До першої категорії належить недостатній розвиток послуг широкосмугового доступу в Інтернет. З даної проблеми випливає ще одна, взаємопов'язана з нею, це недостатньо розвинена інфраструктура, яка зв'язує центр і регіони. До суб'єктивних причин можна віднести наступні:

уразливість в області інформаційної безпеки. Побоювання небезпідставні;

недостатня зрілість бізнес-процесів IT та телеком-провайдерів. У підсумку впровадження «хмар» може виявитися дорожчим будівництва власної інфраструктури або покупки коробкових рішень;

обмеженість доопрацювання та інтеграції додатків. Дійсно, сьогодні великим питанням залишається, наприклад, можливість інтеграції існуючої інфраструктури і «хмарних» обчислень, сумісність «хмар» різних провайдерів;

відсутність довіри до компаній, що надають сервіси. Для появи її компаніям необхідно показати, що вони здатні підтримувати той рівень конфіденційності, цілісності та доступності даних, який забезпечують самі компанії. Дана умова важлива для компаній так як вони віддають свою найбільшу цінність - комерційну таємницю в чужі руки.

відсутність стандартизації послуг. На сьогодні пропозиції постачальників навіть найпростіших сервісів практично не стандартизовані. Але саме через стандартизації з'являється економічна вигода для як постачальника «хмарних» IT-сервісів, так і для споживача. Відсутність стандартів ускладнює конкуренцію між провайдерами і не дозволяє їм активно розвиватися, ринок таких послуг стає непрозорим, а значить неминуче більш дорогим та інші.

Враховуючи перераховані проблеми в найближчій перспективі у «хмарних обчислень» в Україні є два драйвери.

Перший - SaaS. Додаток як сервіс - самий високорівневий варіант «хмарних» продуктів. Він має на увазі, що користувач має доступ тільки до налаштування свого аккаунта в деякому додатку про все інше піклується постачальник. Основна перевага моделі SaaS для споживача полягає у відсутності витрат, пов'язаних з установкою, оновленням і підтримкою працездатності обладнання і працюючого на ньому програмного забезпечення. Провайдери даної послуги найбільш розвинені, питання із захистом інформації практично вирішені. Більше того, наприклад, у малих підприємств (вони і будуть головними споживачами SaaS) немає вибору - користуватися, наприклад, «хмарною» бухгалтерією в рази дешевше.

Світле майбутнє SaaS підтверджують вже досягнуті результати. У 2014-му приріст виручки постачальників SaaS в порівнянні з 2013-м значний. Наприклад, «SoftLine» додала 800%, «МойСклад» - 200%. Вони, звичайно, росли майже з нуля.

Нарешті, другий драйвер - держава. Електронний уряд і держпослуги, міжвідомчий документообіг - все це точки росту для провайдерів «хмарних» сервісів.

Неможливо не визнати - нас чекає не безхмарне, а саме «хмарне» майбутнє, в якому головну роль відіграватимуть «хмарні обчислення». «Хмарні технології» це не майбутнє, це – сьогодення.

Література:

1. Джордж Риз/ перевод. О. Кокорева/ Облачные Вычисления/ БХВ-Петербург / 2011г.
2. Макаров С.В. Социально-экономические аспекты облачных вычислений //Монография - М.: ЦЭМИ РАН, 2010г.
3. Черняк Л. Интеграция - основа облака// Открытые системы. СУБД 16 сентября 2011 г. http://ru.wikipedia.org/wiki

Частокол М.М.
Студент кафедри Систем захисту інформації
Фузік К.М.
Студент кафедри Систем захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ ЗАХИСТУ ТЕЛЕФОННИХ ЛІНІЙ

Незважаючи на бурхливий розвиток комп'ютерних мереж і медіатехнологій, передавання голосових повідомлень через телефонні апарати продовжує домінувати у загальному трафіку сучасної телекомунікації. Це зумовлено передовсім простотою та доступністю телефонного зв'язку. Разом з тим, телефоний зв'язок є одним з найбільш незахищених у сенсі інформаційної безпеки. Під час захисту телефонних ліній, як каналів просочування інформації, необхідно звернути увагу на такі аспекти: 1) навіть при поставленій слухавці телефонні апарати можуть бути використані для підслуховування розмов (акустичної мовної інформації) в приміщеннях, де вони знаходяться; 2) телефонні лінії можна використовувати для передачі перехопленої інформації, а також для живлення акустичних закладок, що встановленні в приміщеннях; 3) також існують наступні методи для перехоплення телефонних розмов, а саме: шляхом гальванічного підключення, за допомогою диктофонів, через індукційний датчик підключення до телефонної лінії, закладок (ретрансляторів) чи за допомогою інших засобів несанкціонованого одержання інформації.

Щоб запобігти несанкціонованого використання телефонних ліній (ТЛ) необхідно використовувати наступні технічні способи (ТС):

застосування пасивних ТС захисту: обриву ліній, лічильників часу розмови, сигналізаторів підключення, у тому числі по міжміському зв'язку;

застосування активних ТС захисту: пристрої кодування доступу до телефонних ліній, пристрої захисту від паралельного підключення, пристрої активного маскування інформації і ін.;

обмеження небезпечних сигналів;

фільтрування небезпечних сигналів;

відключення джерел небезпечних сигналів;

Фундаментальною базою обмеження небезпечних сигналів є нелінійні властивості напівпровідникових елементів, головним чином діоди. Діодні обмежувачі включаються послідовно в лінію дзвінка. Для захисту телефонних апаратів від «високочастотного нав'язування» використовується фільтрація небезпечних сигналів.

Конденсатор є найпростішим фільтром, що встановлюється у ланцюг дзвінка телефонних апаратів з електромеханічним дзвінком, а також у мікрофонний ланцюг всіх апаратів.

Одним з найефективніших методів захисту інформації, що поєднують фільтр та обмежувач, є відключення телефонних апаратів від лінії в приміщенні під час конфіденційних розмов.

Для даного методу захисту слід встановити в телефонній лінії спеціальний пристрій захисту, який відключає телефонний апарат від лінії, при встановленій телефонній слухавці, без участі оператора, тобто автоматично.

Виявлення атак і контроль стану телефонних ліній проводиться за допомогою апаратури контролю ліній зв'язку:

індикаторних пристроїв;

кабельних локаторів (пристроїв, що використовують принципи нелінійної локації і рефлекторметрів), аналізаторів дротяних ліній;

універсальних комплексів контролю.

Можна ефективно знаходити наявність радіо заставних пристроїв з безпосереднім підключенням телефонної лінії при застосуванні стандартних аналізаторів телефонних ліній, але при цьому виникає єдина незручність – необхідність попереднього знеструмлення лінії, що перевіряється.

Щоб визначити відстань до підозрілого місця в телефонній лінії використовують «кабельний радар», тобто рефлектометр. При застосуванні універсальних комплексів контроль здійснюється зі зміною рівня сигналу на вході приймача контролю у момент підняття слухавки. Також захист мовної інформації здійснюється в IP-телефонії.

В IP-телефонії існують два основні способи передачі пакетів з мовною інформацією по мережі: через мережу Інтернет і через корпоративні мережі + виділені канали. Між цими способами мало відмінностей, проте в іншому випадку гарантується краща якість звуку і невелика фіксована затримка пакетів мовної інформації при їх передачі по IP-мережі.

Для захисту мовної інформації, що передається через IP-мережі, використовуються криптографічні алгоритми шифрування початкових повідомлень і пакетів, які в свою чергу дозволяють забезпечити гарантовану стійкість IP-телефонії. Існують ефективні криптографічні алгоритми, які при використанні 256-бітових секретних і 1024-бітових відкритих ключів шифрування практично роблять неможливим дешифровку мовного пакету.

Для забезпечення прийнятної якості звуку на приймальній стороні при передачі мовних пакетів в IP-мережі, затримка в їх доставці (від приймальної сторони) не повинна перевищувати 250 мс. Для зменшення затримки цифровий мовний сигнал стискають, а потім зашифровують з використанням алгоритмів потокового шифрування і протоколів передачі в IP-мережі.

Для запобігання обміну криптографічними ключами шифрування між абонентами мережі, що також є проблемою захищеної IP-телефонії, застосовують криптографічні протоколи з відкритим ключем із використанням протоколу Діффі-Хеллмана, який не дає змогу при перехопленні розмови отримати будь-яку корисну інформацію про ключі, але при цьому сторони мають змогу обмінятися інформацією для формування загального ключа, який застосовується для зашифровки і розшифровки мовного потоку. Для того, щоб звести до мінімуму можливість перехоплення ключів шифрування, використовуються різні технології аутентифікації абонентів і ключів.

Протокол стиснення мовного потоку, так як і всі криптографічні протоколи, вибираються програмами IP-телефонії динамічно і непомітно для користувача, надаючи йому природний інтерфейс, подібний до звичайного телефону.

Реалізація ефективних криптографічних алгоритмів і забезпечення якості звуку вимагають значних обчислювальних ресурсів, в більшості випадків ці вимоги виконуються при використанні достатньо могутніх і продуктивних комп'ютерів, які не вміщаються в корпусі телефонного апарату, але недоліком є міжкомп'ютерний обмін мовною інформацією,який не завжди влаштовує користувачів IP-телефонії. Набагато зручніше використовувати невеликий, а краще мобільний апарат IP-телефонії, який забезпечує стійкість шифрування мовного потоку значно нижче, ніж комп'ютерні системи IP-телефонії. В таких телефонних апаратах для стиснення мовного сигналу використовується алгоритм GSM, а шифрування здійснюється по протоколу Wireless Transport Layer Security (WTLS), який є частиною протоколу Wireless Application Protocol (WAP), реалізованого в мережах мобільного зв'язку.

Майбутнє за невеликими, мобільними, надійними телефонними апаратами, які мають гарантовану стійкість захисту мовної інформації і високу якість звуку.

Література:

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. -М.: Гостехкомиссия РФ, 1998.-320 с.

2. Алексеенко В.Н., Сокольский Б.Е. Технические средства охраны, безопасности и сигнализации: справ. – М. : ВИМИ, 1994.-360 с.

3. Кисилев А.Е. Коммерческая безопасность / А. Е. Кисилев и др. – М. : Иноро Арт, 1993. – 286 с.

4. Барсуков В.С. Безпека: технології, засоби, послуги / В.С. Барсуков. – М., 2001 – 496 с.

Ткач В.І.
Студент кафедри Телекомунікації
ОНАЗ ім.О.С.ПОПОВА
м. Одеса, Україна

ЗАЛЕЖНІСТЬ ШУМОВИХ ХАРАКТЕРИСТИК ОПТИЧНОГО СИГНАЛУ ВІД ПАРАМЕТРІВ МОДУЛЯЦІЇ

Анотація. Проведено оцінку впливу глибини модуляції на співвідношення сигнал/шум волоконно-оптичного підсилювача. Розглянуто волоконно-оптичні підсилювачі з різним значенням коефіцієнту шуму. Показана можливість значного збільшення співвідношення сигнал/шум за рахунок підвищення глибини модуляції

Поява нових технологій, пов’язаних зі спектральним розділенням каналів (СРК) підвищила вимоги до якості модуляції оптичних сигналів. Однією з причин цього є використання на мережах СРК волоконно-оптичних підсилювачів [1]. Перевагою волоконно-оптичних підсилювачів є можливість підсилення групового оптичного сигналу, що складається з ряду оптичних каналів. Недоліком волоконно-оптичних підсилювачів є генерація квантового шуму, який визначається фізичними принципами їх функціонування.

Причиною квантового шуму є спонтанні переходи електронів з верхнього енергетичного рівня на нижній навіть у випадку відсутності сигналу. Під час кожного такого переходу відбувається генерація шумового кванту. Шумові характеристики волоконно-оптичного підсилювача визначаються таким параметром, як коефіцієнт шуму, який може в середньому приймати значення в межах 3-7 дБ.

З метою оцінки впливу параметрів модуляції на шумові характеристики в роботі було використано співвідношення, наведені в [2].

Розрахунки було проведено для співвідношення потужності вхідного сигналу до потужності шуму на вході підсилювача в 10 дБ та різних значеннях коефіцієнту шуму оптичного підсилювача, що лежали в межах від 3 до 9 дБ. Величина глибини модуляції при цьому змінювалась в межах від 0,2 до 0,95. Як випливає з результатів розрахунків, глибина модуляції є важливим фактором для визначення співвідношення сигнал/шум на виході оптичного підсилювача. Так, наприклад, підвищення глибини модуляції від значення 0,2 до 0,95 призводить зміни співвідношення сигнал/шум на виході підсилювача від мінус 12 дБ до + 4 дБ для волоконно-оптичного підсилювача, що характеризується коефіцієнтом шуму 4 дБ. При цьому така ж зміна глибини модуляції для волоконно-оптичного підсилювача з коефіцієнтом шуму, що дорівнює 2 дБ, призводить зміни співвідношення сигнал/шум на виході підсилювача від мінус 9 дБ до + 7 дБ.

В результаті проведеного моделювання в роботі визначено вплив на шумові характеристики вихідного сигналу параметрів модуляції та оптичних підсилювачів. Показано, що підвищення глибини модуляції може значно покращити співвідношення сигнал/шум на виході оптичного підсилювача.

Таким чином, важливою проблемою оптичного зв'язку є створення високошвидкісних модуляторів, які забезпечують глибину модуляції достатню для виконання вимог щодо співвідношення сигнал/шум в лінійному тракті оптичної системи передавання.

Література:

1. Фриман Р. Волоконно-оптические системы связи. – М.: Техносфера, 2003. – 440 с.

2. Recommendation ITU-T G.663 (04/2011) Application-related aspects of optical amplifier devices and subsystems

Солонько О.В.
Студентка ФІТ
Хорунжий О.І.
Доцент кафедри Інформаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

БОРОТЬБА З ПОМИЛКАМИ В ДИСКРЕТНИХ КАНАЛАХ ВОЛЗ

В теперішньому світі 70% всьогомережевого і 99% міжконтинентального трафіку передається через волоконно-оптичнісистеми передачі (ВОСП). Пропускна здатність оптичних ліній зв'язку швидко зростає і вже досягає 20 Тбіт/с. За період свого існування,починаючи з 70-х років ХХстоліття, волоконно-оптичні технології зазнали ряд вдосконалень, що дозволило використовувати їх на всіх рівнях мереж: від міжконтинентальних магістралей до мереж доступу [1].

Подальший розвиток ВОЛЗ за прогнозами спеціалістів буде проходити в кількох напрямках,серед яких покращення основних показників передачі інформації займає важливе місце. Особливу роль відіграє такий показник, як вірність передачі даних,адже саме він визначає загальну ефективність системи ПД. Але його покращення є дуже складною задачею і потребує розробки багатьох досить витончених методів, які мають впроваджуватись одночасно.

Для раціонального та ефективного застосування цих методівслід детально проаналізувати негативні чинники, що впливають на якість сигналу, а отже на вірність передачі даних - це шуми, спотворення, оптичні втрати, згасання сигналу, нелінійні ефекти, дисперсія, чірп-ефект.

В сучасній літературі досить детально висвітлюється одна з основних причин помилок в дискретному каналі ВОЛЗ- дисперсія, тобто розсіювання в часі спектральних або модових складових оптичного сигналу, яке призводить до збільшення тривалості імпульсу оптичного випромінювання при розповсюдженні його по оптичному волокну. В кінцевому рахунку дисперсія призводить до міжсимвольнихзавад, які впливають на помилкові рішення щодо символу сигналу в кожному тактовому інтервалі на прийомі.

Тому сьогодні, крім безпосередньої боротьби з причинами самого явища дисперсії,застосовують багато методів її компенсації. Їх поділяють на широкосмугові і вузькосмугові, а в залежності від місця застосування в структурі ВОСП розрізняють оптичні та електронні методи. Також є методи з фіксованою (нерегульованою), з адаптивною (з динамічним управлінням) та з компенсацією, що перебудовується (регульованою компенсацією). Найбільшого поширення набули такі методи компенсації дисперсії: просторова компенсація за допомогою волокна з негативною дисперсією, компенсація за допомогою дискретних раманівских підсилювачів, компенсація дисперсії на модах вищого порядку, інверсія спектру в середині лінії (завернення хвильового фронту), динамічна компенсація за допомогою керуючої електроніки, компенсуючі пристрої на основі бреггівської решітки або інтерферометра. Кожен метод має свої переваги та недоліки, тому застосування конкретного методу залежить від особливостей системи передачі даних.

Найбільш універсальним шляхом підвищення вірності ПДна базі ВОЛЗ є боротьба з помилками в дискретному каналі[2], оскільки цей метод придатний при впливі різних чинників будь-якої природи і навіть при одночасній дії кількох з них. Для цього можуть бути застосовані численніметоди виявлення і виправлення помилокв дискретному каналі. Вони добре розробленіі як правило, використовують сучасні завадостійкі коди, що можуть виявляти помилки (і тоді потрібно вводити зворотний зв'язок в адаптивних системах) або безпосередньо виправлятиїх.Останнім часом став дуже популярним в різних системах зв’язкуметод безпосередньої корекції помилок - ForwardErrorCorrection – FEC [3], що фактично є давно відомим методом виправлення помилок за допомогою коректуючого коду достатньо великої потужності.

Як один з варіантів можуть бути запропоновані коди Ріда – Соломона, що дозволяють виправляти пакети помилок. При цьому доцільно використати найбільш простий декодерМеггітта.

Існує кілька варіантів кодеківFEC, які відповідають поколінням цього коду, що здатен виправляти не лише однократні помилки, а й послідовність помилок (блоки помилок).

Для оптимізації вибору коду та його параметрів слід обрати модель потоку помилок в дискретному каналі на базі ВОЛЗ, що є досить складною задачею, яка потребує окремої розробки.

За деякими повідомленнями фірм – розробників відповідного обладнання FEC збільшує бітову швидкість BER з 9,95 Гбіт/с до 10,6Гбіт/с, і дозволяє зменшити BER з 10^{-5} до 10^{-15}.Економічно вигідним є застосування FEC у ВОСП високої дальності.

Отже, ВОСП з кожним роком зазнають всебічного вдосконалення, іпідвищення вірності передачі, безперечно, є важливим аспектом їх розвитку, адже саме вона визначає загальну ефективність системи ПД.

Література:

1. Скляров О. К. Сучасні волоконно-оптичні системи передачі, апаратура і елементи / О. К. Скляров. - Київ: СОЛОН-Р, 2001 - 274 с.

2. Хорунжий А.И., Кабасин А.ГПовышениеверностипередачиданных по реальным каналам.Сборникнауч. трудовИнститута автоматики АН УССР.- Киев: 1990г.

3. Clark, GeorgeC., Jr., and J. Bibb Cain. Error-Correction Coding for Digital Communications. NewYork: PlenumPress, 1981

Гаврилюк О.Г.
Научный сотрудник НИЦ ВИТИ
Мальцева И.Р.
Научный сотрудник НИЦ ВИТИ
г. Киев, Украина

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ДКМВ ДИАПАЗОНА ПРИ ПОСТРОЕНИИ РАДИОСЕТЕЙ СПЕЦИАЛЬНЫХ ПОТРЕБИТЕЛЕЙ

Опыт оперативной и боевой подготовки, анализ развития систем управления войсками передовых стран мира, а также военных конфликтов и локальных войн последнего времени выявили острую необходимость в коренном изменении подходов к вопросам использования декаметрового (ДКМВ) диапазона, а следовательно и решения возникающих при этом проблем.

ДКМВ радиоканал является единственным средством связи в местах, не имеющих специальной инфраструктуры и труднодоступных районах. Однако ДКМВ радиоканал существенно зависит от состояния ионосферы, которая, как известно, нестабильна

К основным недостаткам ДКМВ радиосвязи можно отнести:

- зависимость качества радиоканала от времени суток, времени года и погодных условий;
- низкая стабильность параметров радиоканала на расстояниях более 40 – 50 км.;
- зависимость от мощности и взаимного расположения радиоустройств;
- большая загруженность диапазона и, как следствие, обилие помех;

При построении радиосетей в ДКМВ диапазоне существует вероятность невозможности установления связи с требуемым абонентом. Эта ситуация может возникнуть в случае неблагоприятных метеоусловий или нахождения абонента в зоне непрохождения радиоволн. Однако эти обстоятельства могут не влиять на связь с другими абонентами. То есть абонент не доступен именно для определенных узлов связи в данный момент времени. Следовательно, существует задача организации связи с требуемым абонентом в условиях отсутствия прямой связи между приемопередающими устройствами.

Возвращаясь к работе самих устройств, следует уточнить способ передачи данных в среде.

Аналоговый способ передачи предполагает передачу речи или двоичных данных через устройство преобразования сигналов (модем).

В данном случае аналоговый сигнал затухает (ослабляется), что ограничивает длину радиолинии. Увеличение длины радиолинии обеспечивается за счет применения ретрансляционных пунктов, что в свою очередь приводит к снижению качества сигнала за счет накопления помех.

Для передачи цифровых данных на большие расстояния используются ретрансляторы, которые принимают цифровой сигнал, восстанавливают принятую цифровую комбинацию и передают восстановленный сигнал. Таким образом, происходит компенсация затухания радиолинии. Такой же метод используется и при передаче аналогового сигнала, если он переносит цифровую информацию. Для этого в расположенных соответствующим образом точках передающей системы помещаются не усилители, а ретрансляторы. Такой ретранслятор восстанавливает цифровую информацию из аналогового сигнала и создает новый, чистый аналоговый сигнал, препятствуя, таким образом, накоплению помех.

Следовательно, можно ввести в работу самих приемопередающих устройств функцию, позволяющую им работать в качестве ретрансляторов, осуществляющих маршрутизацию трафика [2].

В настоящий момент в Украине не существует современных открытых стандартов беспроводных сетей, работающих в ДКМВ диапазоне. Однако разработка алгоритма защищенного обмена данными в ДКМВ диапазоне подразумевает следование определенным тенденциям, введенным Министерством обороны США в стандарте MIL-STD-188-141B [3].

Наилучшим способом анализа данного алгоритма работы ДКМВ радиосети является построение математической программной модели функционирования данной сети.

Задача разработки алгоритма и форматов системы цифровой радиосвязи для ДКМВ радиостанций предусматривает анализ существующих стандартов, реализующих соединения по радиоканалу. Более того, есть смысл отталкиваться от уже используемых стандартов, зарекомендовавших себя на практике.

Наиболее подходящими для этой цели являются стандарты цифровой радиосвязи серии IEEE 802.11 и MIL-STD-188-141B. Стандарты серии IEEE 802.11 [4] созданы специально для передачи информации между потребителями в УКВ диапазоне и не подходят для организации дальней ДКМВ радиосвязи ввиду существенной разницы в стабильности радиоканалов, а следовательно и скорости передачи информации.

Стандарты MIL-STD-188-141B решают проблему увеличения дальности и стабильности радиосвязи, используя особенности коротких волн отражаться от ионосферы. Однако в ДКМВ диапазоне есть негативные явления не позволяющие осуществлять связь на высоких скоростях.

Другой особенностью стандарта MIL-STD-188-141B является формат передаваемых кадров, наиболее приспособленный для ДКМВ диапазона, который специально создан для передачи цифровых сигналов по низкоскоростному и нестабильному радиоканалу.

Стандарты организации компьютерных сетей IEEE 802.11 и IEEE 802.3 [5] , во многом идентичные, но практически не имеют сходства со стандартом MIL-STD-188-141B. Следовательно необходима доработка канального уровня стандарта MIL-STD-188-141B для оптимального взаимодействия с сетевым уровнем. Требуется подобрать форматы кадров и усовершенствовать алгоритмы канального уровня.

Предусмотренное в MIL-STD-188-141B кодирование позволяет исправлять ошибки, внесенные средой передачи до определенного предела. Но пока не создана модель среды передачи, то есть модуль, который бы вносил в передаваемые последовательности ошибки, свойственные именно ДКМВ диапазону.

Создав модуль, вносящий ошибки и задав вероятности их появления, можно проверить и оценить способности алгоритма канального уровня к устойчивости по отношению к ошибкам различного рода и их комбинациям. Изменяя переменные, можно задать условия, имитирующие нестабильность ДКМВ диапазона. Также можно задавать условия расположения самих радиоустройств. Все это приведет к оптимальным цифрам, которые возможно представить как рекомендации к реализации устройств цифровой ДКМВ радиосвязи.

Полученная модель является аппаратом аналитического расчета для алгоритмов и форматов данных канального уровня модели ISO/OSI для определенных условий функционирования цифровых ДКМВ радиостанций.

Применение полученных рекомендаций, как опциональная функция для устройств цифровой ДКМВ радиосвязи, даст возможность улучшения пользовательских характеристик данных устройств в заранее заданных условиях местности, среды передачи данных или размерах сети.

Литература:

1. Родос Л.Я Электродинамика и распространение радиоволн (распространение радиоволн) СпБ, изд-во СЗТУ – 2007, 90с.

2. Столлингс В. Беспроводные линии связи и сети / Пер. с англ. М.: Изд. дом «Вильямс», 2003.

3. MIL-STD-188-141B. Interoperability and performance standards for medium and high frequency radio systems. DOD interface standard. 1 March 1999 / DoD USA. 1999.

4. IEEE Std 802.11-1999 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications / The Institute of Electrical and Electronic Enginers, inc. 3Park Avenue, New York, USA. 1999.

5. IEEE Std 802.3-2002 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications / The Institute of

Electrical and Electronic Enginers, inc. 3Park Avenue, New York, USA. 8 March 2002.

Герасименко А.А.
Научный сотрудник НИЦ ВИТИ
Мальцева И.Р.
Научный сотрудник НИЦ ВИТИ
г. Киев, Украина

ИССЛЕДОВАНИЕ МЕТОДОВ ПЛАНИРОВАНИЯ ПОСТРОЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Основным функциональным назначением создаваемых телекоммуникационных сетей является своевременная передача поступающих сообщений с требуемым уровнем качества, готовности к работе и стойкости.

Причиной возникновения проблемы выбора оптимального построения телекоммуникационных сетей являются расхождение между желаемыми (заданными) параметрами и неизвестных путях преодоления этого расхождения (несоответствия).

Конечная цель, как правило допускает декомпозицию, в результате которой формируются взаимосвязанные частные цели, которые в общем случае могут быть подвергнуты дальнейшему членению на более простые составляющие (подцели, задачи).

При планировании построения телекоммуникационных сетей различного иерархического уровня целесообразно использовать методики:

1. Методика ограничений.

2.Методика расчёта и сравнения показателей эффективности функционирования.

Сущность методики ограничений заключается в двухэтапном оценивании сравниваемых сетей связи. На первом этапе все сети проверяются на соответствие минимальным требованиям системы более высокого уровня иерархии. Сети связи, не соответствующие этим требованием, на втором этапе не рассматриваются. Второй этап заключается в выборе сети, наиболее полно удовлетворяющей предъявляемым требованиям.

Сравнительное оценивание производиться не по показателю качества функционирования сети (пропускной способности, устойчивости, мобильности и другим), а по показателю качества услуги связи – своевременности (внешнему показателю сети связи).

В общем случае показателем своевременности связи является время установления соединений ($t_{уст}$), определяемое временем ожидания абонентом соединения ($t_{ож}$) и временем непосредственного предоставления услуг ($t_{прс}$).

$$t_{уст} = t_{ож} + t_{прс}. \qquad (1.1)$$

При проведении расчётов предполагается, что для телекоммуникационной сети определяющим критерием является время ожидания абонентом соединения. В этом случае время ожидания соединения абонента не должно превышать требуемого ($\grave{O}_{\text{íæ}}^{\text{òð}}$).

$$t_{\text{ож}} \leq \grave{O}_{\text{íæ}}^{\text{òð}} \quad . \tag{1.2}$$

На первом этапе оцениваются варианты сетей связи с точки зрения соответствия их характеристик заданным требованиям. На втором этапе сравниваются варианты построения сетей по выбранному основному критерию (например, время ожидания абонентом не должно превышать требуемое). В соответствии с этим критерием выбирается вариант построения сети.

Достоинство данной методики – простота, которая достигается за счёт приблизительной точности сравнения. Это обусловлено тем, что после первого этапа все объекты, отвечающие требованиям, ставятся в равные условия, хотя могут иметь существенные различия по частным показателям.

Рассмотренная методика самостоятельно применяется редко.

Исследование операции построения сетей целесообразно целесообразно выполнять и использованием двух методик: сначала выполняется этап методики ограничений, а затем объекты сравниваются с помощью методик абсолютных или относительных показателей эффективности.

Абсолютный показатель эффективности функционирования i – той телекоммуникационной сети вычисляется по формуле:

$$W = \sum_{i=1}^{j} a_i y(e_{ij}) \tag{1.3}$$

где, j – количество частных показателей эффективности, a_i - средний весовой коэффициент i - го показателя, $y(e_{ij})$ – функция затратности j – го показателя i – той сети, характеризующая степень его соответствия заданным требованиям.

Выбор частных показателей осуществляется исходя из требований, предъявляемой к сети, причём частные показатели должны иметь явный физический смысл. Для сети телефонной связи такими требованиями является пропускная способность при заданном качестве обслуживания абонентов, надёжность функционирования сети и её элементов, мобильность (время изменения структуры сети связи и её состояния), количество обслуживающего сеть персонала, качество разговорного тракта (разборчивость или достоверность), своевременность передачи сообщения в сети и др.

В зависимости от иерархии сети и её специфических особенностей этот перечень может быть скорректирован и расширен.

Весовые коэффициенты частных показателей эффективности находятся путём статистической обработки мнений экспертов. Заключение при анализе телекоммуникационной сети даёт лицо принимающее решение.

Предполагается, что при проведении экспертного опроса снижается субъективизм оценок. Экспертам рекомендуется выставлять оценки в пределах от 0,01 до 1. Оценки сводятся в матрицу $\|a_{xy}\|$, столбцы которой представляют совокупность оценок, выставленных одним из экспертов, а строки соответствуют одному из n показателей:

$$\|a_{xy}\| = \begin{Vmatrix} a_{11} & a_{12} & ..... & a_{1m} \\ a_{21} & a_{22} & ..... & a_{2m} \\ ..... & ..... & ..... & ..... \\ a_{n1} & a_{n2} & ..... & a_{nm} \end{Vmatrix} \qquad (1.4)$$

Затем определяется среднее весовое значение для каждого из весовых показателей по формуле:

$$a_i = (1/m)\sum_{i-1}^{m} a_x \ , \qquad (1.5)$$

После этого для каждого показателя выбирается функция затратности, значение которой лежит в пределах от нуля до единицы и зависит от удовлетворения требованиям, предъявляемым к сети по данному показателю эффективности.

При составлении таких функций обращается внимание на их физический смысл.

Например, показателем мобильности сети связи является время изменения её структуры или состояния ($t_{èçì}$), которое требуется для выполнения необходимого комплекса мероприятий $N_{необх}$. Критерием оценки мобильности сети связи служит выражение, показывающее степень соответствия времени изменения её структуры (состояния) установленному (допустимому) времени:

$$\bar{t}_{изм} \leq t_{уст} \qquad (1.6)$$

при $N \leq N_{необх}$,

Исходя из этого функция затратности, характеризующая мобильность сети связи, может быть записана следующим образом:

Значение этой функции изменяется в пределах от нуля до единицы и чем ближе значение $t_{èçì}$ к $t_{óñò}$, тем большее значение принимает данная функция, что не противоречит физическому смыслу описываемого процесса.

Такие функции ограничивают разброс значений параметров, что обеспечивает равные условия учёта каждого из рассматр

$$y(t_{èçì}) = \begin{cases} 1-\lg(t_{уст}/t_{изм} & при \ \ t_{изм}>t_{уст} \\ 1 & при \ t_{изм}<t_{уст} \end{cases} \qquad (1.7)$$

иваемых показателей эффективности. Элемент субъективизма вносят весовые коэффициенты, которые перемножаются на соответствующие значения функций. В теории сетей такой подход называется аддитивной свёрткой. В результате вычислений для каждой из рассматриваемых телекоммуникационных сетей находится абсолютный показатель эффективности. Предпочтение отдаётся сети, у которой абсолютный показатель эффективности окажется выше.

Дружинін В.А.
Професор кафедри Телекомунікаційних технологій,
Кременецька Я.А.
Доцент кафедри Телекомунікаційних технологій,
Державний університет телекомунікацій,
м. Київ, Україна

ОПТИЧНІ МЕРЕЖІ ТА СИСТЕМИ В ЕВОЛЮЦІЙНОМУ ПЕРЕХОДІ НА ФОТОННІ

В фотонних мережах (Photonic network) або повністю оптичних AON (All - optical Networks) і системах усі процеси передачі, прийому, обробки та комутації сигналів відбуватимуться на чисто фотонному рівні, без участі електронних процесів і електронних пристроїв. Використовуючи фотони, можливо досягти більш високої швидкості передачі сигналу, ніж у електронів, до того ж оптоелектронні прилади втрачають 30% енергії на конвертацію електронів у фотони і при зворотному процесі. Прогрес фотонних технологій пов'язаний з розробкою оптичних компонентів: лазери, в яких перестроюється довжина хвилі, оптичні хвильові мультиплексори (із спектральним розділенням каналів до 40 і більше) DWDM, широкосмугові оптичні підсилювачі EDFA, а також підсилювачі з дистанційним оптичним живленням, оптичні комутатори, хвильові конвектори (рис.1).

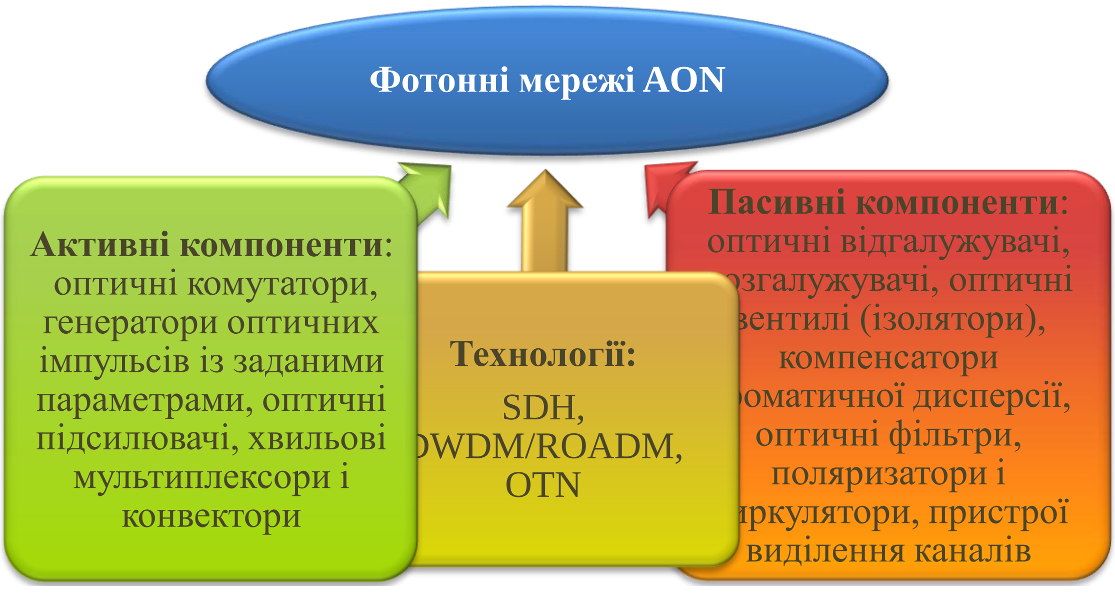


Рисунок 1. Області розробок для фотонних мереж.

Конфігурація фотонних мереж стане в майбутньому повнозв'язною на магістральному рівні, на відміну від класичних популярних сьогодні кільцевих структур. Оптичне обладнання без оптоелектронного перетворення може забезпечити пропускні здібності магістралей до декількох Тбіт/с.

Особливістю розвитку є наскільки швидко здійсниться революційний перехід замінювання електронного обладнання на оптичне. Можливо переважним буде поступовий еволюційний перехід, який грунтується на інтеграції устаткування SDH/SONET і систем DWDM. Очікується, що великомасштабні фотонні мережі будуть розгорнуті в поточному десятилітті в США, а потім і в Європі. В середині наступного десятиліття можливе широке впровадження повністю оптичних вузлів (без електронної регенерації сигналів), в яких оброблятимуться сотні довжин хвиль при швидкостях передачі в інтерфейсах вузлів до декількох десятків Гбіт/с. Однак перші стандарти на оптичне мережеве обладнання (як в МСЕ, так і в ANSI) розроблюються відносно повільно. Сучасні магістральні мережі, які є основою глобальних транспортних мереж, повинні будуватися на базі стандартизованих рішень, що визначаються архітектурою відкритих систем.

Основа сучасних обчислювальних систем для реалізації високої продуктивності - технологія багатоядерної інтеграції процесорів. Подальше підвищення тактової частоти (більше 3,8 ГГц) обмежується рядом фундаментальних фізичних бар'єрів (оскільки технологічний процес майже впритул наблизився до розмірів атома). Зі зменшенням розмірів кристала і з підвищенням тактової частоти зростає струм витоку транзисторів. Це призводить до підвищення споживаної потужності і збільшення викиду тепла. Електричні з'єднання між ядрами також обмежують пропускну здатність через тривалу затримку часу і високу споживану потужність [1]. У порівнянні з традиційними електричними сполуками, оптичні міжз'єднання нероздільні, мають більш високу пропускну здатність, низьку затримку і менші витрати потужності. Отже, фотонні мережі на оптичних інтегральних схемах (photonic integrated circuit) використовуються для підвищення продуктивності, що привертає великий науковий інтерес до цього питання, до того ж процес виготовлення сумісний з метало-оксид-напівпровідниковою технологією (КМОН). Для створення телекомунікаційних систем на основі фотонних технологій спеціалістам необхідно розв’язувати багато технологічних проблем, компоненти для таких систем представлені на рис.2.

Рисунок 2. Компоненти для створення перспективних телекомунікаційних систем на основі фотонних технологій.

В Україні на мережеву арену активно стала входити технологія DWDM (англ. Dense Wavelength Division Multiplexing) - щільне хвильове мультиплексування, у якому використовують тільки одне вікно прозорості 1550 нм ущільнення в якості як магістральної, так і локальної системи. DWDM - технологія ущільнення інформаційних потоків, при якій кожен первинний інформаційний потік переноситься за допомогою світлових пучків на різних довжинах хвиль, а в оптичній лінії зв'язку знаходиться сумарний груповий сигнал, сформований мультиплексором з декількох інформаційних потоків.

Сьогодні для фотонних мереж розроблені нові типи одномодових оптичних волокон TRUEWAVE, ALLWAVE, LEAF та ін. Розробляються також фотонні комутатори на основі фізичних принципів, що використовують квантовооптичні, електрооптичні, магнітооптичні, термооптичні, акустооптичні та інші явища, що відбуваються у відповідних напівпровідникових і оптичних структурах: фотонних кристалах (мікроструктурованих волокнах), на рідкокристалічних матрицях, на дзеркальних відображаючих елементах.

Нещодавно компанія IBM продемонструвала перший монолітний фотонний чіп, виготовлений за 90-нм CMOS-технологією, така подія є великим кроком до створення комп'ютерних чіпів, на кристалах яких інтегровані одночасно елементи оптичних і електронних схем. Представники компанії повідомляють, що їх фахівці вже провели успішні випробування чотирьохпортових кремній-фотонних чіпів, організувавши за їх допомогою мережу, здатну передавати інформацію зі швидкістю 100 Гбіт/с на відстань до 2 кілометрів. Наступним кроком компанії IBM стане інтеграція на кристал чіпа джерел світла - лазерів на основі напівпровідникових матеріалів III-V групи. Цей крок буде досить довгим і важким, але розроблені за цей час технології дозволять включати до складу чіпа не тільки лазери, але і масу інших оптичних компонентів.

Література:

1. Маккавеев В. Фотонные коммутаторы // Компоненты и технологии. – 2006.

2. Гайворонская Г. С. Новый подход к построению структуры коммутаторов оптических сигналов / Г. С. Гайворонская, А. В. Рябцов // Вісник Державного університету інформаційно-комунікаційних технологій. - 2012. - т. 10, № 3. - С. 43-46.

3. http://www.networkcommunicationsnews.co.uk/

Дружинін В.А.

Професор каф. Телекомунікаційних тхнологій,

Кременецька Я.А.

Доцент каф. Телекомунікаційних тхнологій,

Державний університет телекомунікацій,

м. Київ, Україна

ПРОБЛЕМИ СТВОРЕННЯ КЕРОВАНИХ НАПРУГОЮ ГЕНЕРАТОРІВ В ДІАПАЗОНІ СУБМІЛІМЕТРОВИХ ХВИЛЬ

Терагерцове випромінювання завдяки своїм фізичним властивостям [1] знаходить все більше застосування в різних областях, таких як медична діагностика, біохімічна розшифровка, системи безпеки, військова розвідка і т.ін. Великі перспективи для субміліметрового діапазону відкриваються в телекомунікаційних системах завдяки високій інформаційній ємності, високій спрямованості у порівнянні з мікрохвильовими. У середовищах де в ІК-діапазоні о детектування сигналу є затрудненим через фазове спотворення фронту хвиль, можливе отримання зображення високої роздільної здатності в субміліметровому діапазоні. Зазначені вище властивості відкривають також перспективи для цього діапазону в безконтактній швидкодіючій комутації і гібридних оптичних інформаційних системах.

Розробка джерел терагерцового діапазону йде двома шляхами:

- розробкою нових принципів генерування, пов'язаних з мініатюризацією структур приладів до декількох нанометрів і новими фізичними моделями опису процесів в таких структурах, із застосуванням нових матеріалів і нових технологій;

- використання вже розроблених напівпровідникових джерел міліметрового діапазону в помножувачах частоти на основі гармонік - сигналів, кратних основній частоті.

Здатність твердотільних матеріалів генерувати електромагнітні хвилі високої частоти обмежується структурою речовини. Крім того, базова частота зазвичай задається коливальним контуром на основі конденсатора змінної ємності, і у випадку застосування терагерцових хвиль його не вдається точно підлаштувати. Генерований сигнал розмивається в широкому спектрі, і потужність в необхідному діапазоні суттєво зменшується. У роботах проаналізовані ГУН з LC-резонатором с змінної ємністі для налаштування частоти коливань і показано, що цей метод настройки добре працює і досягає помірної перебудови частоти при низьких частотах (100 ГГц) [2]. Показано, що при збільшенні робочої частоти паразитні ємності обмежують можливості налаштування варикапів, також знижується вихідна потужність сигналу. Тому в CMOS осциляторах вище 100 ГГц з високою вихідною потужністю краще не використовувати варактори, оскільки в цьому випадку їх частота не може бути налаштована. Шляхи побудови помножувачів частоти, ефективних в міліметровому діапазоні:

- на основі нелінійних залежностей їх реактивних параметрів від напруги;
- на основі помножувачів частоти високої кратності на ЛПД, що діють в режимі радіоімпульсного порушення коливань в області високих частот і їх синхронізації.

Просування радіосистем в субміліметровий діапазон є перспективним, але поки технологічно важко здійсненним. Напівпровідникові малорозмірні технології менш 130 (65) нм для субміліметрових хвиль складні, вимагають витрат, охолодження, глибокого вакууму і т.д. Помножувальні системи із зовнішнім сигналом накладають певні складності до зовнішньому сигналу також за технологією і синхронізації. Пов'язані системи генераторів можуть генерувати і підсилювати сигнали вищих гармонік з використанням зовнішнього джерела (резонатора) або без нього, покладаючись на параметри взаємозв'язку для синхронізації (режим взаємного захоплення частот). Спосіб внутрішнього з'єднання і його динаміка, а також геометрія пов'язаної системи можуть бути спроектовані для різноманітних функцій (рис.1).

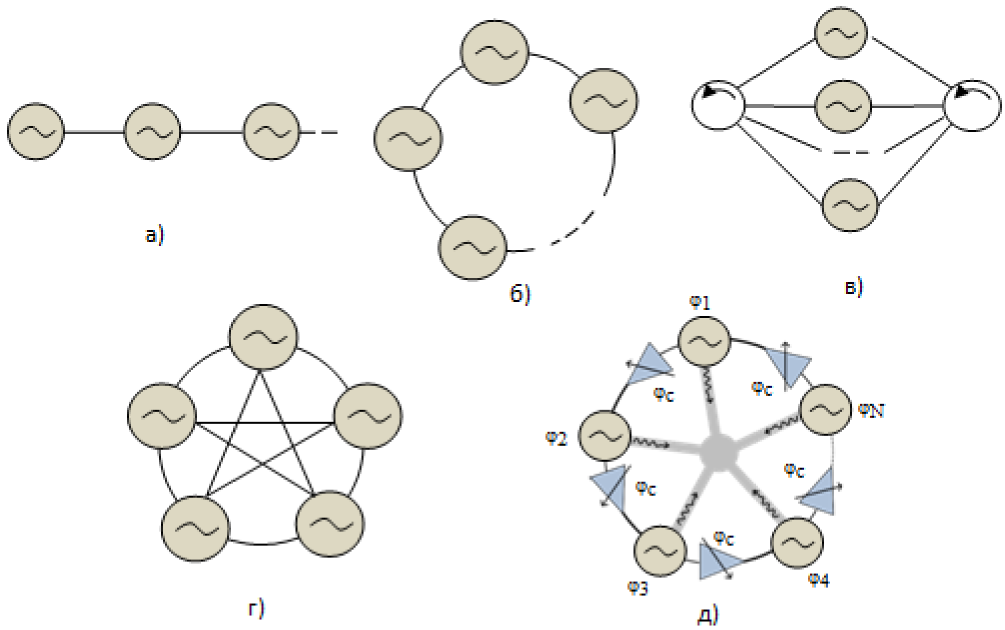


Рисунок 1. Конфігурації взаємозв'язку осциляторів: а) послідовна, б) циклічна, в) паралельна, г) кожен з кожним, д). циклічна конфігурація, запропонована Афшарі [2] (кола представляють основні осцилятори з фазами $\varphi_1, \varphi_{2,} \ldots \varphi_N$, трикутні блоки – фазо зрушуючі φ_c схеми з'єднання).

У роботі Ехсана Афшари (Ehsan Afshari) з Корнельського університету (штат Нью-Йорк) [2] показана можливість реалізації КМОП-транзістров 65 нм технології в циклічній конфігурації взаємопов'язаних мікрогенераторів (без зовнішнього сигналу) для отримання терагерцового випромінювання, де експериментально отримана частота генерації 290 (320) ГГц з кроком перестроювання 13 (8,4) ГГц з посиленням потужності сигналу в 10000 раз ГГц. У роботах пропонують кільцеву сполучну топологію між основними генераторами, а розташовані між ними хвилеводи здійснююють зсув фази. Запропоновані конфігурації з зв'язаних осциляторів здатні створити і об'єднати гармоніки основної частоти з декількох основних генераторів. Управління частотою осциляторів і накладає постійний бажаний фазовий зсув між ними. При певному налаштуванні піки і спади різних гармонік врівноважують один одний, одночасно посилюючи потужність основного сигналу на мікроблок. Постійний зсув фази має вирішальне значення в гармонійному відборі. Зв'язок між послідовними осциляторами здійснюється фазовим зсувом перебудованого, маніпулюючи фазовим розладом між генераторами можливо регулювати частоту. Точний діапазон настройки частоти вимагає чисельного моделювання з підбором параметрів :з'єднують хвилеводи, змінюють фазу, налаштовуючи конденсатори на резонанс.

Тому для подальшого дослідження отримання генерації субміліметрових хвиль в циклічній конфігурації осциляторів необхідно:

- проаналізувати можливості збільшення смуги захоплення виходячи з розрахунків амплітуд осциляцій струму, тимчасових затримок формування імпульсів, тимчасового (фазового) приросту на з’єднувальних елементах;

- провести порівняльний аналіз множення частоти в джерелах міліметрового діапазону: транзистор, лавинно-пролітний діод, тунельний діод, резонансно-тунельний діод, діод Ганна (кожен з цих нелінійних осциляторів має свої характеристики і переваги або по потужності, або по чистоті сигналу);

- чисельно промоделювати амплітуди осциляцій вхідного і вихідного струмів (резонансні частоти), амплітуди гармонік, коефіцієнти перетворення частоти на гармоніках, можливий теоретичний приріст частоти, потужності в циклічній конфігурації взаємопов'язаних осциляторів.

Література:

1. Майская В. На пути к достижению субмиллиметрового диапазона длин волн/В. Майская// Электроника: наука, технология, бизнес, 2013, № 6. - С. 44-58.

2. Tousi Y. M. A novel CMOS high-power terahertz VCO based on coupled oscillators: Theory and implementation / Y. M Tousi., O. Momeni, and E. Afshari // IEEE J. Solid-State Circuits, Vol. 47, No. 12, Dec. 2012. – pp. 3032-3042.

3. Устройства сложения и распределения мощностей высокочастотных колебаний / [В.В. Заенцев [и др.] ; под ред. З.И. Моделя. - М. : Сов. радио, 1980. – 294 с.

Ткаченко О.Н.
Доцент каф. Телекоммуникационных систем
Перепелица Н.Л.
Ст. преподаватель каф. Телекоммуникационных систем
Государственный университет телекоммуникаций
г. Киев, Украина

АЛГОРИТМЫ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ МОДЕЛИ

Под идентификацией модели подразумеваем процесс определения ее параметров

$$C = (c_1, ..., c_k) \tag{1}$$

в режиме нормальной эксплуатации объекта. Структура модели при этом известна (она определена на стадии структурного синтеза):

$$Y = F(X, U, C) \tag{2}$$

т. е. оператор F предполагается заданным. Это означает, что задан алгоритм (правило, инструкция), с помощью которого можно определить состояние Y модели, если заданы состояния X и Y ее входов, а также параметры (1). Именно эти параметры определяются на этапе идентификации [1, с.475].

Очевидно, что для идентификации необходимо иметь информацию об изменении входов и выходов объекта. Но объект пока не управляется (мы только создаем систему управления), поэтому влияние входа U на выход Y не может быть исследовано на этапе идентификации. Это несколько упрощает задачу, так как вместо модели (2) следует брать модель вида

$$Y = F`(X, C), \tag{3}$$

в которой не фигурирует управляемый вход U.

В процессе идентификации используются исходные данные, которые удобно подразделить на два класса:

— априорные, которые содержатся в структуре S^t модели. Это означает, что должен быть задан (или определен на этапе структурного синтеза) вид оператора $F`$. Например, вид уравнения, граф взаимосвязи элементов модели и т. д.;

— апостериорные, которые представляют собой наблюдения состояний входа Xи выхода Yобъекта в процессе его нормальной эксплуатации, т. е. информацию

$$I = (X_i, Y_i), i = 1, ..., N, \tag{4}$$

где i - номер моментов времени t_i, когда фиксировались значения X и Y, т. е. $X_i = X(t_i), Y_i = Y(t_i)$, где $X(t)$ и $Y(t)$ - функции, описывающие поведение входа и выхода объекта в процессе его нормального функционирования в среде.

Моменты времени t_i обычно равномерно покрывают промежуток времени наблюдения [0, T], т. е.

$$t_i = \tau(i-1),$$

где τ - интервал между наблюдениями (4), т. е. $\tau = T/(N-1)$.

Таким образом, исходные данные, необходимые для идентификации, образуются двойкой

$$\langle St, I \rangle \tag{5}$$

т. е. структурой модели (3) и наблюдениями (4). Процесс идентификации параметров модели сводится к определению параметров (1) по исходным данным (4), т. е.

$$C = \varphi(St, I) \tag{6}$$

где φ - алгоритм идентификации, определяющий, каким образом можно найти параметры C, зная St и I.

Рассмотрим различные алгоритмы φ. Эти алгоритмы можно подразделить на два больших класса: адаптивные и неадаптивные [2, с.61].

Под адаптивным алгоритмом идентификации будем понимать алгоритм, позволяющий уточнять значения идентифицируемых параметров модели по мере получения дополнительной информации о работе объекта. Пусть на i-м шаге адаптивной идентификации были какие-то определенные значения идентифицируемых параметров. Отметим их индексом i;

$$C_i = (c_1^i, ..., c_k^i).$$

Пусть, далее, получена дополнительная информация, т. е. пара наблюдений входа и выхода объекта в $(i+1)$-й момент времени:

$$I_{i+1} = \langle X_{i+1}, Y_{i+1} \rangle. \tag{7}$$

Очевидно, что эта информация должна каким-то образом изменить (откорректировать) имеющиеся значения Cи дать возможность получить C_{i+1}- более точное значение параметров. Связь между C_i и C_{i+1}определяется адаптивным алгоритмом идентификации:

$$(C_i, I_{i+1}) \xrightarrow{\tilde{\varphi}_a} C_{i+1}$$

или в обычной рекуррентной форме

$$C_{i+1} = \tilde{\varphi}_a(C_i, I_{i+1}) \tag{8}$$

Здесь $\tilde{\varphi}_a$ - алгоритм адаптивной идентификации, который позволяет определить последующее значение параметров, исходя из новой информации (I_{i+1}) и старых представлений о значениях параметров C_i. Адаптация, таким образом, представляет собой способ получения «нового знания» путем коррекции «старого знания» на основе новой информации [3, с.72].

Алгоритм (8) удобнее записать в виде

$$C_{i+1} = C_i + \varphi_a(F(X_{i+1}, C_i), I_{i+1}) \qquad (9)$$

где φ_a - оператор адаптивной идентификации.

Если адаптивный метод идентификации реализуется в реальном масштабе времени, то его целесообразно называть методом самонастраивающейся модели.Схема этого метода показана на рис. 1. Здесь на вход модели подается вход *X* объекта. Информация о состоянии объекта *Y*, модели *F(X, C)* и среды *X* сообщается блоку адаптации, который вырабатывает сигнал коррекции $\Delta C = \varphi_a(F(X, C), I)$, изменяющий параметры модели в соответствии с (9) с помощью исполнительного механизма.

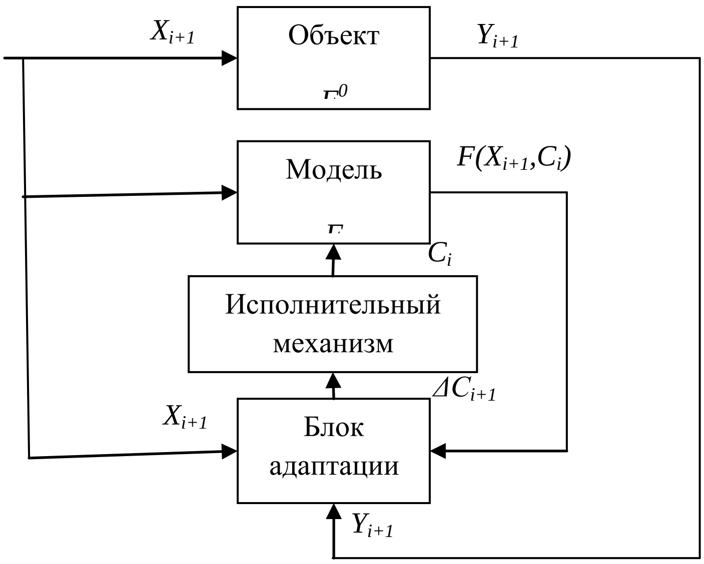


Рисунок 1. Схема адаптивной идентификации

Очевидно, что для реализации адаптивных алгоритмов идентификации вовсе не обязательно использовать реальный масштаб времени. В этом случае роль объекта играет информация *I* (4), которая поступает в алгоритм адаптивной идентификации из памяти порциями $X_i, Y_i\rangle (i = 1, ..., N)$.

В противоположность адаптивному алгоритму идентификации неадаптивный позволяет получить искомые параметры *C* сразу, используя всю информацию *I* (4), а не путем их постепенного уточнения. Если информация *I* задана, то задачу идентификации можно решать как адаптивным, так и не адаптивным способом. На первый взгляд может показаться, что неадаптивный алгоритм всегда лучше адаптивного, но каждый из них имеет свои преимущества и недостатки.

Неадаптивный алгоритм позволяет сразу определить идентифицируемые параметры *C*, но он сложнее и для его реализации требуются значительные вычислительные мощности.

Литература:

1. Стеклов В. К. Оптимізація та моделювання пристроїв та систем зв'язку: підруч. для вищ. навч. закл. / В. К. Стеклов, Л. Н. Беркман, Є. В. Кільчицький; за ред. В. К. Стеклова. – К.: Техніка, 2004. – 576 с.
2. Ткаченко О. М. Ідентифікація параметрів моделі як один з етапів управління складним об'єктом / О. М. Ткаченко // Тези доповідей IV Міжнар. наук.-техн. конференції студентства та молоді «Світ інформації та телекомунікацій-2007». – Київ: 12-13 квітня 2007 р. – С. 61.
3. Ткаченко О. М. Оптимізація параметрів систем управління телекомунікаційними мережами / О. М. Ткаченко, Д. О. Нацик // Вісник Державного університету інформаційно-комунікаційних технологій. – 2005. – Т. 3, № 3–4. – С. 71–73.

Асауленко І.О.
Студентка групи 4-V-T
Український державний університет залізничного транспорту
м. Харків, Україна

ДЕКОДУВАННЯ ЛІНІЙНИХ БЛОКОВИХ КОДІВ НА ОСНОВІ СТОХАСТИЧНИХ ПОШУКОВИХ МЕТОДІВ ОПТИМІЗАЦІЇ

При розгляді сучасних телекомунікаційних систем важливою задачею є забезпечення заданої достовірності передачі даних. Це призводить до необхідності застосування різноманітних методів завадостійкого кодування. У теперішній час широкого розповсюдження набули лінійні блокові коди, зокрема коди з малою щільністю перевірок на парність, із застосуванням методів ітеративного декодування [1, с. 177 – 180]. Показано, що класичні методи жорсткого декодування характеризуються відносно низькою здатністю корегування, що обмежує галузь їх застосування додатками, що допускають високу ймовірність помилки декодування, а класичні методи м'якого декодування через значну обчислювальну складність не підходять для використання в додатках, що підтримують високу швидкість передачі інформації. Встановлено, що задача декодування лінійних блокових кодів може бути сформульована у вигляді задачі цілочисельного програмування, та полягає у пошуку максимального значення цільової функції, що характеризується нелінійністю, багатоекстремальністю (багатомодальністю) та високою розмірністю простору пошуку. Представлена відповідна цільова функція, яка заснована на величині кореляції між прийнятим словом і вектором оцінок, а також штрафі, що враховує значення синдрому для даного вектору. Враховуючи наявні обмеження існуючих методів декодування та виходячи з особливостей цільової функції, для ефективного вирішення задачі декодування лінійних блокових кодів доцільно застосовувати стохастичні пошукові методи оптимізації. Клас таких методів називають поведінковими, інтелектуальними, натхненними природою, ройовими, популяційними і т.д. Розглянуто узагальнений підхід до формалізації основних принципів популяційних методів [2, с. 8 – 12]. Встановлено, що процес поведінки агентів залежить від детермінованих та стохастичних параметрів популяційних методів, що визначають його особливості і характеризують стан популяції в будь-який момент часу. Запропоновано метод ітеративного декодування лінійних блокових кодів, який заснований на процедурах стохастичної оптимізації [3, с. 27 – 28]. У процесі декодування згідно даного методу спочатку виконується жорстке рішення на основі прийнятого вектору, в результаті якого формується відповідний біполярний вектор. Якщо перевірочна умова задовольняється для кожного елементу даного вектору, то приймається рішення, що даний вектор є кодовим словом та процес декодування завершується. В противному випадку здійснюється пошук біполярного вектору з використанням популяційних методів до досягнення максимального числа ітерацій. Пошук завершується формуванням біполярного вектору, що забезпечує максимальне значення цільової функції та приймається у якості переданого кодового слова. Для визначення особливостей і характеристик запропонованого методу декодування кодів з малою щільністю перевірок на парність розроблені відповідні алгоритми та комп’ютерна модель.

Література:

1. Штомпель, Н. А. Вычислительная сложность методов декодирования кодов с малой плотностью проверок на четность [Текст] / Н. А. Штомпель // Системи обробки інформації: збірник наукових праць. – Харків: ХУПС ім. І. Кожедуба, 2013. – Вип. 6 (113). – С. 177 – 180.
2. Карпенко, А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой [Текст]: учебное пособие / А.П. Карпенко. – Москва: издательство МГТУ им. Н. Э. Баумана, 2014. – 446 с.
3. Асауленко, И. А. Метод итеративного декодирования линейных блоковых кодов на основе стохастической оптимизации [Текст] / И. А. Асауленко, С. И. Приходько, Н. А. Штомпель // Матеріали стендових доповідей та виступів учасників 28-ої міжнародної науково-практичної конференції «Інформаційно-керуючі системи на залізничному транспорті» (м. Харків, 24 – 25 вересня 2015 р.). – Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2015. – Вип. 4 (113). – С. 27 – 28.

Могилевський В.Б.
Аспірант каф. Комутаційних систем
Державний університет телекомунікацій
м. Київ, Україна

НАДІЙНІСТЬ ТА ПОКАЗНИКИ ЯКОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

Для забезпечення надійної роботи мереж зв'язку організовуються центри управління мережею (ЦУМ) і центри технічної експлуатації (ЦТЕ). Функціонування цих центрів неможливе без процесів виміру, збору і обробки контрольної інформації. ЦУМ забезпечують оперативне управління засобами і потоками повідомлень в умовах ситуації, що змінюється, з метою задоволення вимог за якістю обслуговування потоків інформації і досягнення максимальної пропускної спроможності мережі. ЦТЕ збільшують безперебійне функціонування мережі, здійснюють технічний контроль і діагностування відмов елементів мережі. ЦУМ працюють в тісному взаємозв'язку з ЦТЕ, використовуючи єдину систему контролю елементів мережі і збору службової інформації[1, с. 39].

В існуючих мережах зв'язку можна виділити наступні методи технічного обслуговування: профілактичний, відновлювальний і статистичний. Кожен з них має певні переваги і недоліки перед іншими, тому використовуються різні поєднання методів. Проте у зв'язку з підвищенням надійності все більшу перевагу в сучасних мережах зв'язку отримує статистичний метод обслуговування, суть якого полягає в тому, що ремонтно-відновлювальні роботи починаються після того, як якість функціонування досягла критичного значення. Дана методика дозволяє виключити багато видів дефектів, які зазвичай виникають при профілактичному обслуговуванні у зв'язку з демонтажем і іншими роботами, а в мережі і її елементах допустиме деяке число несправностей, що не приводять до припинення правильного функціонування завдяки наявності видів надмірності.

Доцільність застосування статистичного методу технічного обслуговування в мережах визначається в основному двома чинниками: розвиненою системою контролю і діагностування і використанням в елементах мережі високонадійної елементної бази. Функціонування мережі зв'язку відбувається в умовах постійної дії різного роду збурень, що приводить до виходу з ладу вихідного каналу і каналів зв'язку, виникненню помилок в повідомленнях, до випадкового характеру циркулюючих потоків інформації. У цих умовах завдання контролю і управління мережею полягає в забезпеченні передачі максимальної кількості інформації з необхідною якістю. Якість зв'язку практично повністю визначають три важливі властивості систем зв'язку – точність, надійність і вірність доставки інформації [2, с. 272].

Так під якістю повідомлень, що передаються за певний інтервал часу з необхідною якістю розуміється продуктивність мережі, а під максимально можливою продуктивністю – пропускна спроможність мережі. Вона залежить як від структури мережі, інтенсивності потоків повідомлень, вимог до якості їх обслуговування, так і в значній мірі від ефективності контролю і управління мережею. Оскільки пропускна спроможність мережі залежить від контролю і управління мережею, то слід розрізняти потенційну і реалізовану пропускну спроможності. Потенційна пропускна спроможність визначається в припущенні ідеальної системи контролю і управління, а реалізована – для реальної системи що вимагає накладних витрат. За відсутності контролю і зі збільшенням навантаження пропускна спроможність різко зменшується, особливо в умовах нестаціонарного характеру навантаження на мережу. Чим досконаліша система контролю і управління мережею, тим ближче реалізована пропускна спроможність до потенційної. В процесі функціонування мережі зв'язку необхідно забезпечувати задану якість з'єднань. Контроль відповідності кількісних параметрів полягає як в безпосередній оцінці критерію правильного функціонування, так і за результатами функціонального діагностування нижчеописаних рівнів доставки. Критерієм правильного функціонування для будь-якого режиму доставки є час безпомилкової доставки повідомлення. Контроль часу доставки повідомлення проводиться від моменту часу, коли перший знак вводиться вперше в мережу відправника, до моменту видачі одержувачу останнього знаку коректного повідомлення. Контроль безпомилковості включає перевірку коректності формату, перевірку відсутності в даних спотворень, що приймаються, вставок, випадань знаків або групи знаків, перевірку відсутності втрат, розмножень і засилань не за адресою[3, с 40].

Таким чином, основним вирішенням, для підвищення вимог до надійності та якості в телекомунікаційних та комп’ютерних мережах є зменшення складності об’єктів центра управління мережею (ЦУМ) та центрів технічної експлуатації (ЦТЕ). Передчасного розширення й удосконалення апаратури для розв’язку поставлених перед об’єктом ЦУМ задач. Статистична розробка рішення проблем якості і надійності мережі, при збільшенні навантаження з підвищенням користувачів. Автоматизація процесу діагностики мережі та подальшого усунення неполадок, для зменшення ролі обслуговуючого персоналу, що займається технічним обслуговуванням [4 с. 160].

Література:

1.Агаян А. А., Захаренко Г. П. Оптимизация структур цифровых сетей связи и технического обслуживания. — М.: Ин-т повышения квалификации руководящих работников и специалистов, 1987. – 39 с.

2. Губин Н. М., Матлин Г. М. Качествосвязи. Теория и практика. –М.: Радио и связь, 1986. – 272 с.

3. Захаренко Г. П., Иванов В. К. Эксплуатация цифровых сетей связи. Часть II. Основные задачи, понятия, определения. – М.: Ин-т повышения квалификации руководящих работников и специалистов, 1986. – 40 с.

4. Аринов М. Н., Присяжнюк С. П., Шарифов Р. А. Контроль и управление в сетяхпередачиданных с коммутациейпакетов. – Ташкент: Фан, 1988. – 160 с.

Срочинська Г.С.
Ст.викладач, аспірант каф. Інфокомунікацій
Довженко Н.М.
Ст.викладач, аспірантки каф. Інфокомунікацій
Державний університет телекомунікацій
м. Київ, Україна

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ QR-КОДУВАННЯ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ УКРАЇНИ

Міжнародні інтеграційні процеси і, перш за все, процеси науково-технологічного і економічного розвитку держави неможливі без впровадження в телекомунікаційну мережу тих технологій та процесів, що зможуть активізувати та підняти рівень послуг на більш вагомий щабель.

Україна не може конкурувати, а тим паче еволюціонувати, не використовуючи досвід світових телекомунікаційних лідерів; влада не може забезпечити стійкий розвиток держави, якщо не будуть введені механізми достовірного інформування користувачів, контролю та управління ресурсами життєдіяльності і бюджетом на всіх рівнях.

Інформація - це особливий вид капіталу країни, а тому, вона повинна бути насамперед доступною, коректно регульованою і вміло керованою. Збір, обробка, зберігання, використання та передача інформації забезпечують нормальну роботу ринку телекомунікацій. Головними вимогами до цього ринку являються: використання інформаційних технологій великої швидкодії, високої точності і надійності, автоматизації та системності.

В умовах конкурентного середовища, значна частина інформації повинна бути оперативною, а також недоступною для її використання нерегламентованими користувачами. Тому більшість інформаційних технологій базуються на зберіганні і передаванні інформації в закодованому вигляді. Одним із кращих, сучасних рішень для інтегрованих телекомунікаційних мереж, є технологія QR-кодування.

На сьогоднішній день, ця технологія використовується банківському секторі економіки, в рекламі, торгівлі, логістиці, туризмі, інтернет-магазинах з метою максимальної економії часу клієнтів та онлайн-покупців. Однак поява вУкраїні нових технологій опрацювання інформації не означає, що вони відразу отримають широкого впровадження.

QR-код (Quick Response Code, 2D Code) –двовимірний (матричний) штрих-код, розроблений японською компанією Denso-Wawe у 1994 році. Абревіатура QR перекладається як “швидка відповідь”. Основна перевага QR-коду – це легке його розпізнавання сканувальним обладнанням, що дає можливість використання коду в багатьох сферах. Для зчитування інформації з QR-коду потрібен мобільний телефон, смартфон чи планшет з камерою і спеціальне програмне забезпечення, яке розповсюджується безкоштовно через мережу Інтернет. Вибір програми диктується типом операційної системи, встановленої на мобільному пристрої. Для Android – це I-Nigma, Google Goggles, QuickMark, Barcode Scanner, Barcode2file, QR Droid, NeoReader, ixMAT Scanner, 2D-код, Elinext UPC; для Java –Kaywa Reader, I-Nigma, UpCode; для Symbian OS – QuickMark, Kaywa reader, Nokia barcode reader, I-Nigma, UpCode, NeoReader, BeeTag; для Windows Mobile –QuickMark, I-Nigma; для Bada – BeeTagg, Quick QR Reader таін. Для деяких операційних систем програми зчитування QR-кодів є вбудовані в магазини додатків для портативних пристроїв [1].

QR-коди не прив’язані до конкретного формату даних, тобто до усталеного стандарту запису інформації у файлі. Програми перегляду QR- кодів розпізнають текст, графічні зображення, інформацію веб-сторінок, E-mail, SMS, номери телефонів, географічні координати та іншу інформацію. Тип інформації вказується при генеруванні QR-коду. Щоб отримати інформацію безпосередньо на екран мобільного телефона, достатньо запустити програму для сканування коду і навести об’єктив камери на код. Програма-декодер розпізнає тип інформації і виконає потрібні дії, наприклад відкриє веб-сторінку (в цьому випадку потрібне ще з’єднання з інтернет).

Для максимального комфорту та швидкості отриманні інформації, QR-код розміщується на: web-сайтах, сторінках блогів, в періодичних виданнях, на туристичних об’єктах, плакатах, на одязі, в музеях, на сувенірах, і т.д. QR-код виконує дві функції: вміщує велику кількість інформації у невеликій картинці (більше двох друкованих сторінок) і дозволяє автоматично зчитувати закодовані дані. Даний код є унікальним в своєму вигляді. Будучи дуже простим, зручним у використанні, а також допомагаючи оперативно отримувати і розповсюджувати інформацію інтерактивним шляхом, саме цей код набув широкого застосування.

Сучасні мобільні телефони, смартфони і планшети мають вбудоване програмне забезпечення для зчитування і розпізнавання QR-коду. Після сканування камероюмобільного пристрою програма, встановлена на ньому, розпізнає вид інформації, що зберігається в QR-коді. Якщо це адреса сайту – відкриває його браузером, якщо електронна візитна картка – додає нову контактну особу в телефонну книгу, якщо звичайний текст – виводить його на екран.

Але враховуючи всі переваги використання, важливо також відмітити і загальні проблеми із якими зіштовхуються користувачі.

Особливості функціонування

QR-код завжди має форму квадрата (матриці) і відрізняється від звичайних штрих-кодів розміщенням інформації в двох напрямах – вертикальному і горизонтальному. Менші квадрати і чорні лінії містять інформацію, яка зберігається в модулях. Кількість модулів залежить від об’єму закодованих даних.

Перша версія QR-коду (найменший код) має розмір 21×21 піксель і 441 модуль, версія 40 (найбільший код) – 177×177 пікселів і 31 329 модулів. Завдяки цьому збільшується максимальна кількість інформації, яку вміщає один QR-код: цифри – 7089, цифри і літери (включно з кирилицею) – 4296, двійковий код – 2953 байт, ієрогліфи – 1817 [2].

Існує мікроQR-код ємністю до 35 цифр, його використовують для розміщення коду на невеликій площі, наприклад на запальничці чи сувенірному брелку. Кількість інформації, яку вміщує мікро QR-код невелика, але в ньому можна закодувати номер телефону чи коротку URL-адресу. Також використовується псевдо-кодування – задання методу кодування даних або розбиття довгого повідомлення на кілька кодів тощо. Розмір QR-коду може бути будь-яким, але для зручності читання і розпізнавання довжина кожної сторони повинна бути не меншою за 2,5 см.

Для зчитування кодів меншого розміру потрібні більш високоточні скануючі пристрої, ніж сучасні смартфони і планшети. На відміну від одновимірного штрих-коду, який сканують тонким променем, QR-код визначається сенсором як двовимірне зображення, але зчитувати його можна в будь-якому напрямку. Три великі квадрати в кутах зображення та контрольна точка поблизу четвертого кута дозволяють при зчитуванні нормалізувати розмір зображення і його орієнтацію, а також кут, під яким камера – зчитувач розташована до поверхні зображення.

QR код можна прочитати і “вручну” без смартфона, для цього слід знати особливості QR-кодів і алгоритм дешифрування інформації [1]. Оскільки є багато готових і безкоштовних програм для генерування QR-кодів та їх розпізнавання, необхідності в цьому немає.

Алгоритмом декодування може бути будь-який відомий та прийнятий, адже QR-код використовує двійкове кодування інформації: чорні квадратики кодуються одиницями, білі – нулями. Крім того, для виявлення і виправлення помилок при декодуванні виконується перевірка контрольних сум з використанням операції XOR (додавання бітів коду за модулем два до спеціальної восьми бітової двійкової маскою, наприклад 10101010). Завдяки виправленню помилок на код можна нанести рисунок, зробити його кольоровим та різнокольоровим – він залишиться читабельним. Розрізняють статичні та динамічні QR-коди.

Статичний QR-код містить інформацію, яку вказали при його генеруванні. Динамічний QR-код є багатофункціональним: до нього можна підключати додаткові функції, які будуть виконуватися одночасно чи змінити їх. Різновидами QR-кодів є DataMatrix та Aztec Code. QR-коди можуть легко генеруватись з використанням вільно розповсюджуваного програмного забезпечення [3].Альтернативними QR-кодуванню технологіями є Sonic Notify, RFID-мітки та NFC.

Література:

1. Вячеслав Логачев. Что несет QR-код -http://www. ridcom.ru/publications/131/.

2. Anna Skryabina. 20 способов использования QR-кодов.— http://computers-the.ru/?p=211/.

3.Читаем QR код - : http://habrahabr.ru/post/127197/.

Штомпель Н.А.
Доцент каф. Транспортной связи
Украинский государственный университет железнодорожного транспорта
г. Харьков, Украина

ОПТИМИЗАЦИЯ КАСКАДНЫХ БЛОКОВЫХ КОДОВ НА ОСНОВЕ ПОПУЛЯЦИОННЫХ МЕТОДОВ

При построении телекоммуникационных систем важной задачей является обеспечение заданной достоверности передачи информации. Для решения данной задачи применяются различные методы помехоустойчивого кодирования. Для снижения вычислительной сложности процесса декодирования целесообразно применять каскадные блоковые коды, которые по своим характеристикам близки к турбо-кодам, использующим в качестве составляющих рекурсивные сверточные коды [1, с. 275]. При построении последовательных и параллельных каскадных кодовых конструкций широко применяются перемежители, назначение которых заключается во внесении в структуру кода некоторой степени случайности для улучшения его корректирующей способности. Исходя из требований, предъявляемых к перемежителям рассмотренных видов каскадных блоковых кодов, сформулированы соответствующие оптимизационные задачи, представлены целевые функции и введены необходимые ограничения. Предложен подход к построению перемежителей на основе популяционных методов оптимизации, которые целесообразно применять для решения оптимизационных задач с данными характеристиками [2, с. 8 – 10]. Для оценки эффективности предложенного подхода к оптимизации каскадных блоковых кодов разработаны вычислительные алгоритмы, реализующие основные этапы предложенного метода построения перемежителей. На основе данных алгоритмов в специализированной среде моделирования создана программная реализация телекоммуникационной системы, использующей данный класс каскадных кодовых конструкций. В результате проведения моделирования для некоторых моделей каналов связи определены особенности и характеристики полученных каскадных блоковых кодов.

Литература:

1. Штомпель, М.А. Розвиток методів завадостійкого кодування у волоконно-оптичних телекомунікаційних системах [Текст] / М.А. Штомпель// 75-та міжнародна науково-технічна конференція кафедр академії, інженерно-технічних працівників залізниць, підприємств та організацій України та інших країн (м. Харків, 24 – 25 квітня 2013 р.). – Тези доповідей. – Збірник наукових праць Української державної академії залізничного транспорту. – Харків: УкрДАЗТ, 2013. – № 136. – С. 275.

2. Карпенко, А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой [Текст]: учебное пособие/ А.П. Карпенко. – Москва: издательство МГТУ им. Н. Э. Баумана, 2014. – 446 с.

Ярцев В.П.
К.т.н.,доцент каф. Вычислительной техника
Государственный университет телекоммуникаций
г. Киев, Украина

СНИЖЕНИЕ ВЛИЯНИЯ МЕЖСИМВОЛЬНОЙ ИНТЕРФЕРЕНЦИИ НА КАЧЕСТВО ПЕРЕДАЧИ ЦИФРОВИХ СИГНАЛОВ С КВАДРАТУРНОЙ АМПЛИТУДНОЙ МОДУЛЯЦИЕЙ

Современные достижения радиоэлектроники обеспечивают возможность реализовать в системе связи достаточно сложные алгоритмы цифровой обработки сигналов. При этом качество передачи сообщений в цифровых системах оказывается выше, чем в аналоговых, при этом возможна передача сигналов в условиях воздействия различных естественных шумов и искусственно созданныхпомех с заданными параметрами качества и большей точностью.

В современных цифровых системах передачи широко применяются фазовый, частотный и с расширением спектра методы цифровой модуляции. Частотная модуляция передаваемого сигнала выполняется с помощью двоичной частотной манипуляции, частотной манипуляции с минимальным сдвигом, Гауссовой частотной манипуляции с минимальным сдвигом, сигналов с постоянной огибающей, М-ичной частотной модуляцией и квадратурной амплитудной модуляцией.

При квадратурной амплитудной модуляции (КАМ) дискретно и конечно изменяются значения амплитуды и начальной фазы каждого канального символа.

Ширина спектра КАМ - сигнала примерно такая же, как и М-ичного ФМ сигнала. Однако данный способ модуляции может обеспечить меньшую вероятность ошибки на бит передаваемой информации и поэтому оказывается более предпочтительным. Следует отметить, что, так как КАМ - сигнал не имеет постоянной амплитуды, то применение этого способа модуляции сопровождается повышением требований к линейности канала передачи. Для передачи информации по телефонному каналу длительность сигнала, соответствующая каждому символу, должна многократно превышать длительность символьного интервала, при этом спектры сигналы соседних символов накладываются друг на друга, вызывая межсимвольную интерференцию (МСИ), что снижает достоверность приема передаваемого сообщения. Для снижения МСИ квадратурным сигналам придают специальную форму, обеспечивая нулевые значения сигнала в моменты времениТ, равные интервалу, выделяемого для передачи одного символа.Это достигается путем использования фильтров нижних частот (ФНЧ) с косинусоидальным сглаживанием АЧХ$|A(f)|$- фильтр Найквиста. Так как фильтрация нижних частот применяется на передающей и на приемной сторонесистемы связи, используется фильтр АЧХ которого равна корню квадратному АЧХ фильтра Найквиста $\sqrt[2]{|A(f)|}$ [1,2].

При увеличении скорости передачи сообщений за счет использования большего числа символов $\boldsymbol{n}$ при фиксированной символьной частоте$\boldsymbol{f_s}= \boldsymbol{1/T}$, число точек в сигнальном созвездии увеличивается в $\boldsymbol{2^n}$раз,а расстояние между ними уменьшается. Это вызывает необходимость повысить качество демодуляции сигнала в приемнике за счет увеличения точности синхронизации несущей частоты и точности формирования отсчетных моментов времени$\boldsymbol{T}$, а также компенсации искажений КАМ - сигнала в канале связи. Эти операции (carrierrecovery, timingrecovery, equalization) решаются схемотехнически или алгоритмически в блоках приемника, реализующих методы автоматического регулирования с обратными связями. Поэтому для повышения эффективности и устойчивости системы управления необходимо до выполнения этих операций обеспечить предварительную частотную и временную синхронизацию приемника, получить информацию о параметрах искажений сигнала.

Предлагается для настройки приемника КАМ- сигнала использовать несколько серий обучающих последовательностей символов, которые состоят из повторяющихся комбинаций используемых символов или их псевдослучайной последовательности с длинной в пределах от256T до1280T[3]. С помощью обучающих серий можно получить сведения о частотных и временных параметрах КАМ – сигнала без использования операции демодуляции при обработке повторяющихся комбинаций используемых символов. Обработка серий с псевдослучайной последовательностью символов с их демодуляцией и сопоставление с априорной известными значениями позволяет выполнить адаптацию приемного устройства и соответственно значительно уменьшить межсимвольную интерференцию КАМ - сигналов.

Литература:

1. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. 2-е изд.: пер. с англ. – М: Вильямс.2003. -1104 с.
2. Сергиенко А.Б. Цифровая обработка сигналов. – СПб: Питер. 2003. - 604 с.
3. Миленький А.В., Сундучков А.К. Оптимизация начального этапа синхронизации приемника КАМ – сигналов /Вісник Державного університету інформаційно-комунікаційних технологій. 2004. Том2,№4. – С.186-191.
4. Jablon N.K. Carrier recovery for blind equalization// Proc.IEEE Int.Conf.Acoust. Speech.Signal Processing. May 23-26.1999. –P. 1211-1214.

Молчанов А. І.
Студент ФІТ
Хорунжий О.І.
Доцент каф. Інформаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

МОДЕРНІЗАЦІЯТЕЛЕФОННОЇ МЕРЕЖІ ЗАГАЛЬНОГО КОРИСТУВАННЯ СЕРЕДНЬОГО МІСТА

Метою модернізації є розвиток телекомунікаційної мережі з мінімальним ризиком для оператора зв'язку з точки зоруможливихвтрат. При цьому потрібно надавати послуги користувачам протягом будь-якого етапу модернізації з мінімальним часом простою мережі, а також у разінеобхідності, призупинити процес модернізації без суттєвих фінансових втрат. Такий підхід є найбільш ефективним у ситуації, яку ми зараз спостерігаємо у нашійкраїні.

Для модернізації існуючої телефонної мережі загального користування у місті середнього розміру в мережу нового покоління (NGN) пропонується використати два базових принципи.

Перший -поетапнамодернізація, що дає можливість надавати послуги користувачам протягом будь-якого етапу з мінімальним часом простою мережі, а також у разі необхідності, призупинити процес модернізації без суттєвих фінансових втрат.

Другий -заміна старої АТС на мультисервісний вузол доступу [1], який забезпечить усіх раніше підключених абонентів окрім послуги телефонного зв`язку, послугою інтернет. Універсальні можливості такого вузла дозволяють використовувати старі лінії зв'язку та забезпечують можливість підключення до наявного обладнання різних поколінь. Головною перевагоювузла є йогоуніверсальність, яка проявляється не лише у кількостітипівпідключення, але і у можливостіпідключення до будь-якоїтехнології доступу. До того ж кількістьпослуг, яку моженадаватитакийвузол, залежить не від самого вузла, а відпідсистеминаданняпослуг, оскількивузолвиконуєлишетранспортнуфункцію.

У якості прикладу розробленопроект модернізації існуючої телефонної мережі загального користування у містіПрилуки. При цьому було запропоновано використати обладнання SmartAXMA5600T компанії Huawei[1], яке повністю інтегрується як в існуючу телефонну мережу загального користування, так і в мережу наступного покоління NGN. У якості додаткового обладнання використовуються мультиплексори типу «IPmux 16» та комутатори типу «PlanetFNSW - 2401» для виконання підключення абонентів телефонії до мережі та раціонального використання пропускної здатності модуля. Розрахованонеобхіднукількістьобладнання для наданнякористувачампослуг з урахуванням запасу на розвиток. Розглянемоможливості та функції старого і нового обладнання.

Таблиця 1 Порівняльна характеристика можливостей АТСДК та мультисервісного вузла доступу

Характеристика	АТСДК-54	MA5600T
Тип обладнання	Аналогове	Цифрове
Тип комутації	Каналів	Пакетів
Ємність	9400 телефонних)	3688 (мультисервісних) 1383000 (телефонних)
Крок озширення ємності	100	Від 16 до 64 иультисервісних)
Можливе озміщення в мережах	ТмЗК	ТмЗК, IP/MPLS, ATM,)DN

ФункціїАТСДК-54: комутаціяканалів, забезпеченнясигналізації, забезпеченнясинхронізації.

Функції MA5600T:

Високопродуктивніслужбибагатоадресноїрозсилки:

Підтримуютьсястекипротоколів IGMPv2 і IGMPv3;

IPTV;

MulticastVLANна основі програми та управління користувачами;

4096 програми;

до 8000 мультисервісних користувачів;

Розподілене групування;

Голосовий сервіс:

VoIP;

Взаємодія із Softswitch в мережі NGN через протокол H.248 або SIP, надаючи користувачам сервіс VoIP (у тому числі послуг голосового, факсимільного і модемного зв`язку);

Підключення до мережі IMS через SIP, реалізації послуги VoIP (у тому числі послуг голосового, факсимільного і модемного зв`язку).

Підтримує реконструкцію традиційних голосових потоків, таких як N * 64K приватні лінії пристрою ISDN PRI АТС, що реалізує архітектуру ВСЕ IP.

Підтримує підключення N * 64K приватних ліній пристрою і ISDN PRI АТС через TDM SHDSL модем.

підтримує перетворення ISDN PRI АТС потоків трафіку вIP-пакети для передачі через вхідний контроль програмних комутаторів, а також підтримує перетворення Н * 64K приватним лініях потоків трафіку в TDM-пакетів для висхідної передачі в мережу SDH. Потоки приватних ліній SHDSL трафіку можуть бути перетворені в пакети IP для висхідної передачі при комутації, або перетворені в пакети TDM для висхідної передачі в мережі SDH.

сумісність з усіма NGN / IBC

Мобільного транспорту:

Здійснює рішення доступу базової станції за допомогою(OLT) + MDU;

Підтримка синхронізації часу в разі доступу базової станції;

MPLS PWE3 забезпечує надійність E2E;

Функція захисту мережі;

Підтримує протокол MSTP, і функцію захисту контуру;

Підтримує протокол RRPP реалізації швидкого перемикання до кільцевої мережі;

Підтримує протокол LACP та настільні функції агрегації, збільшення пропускної спроможності та забезпечення функції захисту;

Підтримка двобічного виявлення переадресації (BFD), підвищення надійності додатків IP (наприклад, голосовий сервіс в режимі реального часу) і надання підтримки в мережі стабільності для постачальників послуг;

Підтримка смарт-додатка, який реалізує резервне копіювання і швидке резервування, міграцію активних і резервних зв'язків, забезпечення високої надійності і високої швидкості;

Функція QoS:

Мітки даних і керування мережею потоків з різними пріоритетами ToS/DSCP, тим самим забезпечуючи пріоритетний механізм переадресації на основі 3 рівня;

Мітки даних і керування мережею потоків з різними пріоритетами 802.1p, тим самим забезпечуючи пріоритетний механізм переадресації на основі 2 рівня;

Підтримка рівнів з 2 по 7 класифікаціїтрафіку на основі портів, VLAN, MAC-адресу, IP-адреса, номер TCP порту або UDP номера порту;

Підтримка пріоритету управління (на основі порту, MAC-адреси, IP-адресу, номер порту TCP, UDP або номер порту), пріоритет відображення і модифікації на основі області ToS і 802.1p, DSCP;

Підтримка управління смугою пропускання (на основі порту, MAC-адреси, IP-адреси, номера порту TCP або UDP) з контрольною деталізацією 64 кбіт/с;

Підтримує три режими планування черг: пріоритетної черги (PQ), WeightedRoundRobin (WRR), та PQ + WRR.

Підтримка можливостей QoS на основі верховенства потоку.

Запропоновані принципи модернізації є універсальними. Їх можна використовувати для будь-якого покоління обладнання та стану фізичнихлінійзв`язку.

Література:

1. SmartAX MA5600T/MA5603T Multi-service Access Module V800R011C00 Product Description, 2012

2. Електроннабазаданихзнань, http://allbest.ru

Якименко Ю.М.
Доцент каф.Управления информационной безопасностью
Государственный университет телекоммуникаций
г. Киев, Украина

ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Бурное развитие средств вычислительной техники и интенсивное оснащение ими практически всех государственных и негосударственных организаций накладывает огромную ответственность на соответствующих руководителей за их эффективное использование и, прежде всего, по обеспечению выполнения возложенных на них задач.

Создание большого числа разного рода автоматизированных информационных и управляющих систем привело к возникновению принципиально новых, так называемых, информационных технологий.

В своей повседневной деятельности в организации имеет место в обращении большие объемы конфиденциальной информации, которые имеют тенденцию к росту (к тому же еёстоимость в большинстве случав уже в десятки – сотни раз превышает стоимостьсамих компьютерных систем). Искажение или фальсификация, уничтожение или разглашение определенной части информации, равнозначно как и нарушение процессов ее обработки и передачи в информационных и управляющих системах наносят ощутимый ущерб активам организации и могут привести к её полнейшему краху. Современные злоумышленникив основном ознакомлены с достоинствами и слабыми местами практически всех вычислительных систем и для достижения своих целей используют самые совершенные инструментальные и технологические средства для анализа и взлома механизмов их защиты.Применяемые в настоящее время в системах обработки информации организационные меры и особенно аппаратно-программные средства защиты не всегда могут обеспечить достаточную степень безопасности субъектов, участвующих в процессах информационного взаимодействия.

Исследования проблемы обеспечения безопасности компьютерных систем ведутся как в направлении раскрытия природы явлений, заключающиеся в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерной системы, так и в направлении разработки конкретных практических методов и средств их защиты. Необходимость исследования процессов, именно информационной безопасности, эффективного управленияими, выдвигает насущные требования к использованию имеющихся методик и моделей в этой области (особенно, оценки состояния уже существующих в организациях компьютерных систем) , а при необходимости - и созданию новейших инструментов.

При решении многих прикладных задач, связанных ссозданием систем защитыинформации, приходится сталкиваться с неопределенностью в исходных данных, к которым относятся:

неполнота и неопределенность исходной информации о составе информационной системы и характерныхугрозах;

многокритериальность задачи, связанная с необходимостью учетабольшого числа частных показателей (требований) средств защиты информации;

наличие как количественных, так и качественных показателей, которые необходимо учитывать при решениизадач разработки и внедрения систем защиты информации;

невозможность применения классически хметодов оптимизации.

Основным методом исследования систем защиты информации является моделирование. Моделирование предусматривает создание модели и её использование для исследований (анализа).

Неполнота информации и неточность исходных данных для используемых моделей неизбежно приводят к ошибкам выходных данных - до 80 процентов от общего их количества [1,с.22].

Судя по растущему количеству публикаций, посвященных обсуждаемой проблеме - исследованию систем защиты информации, все большее число исследователей склоняется к тому, что *в реальном математическом моделировании* наиболее целесообразным подходом можно считать представление исходных данных в виде нечетких множеств или интервальных значений.

Проблема неопределенности цели *также должна приниматься во внимание при математическом моделировании, и прежде всего, учёт противоречий в требованиях, например* - при минимуме затрат добиться максимума выпуска продукции или качества оказываемых услуг.

Таким образом, в рамках дискретной оптимизации можно говорить о самостоятельном направлении дискретного программирования для решения многокритериальных задач, связанных с обеспечением информационной безопасности. Однако, пока ещё не создан и неизвестен эффективный алгоритм решения какой-либо многокритериальной задачи с нечеткими данными.

Поэтому при исследовании дискретной многокритериальной задачи в качестве основной математической проблемы обычно рассматривается *вопрос построения достаточно эффективного алгоритма нахождения требуемого* множества альтернатив *этой задачи, с последующим* выбором оптимального варианта и принятием решения.

Практически задача обеспечения информационной безопасности заключаетсяв *разработке модели представления системы (процессов) информационной безопасности*, которая на основенаучно-методического аппарата, позволила бы решать *задачи создания, использования и оценки эффективности*средств защиты информации для проектируемых и существующих информационных системлюбойорганизации.

Система информационной безопасности может быть представлена в виде упрощенной модели процессов информационной безопасности: математический аппарат, набор методик и программные средства[2,с.23].

Основной задачей такой модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Определённый опыт исследования безопасности информационных систем уже имеется и отражён в работахВ.В. Домарева [2;3,с.516,567]. Используемая модельдля оценки средств защиты информациидля проведения исследований позволяет:

- установить взаимосвязь между показателями (требованиями);
- задавать различные уровни защиты (безопасности);
- получать количественные оценки;
- контролировать состояние системы защиты информации;
- применять различные методики оценок.

Решение задачи защиты информации с точки зрения системного подхода можно сформулировать как трансформацию существующей системы, не обеспечивающей требуемый уровень защищенности, в систему с заданным уровнем безопасности информации.

Литература:

1. Моделирование систем и процессов защиты информации в условиях неполноты и недостоверности данных.- [Электронный ресурс]: статья / Режим доступа:http://knowledge.allbest.ru/programming/2c0b65625b3bc78b5c53b89521316c27_0.htm.

2. Домарев В.В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД «Диасофт», 2004. – 992 с.

3.Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО ТИД «Диасофт», 2002. - 688с.

Лобанов Л. П.
Доцент каф. Вычислительной техники
Котомчак А. Ю.
Ст.преподаватель каф.Вычислительной техники
Государственный университет телекоммуникаций
г. Киев, Украина

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ АВТОМАТОВ С ЦЕЛЕСООБРАЗНЫМ ПОВЕДЕНИЕМ

Автоматы с целесообразным поведением (АЦП) находят применение при решении задач поискового характера и принятия решения. Качество функционирования АЦП принято оценивать величиной математического ожидания штрафа (или нештрафа). Анализ известных конструкций АЦП показал, что указанный параметр не в полной мере отражает качество функционирования. В работах[1, с.51;2,с.76;3,с.484] утверждается, что АЦП обладает оптимальным поведением во всех случайных средах, если оценивать качество поведения на величине математического ожидания штрафа. Реально АЦП обладают оптимальным поведением в средах только с определенными параметрами (табл. 1).

Таблица 1

Тип АЦП	Область 1	Область 2
Цетлина	*p1 < 1/2*	*p2 > 1/2*
Крылова	*p1< 2/3*	*p2 >2/3*
Кринского	*p1 < k/(k+1)*	*p2 > k/(k+1)*
Вавилова	*p1 < k/(k+m)*	*p2 > k/(k+m)*

где *p1,p2* – вероятности штрафа в областях 1,2,

k – величина скачка под штрафом,

m– величина скачка под нештрафом.

Приведенные результаты получен при условии, что качество поведения АЦП оценивают по такому параметру как скорость изменения числа состояний при функционировании за один такт, который однозначно определяется структурой АЦП и величинами вероятностей штрафа в областях. Скорость изменения состояния за один такт может быть использована для определения структур АЦП, обладающей оптимальным поведением в заданной случайной среде. Структура определяется из выражения:

$$\alpha 1 = \frac{k}{m} = \frac{1}{\sqrt{q1 * q2}} - 1, \qquad (1)$$

где $q1 = 1 - p1$,

$q2 = 1 - p2$

Наиболее близок к полученной структуре АЦП Вавилова Е. Н.[4,с.42], который определяется по критерию максимума правдоподобия из выражения (2)

$$\alpha 2 = \frac{k}{m} = \frac{ln\frac{q_2}{q_1}}{ln\frac{p_2}{p_1}}, \qquad (2)$$

Таблица 2 демонстрирует близость результатов, полученным по выражениям (1) и (2) для конкретных значений p_1иp_2.

Таблица 2

p_1=0.9	p_2	0.1	0.2	0.3	0.4	05	0.6	0.7	0.8
	α_1	2.33	2.34	2.78	3.28	3.47	4.00	4.77	6.07
	α_2	1.00	1.38	1.77	2.21	2.78	3.42	4.37	5.89

Литература:

1. Цетлин М. Л. Исследование по теории автоматов и моделирование биологических систем. М., Наука, 1981.

2. Крылов В. Ю. Об одном стохастическом автомате асимптотически оптимальном в случайной среде. ж. Автоматика и телемеханика, XXIV, №9, 1963

3.Кринский В. И. Асимптотически оптимальный автомат с экспоненциальной скоростью сходимости. ж. Биофизика, 1964, №8, вып.4.

4.Андрющенко В. А., Вавилов Е. Н., Лобанов Л. П. Синтез автоматов, асимптотически оптимальных в стационарных случайных средах. Ж. Кибернетика,1972, №1

Котомчак О. Ю.

Ст.викладач каф. Обчислювальної техніки

Державний університет телекомунікацій

Кононов М. В.

Доцент факультет Радіофізики, електроніки та комп'ютерних систем

Київський Національний університет ім. Тараса Шевченка

м. Київ, Україна

ПОЛІМЕРНІ КОМПОЗИЦІЙНІ МАТЕРІАЛИ ДЛЯ КВЧ ЕЛЕКТРОНІКИ

Розвиток сучаснихзасобів передачі інформації потребує сучасних матеріалів, які за своїми якостями (міцністю, пружністю, електрофізичними властивостями) переважають існуючі. Одними з перспективних є композиційні полімерні матеріали. Такі матеріали складаються з полімеру, який є сполучавачем та наповнювача, який є армуючим компонентом. Для застосування в інтегральних схемах такі матеріали повинні мати окрім міцності та пружності певні електрофізичні властивості - діелектричні втратиtg δ= $(1\div10)*\ 10^{-4}$ та регульовану діелектричну проникність $\varepsilon=(2\div10)$. Для отримання матеріалів, які задовольняють вказаним умовам використовують композити, вихідними компонентами яких є неполярні поліолефіни з $\varepsilon=(1{,}8\div2{,}4)$, tg $\delta= 2*\ 10^{-4}$[1, с.525] та дрібнодисперсні термостабільні наповнювачі з $\varepsilon=(10\div80)$, tg $\delta= 5*\ 10^{-4}$, такі як TiO_2, Al_2O_3, MgO, GaAs [2. С.206]. Для отримання однорідної структури використовують традиційні методи змішування компонентів в розплаві та у порошкоподібному стані. З отриманого однорідного пластичного композиту формується пластина розрахованої товщини, зякої згодом за допомогою прес-форми формуютьсядіелектричні хвилеводи та резонатори для КВЧ діапазону. Активні напівпровідникові елементи, наприклад ЛПД (лавино-пролітні діоди), додаються до вже сформованої конструкції полімерної композитної планарної структури. За вищенаведеною технологією було експериментально створена генераторна секція з вихідною потужністю ≈10мВт в діапазоні 120÷140 Ггц, та потужністю ≈ 100 мВт в діапазоні 40÷50Ггц. А також за аналогічною методикою була розроблена детекторна секція з чутливістю 0,25 кВ/Вт в діапазоні 120÷140 Ггц, та 1,5 кВ/Вт в діапазоні 40÷50Ггц відповідно.

Література:

1. О. Уайэтт, Д.,Дью-Хьюз. Металлы, керамики, полимеры. М., Атомиздат, 1979.

2. В. А. Пахаренко, Р. А. Яковлева, А. В. Пахаренко. Переработка полимерных композиционных матариалов.Киев: Издательскаякомпания «Воля», 2006.

Вишнівський В.В.

Д.т.н., професор, зав. каф. Інформаційцних технологій

Гайдур Г.І.

к.т.н., доцент каф. Інформаційцних технологій

Державний університет телекомунікацій

м. Київ, Україна

ГЛОБАЛЬНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА - ОСНОВА ДЛЯ СТВОРЕННЯ ЄДИНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Сучасний етап розвитку світової цивілізації характеризується переходом від індустріального до інформаційного суспільства. Такий перехід передбачає наявність нових форм соціальної та економічної діяльності, що базуються на масовому використанні інформаційних і телекомунікаційних технологій. Стрімкий розвиток науково-технічного прогресу в світі супроводжується зростанням науково-технічних знань і інформації в результаті людством накопичений величезний об'єм інформації, усвідомлена цінність інформації, її важливість в забезпеченні життєдіяльності суспільства. Інформаційне суспільство це нове поняття, нова суспільно-політико-економічна категорія, яка характеризує новий ступінь в розвитку людської цивілізації. Інформаційне суспільство має глобальний характер, воно об'єднує інформаційні ресурси всіх країн в єдину всесвітню інформаційну систему, доступ до якої буде можливий в будь-якому місці Землі, будь-якому члену світової спільноти.

Глобальна інформаційна інфраструктура є новим поняттям в зв'язку і інформатиці. Вона пішла від ідеї "національної інформаційної інфраструктури (НІІ)” розробленої в рамках ініціативи Клінтона - Гора, висунутою Адміністрацією США в 1993 р. і проголошеної в 1994 р. в Буенос-Айресі на зборах Міжнародного Союзу Електрозв’язку ООН. Метою НІІ, як було сформульоване в пропозиціях Адміністрації США, є створення "мережі мереж" (тобто об'єднання мереж електрозв'язку, комп'ютерних мереж, баз даних і побутової електроніки). Таку мережу американці назвали “супер-магистраль".

Технологічна мета НІІ була пов'язана з політичними і економічними інтересами. Завдяки НІІ, США мають намір створити нові робочі місця, успішно конкурувати в глобальній економіці.

Ідея НІІ була розвинута в ідею Глобальної інформаційної інфраструктури, розробка якої стала задачею Організації Об'єднаних Націй (Міжнародного союзу електрозв'язку і його 13-й Дослідницької комісії)

Технологічною основою інформаційного суспільства є Глобальна Інформаційна Інфраструктура, яка повинна забезпечити можливість доступу до інформаційних ресурсів кожного жителя планети без дискримінації. Інформаційну інфраструктуру становить сукупність баз даних, засобів обробки інформації, взаємодіючих мереж зв'язку і терміналів користувача.

Доступ до інформаційних ресурсів Глобальної інформаційної інфраструктури реалізується за допомогою послуг зв'язку нового типу, що одержали назву послуг Інформаційного суспільства або інфокомунікаційних послуг. Інфокомунікаційною послугою називається послуга електрозв'язку, що припускає автоматизовану обробку, зберігання або надання інформації за запитом з використанням засобів обчислювальної техніки, як на вхідному, так і на вихідному кінці з'єднання.

В даний час спостерігаються високі темпи зростання обсягів надання інфокомунікаційних послуг дозволяють прогнозувати їх перевагу на мережах зв'язку в найближчому майбутньому.

На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках Internet, доступ до послуг якої забезпечується через традиційні мережі зв'язку. У той же час, у ряді випадків послуги Internet, зважаючи на обмежені можливостей її транспортної інфраструктури, не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим, розвиток інфокомунікаційних послуг вимагає вирішення завдань ефективного управлінні інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу, це стимулює процес інтеграції Internet і традиційних мереж зв'язку.

Глобальної інформаційної інфраструктури з погляду користувача складається з: терміналу користувача; телефонної мережи загального користування, локальної обчислювальної мережі; цифрової мережі з інтеграцією служб, телевізійне мовлення, звукове мовлення.

Рушійною силою напрямка технічного розвитку Глобальної інформаційної інфраструктури є: нове середовище та цифровізація. Тому основним напрямком технічного розвитку є конвергенція мереж, яка передбачає використовувати нові мережні технології. Це забезпечить дерегуляцію інформаційного бізнесу.

Стандарти глобальної інформаційної інфраструктури повинні забезпечити можливість взаємодії і взаємозв'язку як з орієнтацією на з'єднання так і без орієнтації на з'єднання між великою різноманітністю додатків і різних платформ.

Телекомунікаційні мережі, що використовують різні технології в даний час забезпечують передачу даних і мови з високою якістю і взаємодіють один з одним.

Мережі з протоколами TCP / IP створюють платформу, яка дозволяє користувачам, пов'язаним з різними мережними інфраструктурами, мати загальний набір додатків і обмінюватися потоками даних, якість доставки яких не гарантується. Стек протоколів TCP / IP вдосконалюється (наприклад, IPv6) з метою підтримки додатків голосу, відео, мультимедіа підвищеної якості.

Технології з комутацією пакетів (що раніше були не орієнтовані на встановлення з'єднань), наприклад, використовують протокол IP, удосконалюються з метою підвищення якості доставки інформації, завдяки попередньому встановленню віртуальних з'єднань.

Вузли мереж з комутацією каналів будуть обмінюватися інформацією через транспортні мережі нового покоління з КП, що призведе до зниження якості доставки інформації, чутливої до затримки, джиттеру і втрат пакетів.

Мережі з технологією ATM, що забезпечують доставку інформації будь-яких додатків з високою якістю, надають послуги доставки як з орієнтацією на з'єднання, так і без орієнтації на з'єднання.

Література:

1. Беркман Л. Н., Гніденко М. П., Чумак О. І., Булгач С. В., Григорович В. В. Основи побудови мереж NGN із забезпеченням належної якості обслуговування. - Навч. посібник підготовлено для самостійної роботи студентів вищих навчальних закладів. – Київ: ННІТІ ДУІКТ, 2008. – 113 с.

2.В.И. Битнер, Ц.Ц. Михайлова Сети нового поколения – NGN. Учебное пособие для вузов. - Питер: Горячая линия телеком. - 2011. – 226 с.

Кузавков В.В.
К.т.н., доцент, докторант НОВ (ВІТІ)
Гайдур Г.І.
к.т.н., доцент каф. Інформаційних технологій
Державний Університет телекомунікацій
м. Київ, Україна

ЧАС ЛОКАЛІЗАЦІЇ НЕСПРАВНОГО РАДІОЕЛЕКТРОННОГО КОМПОНЕНТУ МЕТОДОМ ВЛАСНОГО ВИПРОМІНЮВАННЯ

Будь-яка система має кінцеву надійність і при виникненні в ній відмов, виникає необхідність швидкого виявлення, пошуку та усунення несправностей і відновлення заданих показників надійності. Особливе значення має той факт, що традиційні методи діагностування вимагають або наявності висококваліфікованого обслуговуючого персоналу або складного діагностичного забезпечення. Необхідно відзначити, що з підвищенням загальної надійності цифрових систем зменшується кількість відмов і втручань оператора для пошуку та усунення несправностей. З іншого боку, поряд з підвищенням надійності цифрових систем спостерігається тенденція до певної втрати обслуговуючим персоналом навичок усунення несправностей. Виникає парадокс, чим надійніше цифрова система, тим повільніше і з меншою точністю відшукуються несправності, тому що у цифрових системах підвищеної складності ускладнюється та уповільнюється накопичення досвіду пошуку та локалізації несправностей обслуговуючим персоналом [1,2]. У цілому до 70-80% часу відновлення систем, становить час технічної діагностики, що складається із часу пошуку та локалізації елементів, які відмовили. Експлуатаційна практика показує що, сьогодні інженери не завжди готові вирішувати на необхідному рівні завдання технічної експлуатації сучасних систем. Тому зростання складності цифрових систем і важливість забезпечення їхнього якісного функціонування вимагає організації технічної експлуатації (контролю технічного стану) на наукових основах.

З метою попередження відмов та аварій, скорочення часу та витрат, пов'язаних з виявленням несправностей сучасних цифрових систем, побудованих за комп’ютерною архітектурою, і для менш складних технічних виробів (моноблочних (моноплатних) конструкції), виникає необхідність створення та введення в систему військового ремонту автономних автоматизованих систем діагностування (АА СД) [3].

Подібні системи є автономними уніфікованими комплексами для автоматизованої перевірки ступеня працездатності та справності блоків та РЕО у цілому, що дозволяє локалізувати несправності за результатами контролю діагностичних і функціональних параметрів в експлуатаційних або спеціальних тестових режимах, причому результати діагностування можуть бути представлені оператору або накопичуються для наступної обробки.

Існуючі технології, технічна і теоретична база дозволяють реалізувати та впровадити в систему ремонту РЕО автономної автоматизовані СД. Один з режимів функціонування запропонованої АА СД є режим локалізації несправного РЕК.

Локалізацію несправності до рівня нерозбірної конструкції – до радіоелектронного компоненту (РЕК) дозволяє здійснити розроблений метод власного випромінювання (другий режим роботи АА СД).

Сутність методу власного випромінювання полягає в тому, що в якості діагностичного параметру використано параметри поля в інфрачервоному діапазоні хвиль, сформованого навколо (над) поверхнею РЕК під дією на його вході перевірних тестових послідовностей. Метод використовується автономною автоматизованою системою діагностування для локалізації несправного радіоелектронного компоненту цифрового блоку РЕО та ґрунтується на наявність прямого зв'язку ресурсу РЕК з його температурою [4].

Метод ґрунтуються на діагностичні моделі (ДМ) РЕК яка враховує фізико-хімічні процеси в напівпровідниках під час експлуатації.

Час визначення технічного стану (t_{TC}) методом власного випромінювання визначається двома складовими: часом реєстрації діагностичної інформації (t_r), часом прийняття рішення (часом обробки інформації) (t_o).

В практиці діагностування мають місце два варіанти обробки ДІ:

обробка ДІ відбувається після проходження всіх тестових послідовностей, при цьому час визначення ТС визначається $t_{TC} = t_r + t_O$;

обробка ДІ відбувається паралельно з реєстрацій ДІ, при цьому $t_{TC} = t_r$.

В свою чергу, час прийняття рішення t_o залежить лише від потужності обчислювальних засобів автономної автоматизованої системи діагностування в режимі визначення ТС, і на сьогодні практично не має технічних обмежень (існують обмеження лише фінансового плану).

Таким чином, час визначення технічного стану (t_{TC}) безконтактним індукційним методом визначається виключно часом реєстрації діагностичної інформації (t_r), який залежить від часу прояву діагностичного параметру на поверхні РЕК – часу виходу РЕК на сталий режим,

Для локалізації несправного РЕК методом власного випромінювання перевірна тестова послідовність подається на «підозрюваний» РЕК декілька разів, доки ДП (температура поверхні РЕК) не досягне сталого режиму. При детермінованому тестовому впливі час виходу РЕК на сталий режим (від температури T_1 до T_2) визначається за виразом:

$$t_{1-2} = mCR_T \ln \frac{PR_T - (T_1 - T_0)}{PR_T - (T_2 - T_0)}. \quad (1)$$

де: m - маса РЕК, T_0 – температура, рівна температурі навколишнього середовища, у момент часу $t = 0$, P – потужність, що виділятися рівномірно за об'ємом, C – питома теплоємність тіла, R_T – тепловий опір поверхні що вкриває кристал.

Рівняння теплопровідності через коефіцієнт a враховує фізичні характеристики матеріалу що виконує захисні функції кристалу напівпровідника – шару який вкриває кристал [5].

В наслідок рішення рівнянь отримуємо значення температур до початку імпульсу впливу та між ними:

$$T_1 - T_0 = P_i R_T \frac{e^{\tau_u / \tau_0} - 1}{e^{T_n / \tau_0} - 1} \quad (2)$$

$$T_2 - T_1 = P_i R_T \left(e^{T_n - \tau_u / \tau_0} - 1 \right) \quad (3)$$

Вирази (2), (3) використаються для розрахунку температури сталого режиму при імпульсному (тестовому) впливі на РЕК [6].

Література:

1. Abramovici M, Breuer M.A, Friedman A.D. Digital Systems Testing and Testable Design. IEEE Press, Piscataway, New Jersey, 1994.
2. Zherdev M. K., Kredentser B. P., Kuzavkov V. V. Ways and methods of efficiency increasing of the independent automated test systems of radio-electronic devices. National Aviation University. Electronics and Control Systems 2014. № 4(42):) стр.150-154.
3. В. В. Кузавков, О. Г. Янковський. Застосування методу власного випромінювання для технічної діагностики радіоелектронних блоків. Збірник наукових праць. Одеської державної академії технічного регулювання та якості, Одеса 2(5) 2014г с.58-62.
4. Кузавков В. В., Редзюк Є. В., Коваль Л.Т. Математична модель задачі про поширення теплоти в радіоелектронних компонентах. ДУТ Зв'язок. Загальногалузевий науково-виробничий журнал. – К.: ДУТ, 2014. – Вип. №2 (108) – с. 51-55.
5. В. Кузавков Забезпечення робочого режиму радіоелектронних компонентів в методі власного випромінювання. КПІ Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. – К.: КПІ, 2015. – Вип. №1(29). – с.97-101.

Гайдур Г.І.
К.т.н., доцент каф. Інформаційцних технологій
Прокопенко В.І.
Студент кафедри Інформаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

МЕРЕЖІ З ОПТИЧНИМ ДОСТУПОМ ДЛЯ НАДАННЯ СУЧАСНИХ ПОСЛУГ

Нині у світі силу має той, хто володіє інформацією, яка відіграє незмінно важливу роль у будь-якій сфері людської діяльності. XXI століття — ера інформаційного суспільства, у якому інформація все частіше визначається як основний ресурс майбутнього. Звичайно, є багато джерел черпання інформації, та, мабуть, інтернет все-таки посідає перше місце. І в наш час складно уявити людину, яка ним не користується.

Сьогодні практично всі мають вдома інтернет. Але на всіх він задовольняє. Цьому може сприяти багато причин, і однією з таких може бути вартість абонементної плати, тобто тариф. Для того, щоб це зробити, необхідно врахувати ряд чинників і найдрібніших деталей. Отож, треба розробити проект проведення інтернету в деякому районі. В цьому проекті обрати технологію, розробити план прокладання кабелів і встановлення обладнання, розрахувати необхідні показники для прорахунку тарифу.

Мережі доступу є, мабуть, найбільш витратним ланкою операторських мереж зв'язку. В даний час на ділянці доступу використовуються переважно мідні кабелі (виті пари). Пропускна здатність та канальна ємність таких кабелів не дозволяє повною мірою реалізувати сучасні мультисервісні послуги, тобто послуги з передачі мови, даних і мультимедійного трафіку, включаючи відеоінформацію. Для надання нових мультисервісних послуг потрібна певна смуга пропускання, зазвичай ширша, ніж та, яку можуть забезпечити існуючі технології в мідно-кабельної інфраструктурі. Тому для організації доступу до широкосмугових послуг часто доводиться прокладати кабелі з високою пропускною здатністю. Найбільш ефективним в таких випадках є побудова волоконно-оптичної кабельної інфраструктури. Тому ми будемо розглядувати технологію FTTB, яка на даний момент є дуже цікавою для провайдерів інтернет.

Архітектура FTTB отримала найбільше поширення, оскільки при будівництві мереж FTTx на базі Ethernet Архітектура FTTB домінує у новозведених будинках і у великих операторів зв'язку, тодіяк FTTH буде затребувана тільки в новому малоповерховому будівництві.У першу чергу це пов'язано із суттєво вищою вартістю її реалізації в порівнянн із вартістю мережі FTTC/FTTB, відсутністю переваг у смузі пропускання для користувача.

FTTB (Fiber To The Building) - оптикадобудівлі. Під такою технологією розуміють відносно глибоке проникнення оптики до абонента, тобто роботу оптичного вузла (ОВ) в середньому на 100…250 абонентів (наприклад 9…12-ти поверховий будинок на 4..6 під'їздів). Враховуючи, що вартість оптико-волоконных кабелів, оптичних передавачів і приймачів постійно знижується, в найближчому майбутньому технологія FTTH буде виправдана. Першим етапом для спорудження FTTH є будівництво FTTB мереж.Особливостями технології FTTB є:

- підвищена надійність. Як відомо з практики, найбільше число відмов доводиться саме не на ВОЛС, а на коаксіальні мережі. Зважаючи на наявність каскадного включеного не більше за один підсилювач (наприклад, підсилювач на під'їзд), вірогідність відмови є низькою.

- простота побудови паралельних цифрових мереж є найважливішою гідністю FTTB технології. При цьому під паралельну цифрову мережу виділяється окреме оптичне волокно (замість жили під реверсный канал).

-зниження шумів досягається за рахунок малого числа абонентів, що підключаються до одного ОВ.

-можливість використання економічних ОВ досягається за рахунок того простого факту, що вслід за ОВ встановлюється потужний будинковий підсилювач, отже, до вихідного каскаду ОВ не пред'являється жорстких вимог як по коефіцієнту посилення, так і по вихідному рівню.

У волоконно-оптичному кабелі, що проходить до оптичного вузла будівлі, використовується як мінімум, три активні волокна. Вартість кабелю з числом волокон менше восьми менше ніж, вартість магістрального коаксіального кабелю. По парі волокон забезпечується канал зв'язку мережі з ієрархією Ethernet 10/100/1000. До абонента прокладається вита пара довжиною до 200 метрів на інтерфейси 10 Base - T або 100 Base - TX. При підключенні індивідуальних абонентів краще повністю відмовитися від мультиплексорів, а усі канали зробити дуплексними. Використання комутаторів дозволить організувати ієрархію за швидкостями, ввести тарифікацію абонентів при їх підключенні до 10 Base - T або 100 Base - TX, а також використати швидкісніші канали на магістральних ділянках мережі.

Вираховуючи вартість обладнання, прокладки кабелю можливо визначити тариф, який зможе окупити мережу і приносити прибуток. Для збільшення прибутку від мережі, провайдеру необхідно пропонувати нові додаткові послуги. Такою на данний момент є послуга 3DTV.

Тому можна впевнено говорити, що технологія FTTx є дуже вигідна технологія з поглядом на майбутнє розширення мережі та впровадження нових послуг.

Література:

1. Каток В.Б., Солодовнік А.І. Волоконно-оптичні мережі доступу за технологією FTTx. – К: - 2010. – 89 с.

2. Департамент научно - технической политики ОАО «Укртелеком». Вихідні дані на проектування мереж доступу на базі технології FTTB. – К: - 2010. – 210 с.

3. Патий Є. FTTx: обозримое будущее Интернета. – Экспресс Электроника, 2007. – 125 с.

Сабадаш В.А.

Аспірант каф.Обчислювальної техніки

Державний університет телекомунікацій

м.Київ, Україна

АВТОМАТИЗАЦІЯ ПРОЦЕСА КЕРІВНИЦТВА ЕКСПЛУАТАЦІЇ ЛІНІЙНО-КАБЕЛЬНИХ СПОРУД МІСЦЕВИХ МЕРЕЖ ЗВ'ЯЗКУ

Актуальним питанням є розробка інформаційної системи експертної оцінки автоматизації процеса керівництва експлуатації лінійно-кабельних споруд місцевих мереж зв'язку. Для зібрання і аналізу результатів потрібна база даних.

Створення організаційної автоматизованої системи управління, наприклад,для лінійно-кабельних споруд– це шлях до впровадження нової інформаційної технології. Одним з головних завдань поряд з розробкою основ економіко-організаційного моделювання апарату управління є раціоналізація організаційних зв'язків і приведення структури апарату управління у відповідність з реальними умовами, характерними для споруд місцевих мереж зв'язку.

В останні роки в місцевих мережах зв'язку почали застосовувати оптичні кабельні системи, багатопарні кабелі з металевими провідниками в алюмінієвій і сталевій гофрованих оболонках, а також кабелі в пластмасовій оболонці з гідрофобним заповненням. Розроблено і впроваджено нові типи пристроїв кабельної каналізації.Застосування методів щодо технічної експлуатації лінійно-кабельних споруд.

Повна інтегрована автоматизація містить у собі такі інформаційно-управлінські процеси: зв'язок, збір, збереження і доступ до необхідної інформації, аналіз інформації, підготовка тексту, підтримка індивідуальної діяльності, програмування і вирішення спеціальних завдань.

Автоматизація процеса керівництва експлуатації лінійно-кабельних споруди місцевих мереж зв’язку потребує в собі певну базу даних, яка працює автоматично без втручання людини, та доступ до якої можливий з любою точки світу, а також швидкий доступ для її використання: читання, копіювання тощо.

Основою ефективного функціонування системи на високому рівні є автоматизація процесів. Виходячи с цього, істотно зростає необхідність автоматизації процеса керівництва експлуатації лінійно-кабельних споруд місцевих мереж зв’язку.

Література:

1.«Експлуатації лінійно-кабельних споруд» - мережа Internet

Мушта С.С.

Аспірант каф. Вищої математики

Державний університет телекомунікацій

м.Київ, Україна

АНАЛІЗ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНИХ ЦІЛЯХ

Існує велика кількість хмарних сервісів і застосувань (операційні системи, офісні застосування та ін.), які можна використовувати в навчальних цілях не тільки як новий засіб навчання, але і як доступна альтернатива традиційному програмному забезпеченню. Адже в більшості сучасних навчальних закладах та комп'ютерних лабораторіях встановлене програмне забезпечення від компанії Microsoft, представлене операційною системою сімейства Windows і інтегрованим офісним пакетом Microsoft Office. Досить рідко на учбових комп'ютерах встановлене вільне програмне забезпечення – операційна система сімейства Linux та офісний пакет LibreOffice. При цьому зміст навчальної, науково-методичної літератури та навчальних програм практично не враховує можливості використання хмарних операційних систем Google Chrome OS, JoliCloud, CloudTop тощо, та хмарних офісних пакетів Office 365, Документи Google, Zoho Office, базові функціональні можливості яких відповідають основним вимогам до навчального програмного забезпечення.

Одним із яскравих прикладів впровадження корпорацією IBM хмарних технологій в освіту можна назвати проект, що розпочався 2010 року для іспанського фонду Fundacion German Sanchez Ruiperez (www.fundaciongsr.com). Мета проекту полягає в широкій підтримці освіти і культури населення. Використовуючи хмарні технології IBM планували надавати студентам доступ до навчальних матеріалів з будь-якого пристрою через мережу Інтернет.

Сервіс IBM Smart Business Desktop Cloud використовувався студентами під час їх літніх навчальних програм. Вони отримали доступ до навчальних матеріалів, інструментів для створення власного контенту, можливість спілкуватися між собою за допомогою соціальних мереж, он-лайн товариств та відео конференцій. Цей проект дозволив викладачам повністю сконцентруватися на змісті навчальних програм, а не на вирішенні технічних проблем.

Один з прикладів віртуалізації середовища доступу є створена система на базі Державного університету телекомунікацій *(MOODLE)*, в якій студент отримує доступ до навчальних матеріалів, при цьому може відразу почати роботу над завданням у спеціалізованій програмі чи пакеті. Водночас викладач має можливість контролювати роботу студентів, перевіряти виконані завдання, допомагати порадами.

Рисунок 1. Система дистанційного навчання Moodle

Узагальнюючи вищесказане слід зазначити, що хмарні сервіси сприяють підвищенню мотивації самостійної навчально-пізнавальної діяльності студентів, що відповідає завданням формування кваліфікованого спеціаліста засобами ІКТ та забезпечують швидку комунікацію між викладачем і студентом.

Література:

1. Алгазинов, Э. К. Анализ и компьютерное моделирование информационных процессов и систем: учебное пособие для студентов вузов / Э. К. Алгазинов, А. А. Сирота. - Москва : Диалог-МИФИ, 2009. - 416 с. - ISBN 978-5-86404-233-5.

2. Дворников, В. К. Исследование клиент-серверной нагрузки центра дистанционного обучения : дис. канд. техн. наук : 05.12.13 / В. К. Дворников. - Москва, 2009. - 162 с.

3. Биков В.Ю. Технології хмарних обчислень, ІКТ-аутсорсінг та нові функції ІКТ-підрозділів навчальних закладів і наукових установ / В. Ю. Биков // інформаційні технології в освіті. Збірник наукових праць. Випуск 10. – Херсон : ХДУ, 2011. – 271 с. – С.8-23.

Батрак Є.О.
Аспірант каф. Радіомоніторингу та радіочастотного менеджменту
Державний університет телекомунікацій
м. Київ, Україна

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ВУЗЬКОНАПРАВЛЕНИХ АНТЕННИХ СИСТЕМ У СКЛАДІ КОМПЛЕКСУ ЗВ'ЯЗКУ

Аналіз сучасного стану радіозасобів, показав що вони своїми технічним характеристикам не повною мірою задовольняють сучасним вимогам до системи зв'язку й автоматизації управління. оскільки використовують застарілі принципи побудови апаратури, неефективні види модуляції сигналу, мають низьку завадозахищеність від впливу навмисних завад, малу пропускну здатність, низький рівень автоматизації процесів встановлення, ведення та підтримання радіозв'язку [1].

Основним напрямом удосконалення сучасних засобів радіозв'язку управління є перехід до програмованих радіо засобів із застосуванням вузько направлених антен, які дозволяють гнучко управляти конфігурацією мережі радіо доступу мобільних абонентів і режимами її роботи. Застосування вузько направлених антенних систем в свою чергу вимагає оцінки параметрів систем автоматичного керування у відповідності до існуючих вимог.

Аналіз існуючих методів підвищення ефективності функціонування систем автоматичного керування активних фазових антенних решіток показав, що найбільш простими і прозорими є безпосередні методи, серед яких: частотний метод, коефіцієнтів помилок, квадратичних інтегральних оцінок. Але використання безпосередніх методів не завжди доцільно для випадків, коли не можливо з максимальною точністю визначити в якому саме елементі структурної схеми змодельованої системи здійснюється збурююча дія, тобто цей процес має випадковий характер.

Вирішення даного завдання має два шляхи, а саме:

- використання прямих методів;
- побудова еквівалентної системи автоматичного керування діаграмою направленості активної фазової антенної решітки відповідно збурюючій дії.

Таким чином завчасно змодельована система дозволить не тільки оцінити, а й керувати параметрами активної фазової антенної решітки в умовах часу обмеженому обчислювальними операціями та максимально наближеному до реальних [2].

Тому предметом досліджень є методи підвищення швидкодії та динамічної точності систем автоматичного керування діаграмою направленості активної фазової антенної решітки в умовах випадкових збурюючих дій.

Метою є підвищення швидкодії та динамічної точності наведення активної фазової антенної решітки рухомих мобільних станцій зв’язку шляхом використання систем автоматичного керування діаграмою направленості активних фазових антенних решіток за рахунок автоматичного керування параметрами цих систем. Для досягнення мети необхідно розв’язати наукову задачу, що полягає в розробці методики підвищення швидкодії та динамічної точності систем автоматичного керування діаграмою направленості активних фазових антенних решіток [3,4].

Література:

1. Справочник по радиоконтролю. - Женева: Бюро радиосвязи МСЭ, 2002. - 585 с.

2. Ступак В.С. Долматов СО. Основи радіочастотного контролю: практичний посібник /В.С. Ступак, С.О. Долматов; за ред. д.т.н. Олійника В.Ф. – К.: 2004. – 231 с.

3. Регламент радиосвязи. Сборник рабочих материалов по международному регулированию планирования и использования радиочастотного спектра. - М.: 2004. – 560 с.

4. Логинов Н.А. Актуальные вопросы радиоконтроля в Российской Федерации / Н.А. Логинов - М.: Радио и связь, 2000. - 240 с.

Тихонов Е. С.

Аспирант каф. Прикладного программирования

Коник Р. С.

Аспирант каф. Прикладного программирования

Государственный университет телекоммуникаций

г. Киев, Украина

ПРОБЛЕМЫ ПРОГРАММИРОВАНИЯ

Основной проблемой разработчиков программного обеспечения с увеличением числа распределенных систем стала организация взаимодействия между различными системами и их компонентами. Само собой, такие проблемы существовали и за много лет до этого, поэтому для их решения уже существовали некоторые стандарты и архитектуры, с разной степенью успеха справляющиеся с ними.

Такие проблемы принято делить на две общие категории:

- локальное программирование;

- глобальное программирование.

Локальное программирование

В локальном программировании проблемы и их решения в некотором смысле отличаются по своей сложности и организации:

- проблемы системы типов;
- проблемы с метаданными;
- проблемы выполнения.

Глобальное программирование

При работе с программными компонентами, написанными разными программистами и при помощи разных языков программирования в различных средах, и последующих попытках собрать эти компоненты в одну распределенную систему, программисту придется решить бесчисленное множество проблем глобального программирования:

- проблема именования (naming);
- обработка ошибок (error handling);
- безопасность (security);
- контроль версий (versioning);
- масштабируемость (scalability).

Язык Java – как один из методов решения проблем

- Java используется на 97% корпоративных настольных ПК.
- Java используется на 89% настольных ПК в США.
- 9 млн разработчиков на Java в мире.
- Инструмент номер 1 среди разработчиков.
- Программа номер 1 среди разработчиков.
- Java используется в 3 млрд мобильных телефонов.
- Java входит в комплект поставки 100% всех проигрывателей дисков Blu-ray.
- Используется 5 млн Java Card.
- Java используется в 125 млн ТВ-устройств.
- 5 из 5 основных производителей оригинального оборудования включают в комплект поставки Java ME.

Преимущества языка Java

1) Одно из основных преимуществ языка Java — независимость от платформы, на которой выполняются программы.

2) Синтаксис языка Java похож на другие синтаксисы программирования.

3) Java — полностью объектно-ориентированный язык.

4) Исключена возможность явного выделения и освобождения памяти. Память в языке Java освобождается автоматически с помощью механизма сборки мусора.

5) Введены истинные массивы и запрещена арифметика указателей.

6) Исключена возможность перепутать оператор присваивания с оператором сравнения на равенство.

7) Исключено множественное наследование. Оно заменено новым понятием - интерфейсом.

Характерные особенности языка Java

- Простой.

- Интерпретируемый.
- Распределенный.
- Надежный.
- Безопасный.
- Машино-независимый.
- Объектно-ориентированный.
- Высокопроизводительный.
- Многопоточный.
- Динамичный.
- Не зависящий от архитектуры компьютера.

Освещены следующие стороны Java как объектно-ориентированного языка программирования. Классы определяют шаблон, по которому создаются конкретные объекты. Поля данных объекта определяют состояние объекта.

Объекты обмениваются сообщениями между собой. Получение сообщения приводит к вызову одного из методов. Методы определяют поведение объекта данного класса. Методы для разных классов могут иметь одно и то же имя, но различное содержание.

Система Java достаточно безопасна, чтобы жить в сетевом окружении. Нейтральность к архитектуре и переносимость делают ее достаточно привлекательной для создания распределенных по сети приложений.

Литература:

1) https://www.java.com/ru/about/
2) http://habrahabr.ru/post/201612/
3) http://java-study.ru/java-uchebnik/2-vvedenie
4) http://citforum.ck.ua/internet/iinet96/17.shtml
5)http://www.program-code.ru/index.php/net-framework/problemy-programmirovaniya

Вишнівський В.В.
Д.т.н., професор каф. Інформаційних технологій
Прилєпов Є.В.
Аспірант каф. Інформаційних технологій
Державний Університет Телекомунікацій

ІНТЕГРАЦІЯ SDN РІШЕННЯ В ІСНУЮЧІ КОМП'ЮТЕРНІ МЕРЕЖІ

Майбутні мережі все більше будуть спиратися на програмне забезпечення, що прискорить впровадження інновацій в мережах, як це вже має місце в області обчислень і зберігання даних. Основними трендами розвитку корпоративних мереж і мереж центрів обробки даних є:

стрімке зростання обсягів трафіку і зміна його структури у бік передачі відео та уніфікованих комунікацій;

необхідність підтримки мобільних користувачів і соціальних мереж;
високопродуктивні кластери для обробки великих даних;
віртуалізація для надання хмарних сервісів.

На даний час технологія SDN відноситься до технологій нового покоління і здатна вирішити перераховані завдання.

Метою дослідження є розробка універсального протоколу передачі даних для підвищення ефективності клієнт-серверних систем середньої складності.

Особливості переходу від традиційних мереж до SDN

Перехід до SDN вимагає одночасну підтримку як SDN так і застарілого обладнання. Протокол IETF PCE (Path Computation Element) може допомогти в поступовій або частковій міграції SDN. З PCE, обчислення шляху компонентів мережі переміщується з мережі вузла до централізованого розподілення в той час як традиційні мережеві вузли що не використовують PCE продовжуватимуть використовувати їх існуючу функцію обчислення шляху. Специфічний протокол (PCEP) забезпечує зв'язок між мережевими елементами але не забезпечує повноцінний SDN. Централізований контролер SDN підтримує повний розрахунок шляху з по декількома вузлам мережі. Подальший розвиток необхідний для досягнення гібридної SDN інфраструктури, в якій традиційні, SDN-включені і гібридні мережеві вузли можуть працювати в гармонії. Така сумісність вимагає підтримки відповідного протоколу, який і задає вимоги до інтерфейсів зв'язку SDN і забезпечує зворотну сумісність з існуючими технологіями маршрутизації IP та MPLS. Таке рішення дозволить скоротити витрати та ризики для корпоративних і клієнтських мереж, що переходять на SDN. ETSI NFV (Network Function Virtualisation) Industry Specication Group має намір стандартизувати компоненти базової мережі, які можуть бути віртуалізовані для забезпечення ефективної масштабованості та розміщення цих послуг. IETF ForCES WG (Forwarding and Control Element Separation) виконує стандартизацію інтерфейсів, механізмів та протоколів з метою розділення управління переадресації IP маршрутизаторів. ONF стандартизує OpenFlow як протокол зв'язку в мережі і керує стандартом відповідних протоколів, таких як управління OpenFlow і протоколу конфігурації. IETF, ETSI, ONF наразі найбільш ефективні стандарти для підтримки міграції від традиційної моделі мережні до SDN.

Майбутнє мереж буде формуватися навколо цього спрямування. Мета полягає в забезпеченні ефективної комунікації та якісних послуг, де мережі, дані і обчислення об'єднані в сервісну архітектуру. У майбутньому, для конкретного процесу, дані вимагатимуть обчислення, зберігання і підключення, перед запуском додатка. Розташування елементів мережі може бути розподілено фізично і віртуально але це буде зовсім непомітно для кінцевого користувача. Всі користувачі будуть спостерігати якість отримання запитаної послуги.

Література:

1."NetworkFunctionVirtualisation" ETSIIndustrySpecificationGroup. [Online]. http://portal.etsi.org/portal/server.pt/community/NFV/367

2.S. Yeganeh, A. Tootoonchian, and Y. Ganjali, On scalability of software-defined network- ing," IEEE Communications Magazine, vol. 51, no. 2, pp. 136-141, February 2013.

3."Path Computation Element" IETF Working Group. [Online]. http://datatracker.ietf.org/wg/pce/charter/

Борисенков Є.А.
магістр ФІТ
Державний університет телекомунікацій
м.Київ,Україна

АСПЕКТИ ПЛАНУВАННЯ МЕРЕЖІ ЧЕТВЕРТОГО ПОКОЛІННЯ

На етапі динамічного розвитку інформаційно-комунікативного суспільства виникає необхідність у нових підходах для освоєння можливостей інформаційних процесів, наслідком чогойде впровадження нових технологій, що є передумовою для повсюдного проникнення широкосмугового мобільного доступу.

Однією з інноваційних технологій, яка покликана вирішувати питання інформаційного обміну, створення єдиного інформаційного простору, а також забезпечити входження України в європейську та глобальну інформаційну інфраструктуру цебезпроводова технологія LTE (Long Term Evolution).

Long Term Evolution (довгостроковий розвиток) – це інтеграція з уже існуючими протоколами, підвищення швидкості і ефективності передачі даних, зниження витрат, а також поліпшення і розширення наданих послуг. Сервіси, які може запропонувати мережа четвертого покоління, починаються від передачі голосу і даних до мультимедіа і відео. Для реалізацій цих вимог мережа повинна мати високу швидкість прийому/передачі сигналу. В ідеалі технологія LTE може надавати швидкість передачі 173 Мбіт/с на прийомії 58 Мбіт/с на передачу. Перевагою мережі є не тільки висока швидкість, але і радіус покриття базової станції від 5 км до 30 км.

При переході від мереж попередніх поколінь до мереж LTE необхідно, без сумніву, враховувати все більш зростаючу активність користувачів. На теперишній момент вже не достатньо проаналізувати покриття і оцінити взаємний вплив BS, а оцінка пропускної здатності повинна проводитися з урахуванням моделювання параметрів трафіка і розподілу абонентів [1].

При плануванні мережі LTE, в першу чергу, необхідно визначити яким чином будуть реалізовані рішення побудови транспортної мережі і мережі радіодоступу E - UTRA.

Існують три основні варіанти організації зв'язку:

Побудова мережі LTE "з чистого аркуша". В цьому випадку компанія-оператор зв'язку здійснює будівництво повністю усіх об'єктів зв'язку, які будуть включені в мережу LTE.

Побудова мережі LTE способом оренди усіх компонентів зв'язку у сторонніх операторів, за винятком устаткування базових станцій. Об'єктами, що орендуються, будуть: вишки для базових станцій і усі компоненти транспортної мережі.

Побудова мережі LTE універсальним способом. Цей варіант включає обидва способи побудови мережі, при ведені вище.

Компанія, яка вже займається наданням послуг фіксованого зв'язку і що має розвинену транспортну мережу в районі планування при проектуванні мережі LTE, ідеально підходить універсальний спосіб побудови мережі LTE.

Процес планування радіомережі LTE описаний алгоритмом, який представлений на рис. 1.

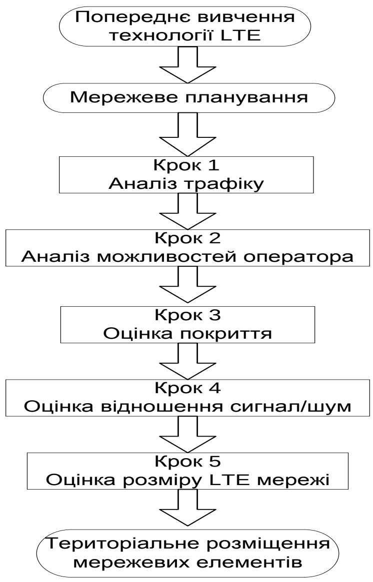


Рисунок 1 - Алгоритм процес упланування радіомережі LTE

Значення для технології LTE враховують такі припущення: сервер знаходиться в будинку з мережею радіодоступу, відстань між базовими станціями (BS) - 500 м, стандартна швидкість руху - 5 км / год.

Планування радіомережі LTE буде проводитися в міській місцевості, а це означає, що щільність абонентів буде висока і базові станції повинні встановлюватися на мінімальному видаленні один від одного з метою закрити кожної eNB якомога більшу територію. У зв'язку з цим потрібно підібрати відповідний частотний діапазон. В даному випадку потрібно керуватися правилом, що чим нижче частота, тим далі поширення радіосигналу; вибираючи структуру абонентської мережі, необхідно враховувати вже наявну структуру мережі оператора.

На рис.2 представлена залежність площі стільників від частоти передачі в умовах міської забудови.

Ще одним важливим питанням при плануванні мережіLTE є вибір устаткування. Основними критеріями по вибору високотехнологічного устаткування для мережі LTE виступають:

Ціна/якість.

Діапазон робочих частот.

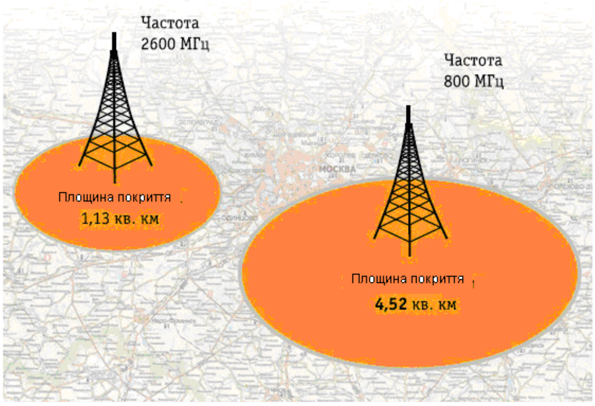


Рисунок 2 - Залежність площі стільників від частоти передачі

Можливість «безшовної» інтеграції в існуючі мережі.

Необхідна функціональність, яка визначається безпосередньо бізнес-планом оператора.

Відношення заявлених можливостей до дійсних.

Інформаційна підтримка.

Гарантійні зобов'язання.

Можливість збільшення кількості інтерфейсів і продуктивності.

Можливість впровадження нових функціональних можливостей.

Можливість резервування та ін.

Усі ці критерії є досить важливими, проте усе устаткування є взаємозамінним, тому на перше місце при виборі устаткування часто виходить відношення ціна/якість[2].

При впровадженні мереж четвертого поколінняна міських мережах головним є планування цієї мережі за допомогою представленого алгоритму.

Література:

1.Тихвинский, В.О. Сети мобильной связи LTE: технология и архитектура [Текст] / В. О. Тихвинский, С.В. Терентьев, А. Б. Юрчук. – М.: Эко-Трендз, 2010. – 284 с.

2.Кааринен Х. Сети UMTS. Архитектура, мобильность, сервисы. – М.: Техносфера, 2007.

Зоценко В.С.

Аспірант каф. Вищої математики

Державний університет телекомунікацій

м. Київ, Україна

АНАЛІЗ ВИМОГ ДО ЗВ’ЯЗНОСТІ СТРУКТУР ПЕРВИННИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Телекомунікаційа мережа являє собою сукупність технічних засобів, що забезпечують передачу і розподіл потоків інформації при взаємодії віддалених об'єктів. Телекомунікаційні мережі прийнято оцінювати низкою показників, що відбивають у цілому можливість і ефективність транспортування інформації в них[1].

Основними технологічними вимогами до мереж є[2]:

- висока продуктивність (пропускна здатність) ТКС;

-семантична і часова прозорість ТКС, тобто система має бути інваріантною до структури трафіка існуючих мережних технологій і забезпечувати в заданих межах значення ймовірнісно-часових показників якості його обслуговування;

-«широкосмуговість», під якою розуміється можливість гнучкої і динамічної зміни швидкості передачі інформації в широкому діапазоні залежно від поточних потреб користувача;

-ефективність використання мережних ресурсів (канальні, фізичні ресурси і ресурси мережного обладнання);

-надійність ТКС як на експлуатаційному рівні (відмовостійкість), так і на рівні доставки пакетів (імовірність доставки);

-масштабованість, тобто здатність ТКС нарощувати кількість вузлів і протяжність зв’язків в дуже широких межах із збереженням продуктивності мережі в заданих межах, що досягається сегментацією ТКС і використанням ієрархічних структур.

Структура первинної мережі природним чином може бути задана графом G=(N, R), де N=$(n, \ldots n_k)$ – множина вершин, а R= $(r_1, \ldots, r_m)$–множина гілок.

Взаємне розташування пунктів та ліній характеризує зв’язність мережі і здатність до забезпечення доставки інформації в різні пункти.

Поняття зв'язності графів відіграють фундаментальну роль при аналізі та синтезі структур мереж зв'язку. Особливі значення характеристики зв'язності мають при дослідженні живучості та структурної надійності мереж зв'язку[3].

Граф є топологічною моделлюструктури інформаційної мережі [5].

Вибір топології мережі є щонайпершою задачею, розв'язуваною при її

побудові, і визначається такими вимогами, як економічністьта надійність зв'язку. [4]

Топологія «точка – точка» є найбільш простим прикладом базової топологіїі являє собою сегмент мережі, що зв'язує фізично і логічно два пункти.

Надійність зв'язку в такому сегменті може бути підвищена за рахунок

введення резервного зв'язку, який забезпечує стовідсоткове резервування,

називане захистом типу 1+1. При виході з ладу основного зв'язку мережаавтоматично переводиться на резервну.

Топологія «кільце» характеризує мережу, в якій до кожного пункту приєднано дві, й лише дві лінії.

На логічному рівні поміж кожною парою пунктів може бути зорганізовано h = 2 незалежних зв’язуючих шляхів (прямий та альтернативний).

Повнозв’язна топологія забезпечує фізичне і логічне з'єднання пунктів за принципом «кожний із кожним».

Повнозв’язна топологія на логічному рівні має максимальну надійність зв'язку завдяки можливості організації великої кількості обхідних шляхів.

Комірчаста топологія . Кожний пункт сегмента має безпосередній зв'язок з невеликою кількістю пунктів, найближчих за відстанню.

Комірчасті сегменти мають високу надійність зв'язку при меншому числі ребер порівняно з повнозв'язним сегментом.

На основі викладеного матеріалу можна побачити, що кожна структура має як свої переваги так і недоліки. Під час проектування телекомунікаційних мереж часто потрібно знаходити компромісне оптимальне рішення, яке б дало змогу отримати якомога надійну мережу (із найбільшим коефіцієнтом зв'язності) за мінімальну вартість.

Література:

1.Нікітюк Л.А. Архітектура інформаційних мереж / Л.А. Нікітюк // – О.: УДАЗ ім. О.С.Попова, 2000. – 60 с.

2.Барабаш О.В. Оценка показателя функциональной устойчивости псевдорегулярных структур распределенных информационных систем / О.В. Барабаш, А.А. Бельская // Проблеми транспорту: збірник наукових праць. – К.: НТУ, 2011. – Вип. 8. – С 245-250.

Барабаш О.В., Машков О.А. Топологічні критерії та показники функціональної стійкості складних ієрархічних систем. / Моделювання та інформаційні технології: збірник праць. – К.: ШПМЕ НАН України, 2003. – Вип.25. – С. 29-35

Барабаш О.В. Построение функционально устойчивых распределенных информационных систем / О.В. Барабаш // – К.: НАОУ, 2004. – 226с.

Колчин В.Ф. Случайные графы. / В.Ф. Колчин // – М.: Физматлит, 2002. – 256 с.

Птах О.І

Студентка ФІТ

Державний університет телекомунікацій

м. Київ

ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ В КОМУТАЦІЙНИХ ПРИСТРОЯХ

В наш час технології хмарних обчислень стають дедалі популярнішими, а концепція хмарних обчислень є однією із самих актуальних тенденцій розвитку інформаційних технологій. Зокрема, концепція «Хмарних обчислень» передбачає, що користувач має доступ до власних даних, але він не повинен піклуватися про інфраструктуру, операційну систему та програмне забезпечення, з яким він працює. Особливістю хмарних технологій є можливість масштабованості. Клієнт може працювати з хмарними сервісами з будь-якої точки планети і з будь-якого пристрою, що має доступ до мережі Інтернет «Хмарою» метафорично називають Інтернет, який приховує всі технічні деталі.

«Хмарні обчислення» – це комп’ютерна модель, яка передбачає, що усі сервери, мережі, додатки та інші елементи, пов’язані з центрами обробки даних, доступні ІТ-службі та кінцевим користувачам через Інтернет.[2,204] Іншими словами, «Хмарні обчислення» (англ. CloudComputing) це модель забезпечення повсюдного та зручного доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.[3]

При використанні хмарних обчислень програмне забезпечення надається користувачеві як Інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему і програмне забезпечення, з яким він працює.Загалом можна виділити три головні напрямки хмарних обчислень: IaaS (InfrastructureasaService), PaaS (PlatformasaService) ,SaaS (SoftwareasService):

*Програмне забезпечення як послуга (SaaS)- дає доступ до інтегрованої платформи для розробки, тестування та підтримки різноманітних проектів. Прикладами програмного забезпечення як послуги, що працює на основі обчислювальної хмари, є сервіси Gmail та Googledocs.

*Платформа як послуга (PaaS). Наприклад, GoogleApps надає стосунки для бізнесу в режимі онлайн, доступ до яких відбувається за допомогою Інтернет-браузера тоді як ПЗ і дані зберігаються насерверах Google.

*Інфраструктура як послуга (IaaS)- представлення комп’ютерної інфраструктури у вигляді віртуалізації, що включає в себе операційні системи та системне програмне забезпечення, а також апаратну частину сервера.

Цей тип розрахований спеціально на фірми,установи, яким необхідно мати інфраструктуру власної компанії і для цього вони можуть оплачувати дану послугу.

Найбільшими гравцями на ринку інфраструктури як послуги є Amazon, Microsoft, VMWare, Rackspace та RedHat. Хоча деякі з них пропонують більше чим просто інфраструктуру, їх об’єднує мета продавати базові обчислювальні ресурси.

Загалом, ця технологія має як плюси так і мінуси. Вона доволі економічна і доцільна для організацій, корпорацій, фірм і т. д. Вона не потребує значних ресурсів вашого пристрою(будь-то, КПК, планшет, смартфон,нетбук або комп’ютер), але вона вимоглива щодо доступу до інтернету.Це означає, що ви повинні мати безперебійний швидкісний інтернет. Другим мінусом є те, що хоча надавачі послуг і стараються працювати онлайн цілий час, але завжди бувають випадки, коли сервер може бути оффлайн і тоді доступ до ваших послуг буде недоступний.

Література:

1.Теленик С.Ф., Ролик О.І., Букасов М.М., Лабунський А.Ю. Моделі управління віртуальними машинами при серверній віртуалізації// Вісник НТУУ

«КПІ»: Інформатика, управління та обчислювальна техніка. - К.: «ВЕК+», 2009. - № 51. - С. 147-152.

2.Облачные технологии и образование / [Сейдаметова З. С., Аблялимова Э. И., Меджитова Л. М., Сейтвелиева С. Н., Темненко В. А.]. – Симферополь : "ДИАЙПИ", 2012. – 204 с

3.Щотакехмарніобчисленняабохмарнітехнології? [Електронний ресурс] // Режим доступу документаhttp://programming.in.ua/other-files/internet/100-cloud-technologics.html/

4.Орлов С. Облака: низкий старт, быстрый рост // Журнал сетевых решений / LAN. – 2012. – № 6. 4. Риз Дж. Облачные вычисления. – СПб.: БХВ-Петербург, 2011.

Шевченко В.Л.
Директор Навчально-наукового інституту захисту інформації
Рабчун Д.І.
Аспірант каф. Управління інформаційною безпекою
Державний університет телекомунікацій
м. Київ, Україна

ВПЛИВ ДУБЛЮВАННЯ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ СИСТЕМАХ НА ОПТИМАЛЬНИЙ РОЗПОДІЛ РЕСУРСІВ ЗАХИСТУ

В інформаційних системах часто спостерігається перекриття інформації в різних об’єктах, котрі можуть мати фізичну або електронну природу, являти собою носії або канали передачі даних. Навмисне дублювання у корпоративних інформаційних системах (КІС), зазвичай, являє собою технологію резервного копіювання на серверах. В залежності від цінності інформації, особливостей побудови і режимів функціонування КІС виділяють різні види дублювання, котрі класифікуються за певними ознаками. Одна з таких ознак — процедура дублювання. За цією ознакою, дублювання може бути повним, дзеркальним, частковим та комбінованим [1,75].

Мета роботи — виявити вплив дублювання на показники системи захисту інформації і на процес оптимізації розподілу ресурсів між об’єктами. Величини, котрі ми повинні визначити: оптимальна кількість ресурсів захисту Y^{*0} і оптимальний розподіл цих ресурсів $\{y^{*0}\}$ між об’єктами для кожного значення g_{12} при різних формах вразливості $f_k(x,y)$ об’єктів і різних розподілах $\{g_k\}$ інформації по об’єктах. Критерієм оптимальності вважаємо мінімізацію загальних втрат, котрі включають втрати від витоку інформації та витрати на її захист.

Для нападу цільова функція визначає частку здобутої інформації (та одночасно частку втраченої для захисту) і має вигляд [2]:

$$i(x,y) = i_1(x,y) + i_2(x,y) - i_{12}(x,y) = g_1 p_1 q_1(x,y) f_1(x,y) + g_2 p_2 q_2(x,y) f_2(x,y) - g_{12} p_{12} q_{12}(x,y) f_{12}(x,y),$$

Спростимо задачу, покладаючи $p_1 = p_2 = 1$, $q_1(x,y) = q_2(x,y) = q_{12}(x,y) = 1$. Тоді в системі з двох об'єктів матимемо:

$$i(x,y) = i_1 + i_2 - i_{12} = (g_1 + g_{12}) f_1(x,y) + g_2 f_2(x,y) - g_{12} f_{12}(x,y)$$

Величина i_{12} входить у вираз (1) зі знаком мінус, оскільки вона міститься у виразах, i_1 та i_2 і, таким чином, враховується двічі. Імовірність f_{12} вилучення інформації з обох об'єктів визначається більш вразливістю більш захищеного об'єкта: $f_{12} = f_2$. Тоді

$$i = (g_1 + g_{12}) f_1(x,y) + (g_2 - g_{12}) f_2(x,y)$$

Аналіз цільової функції, адаптованої для комп'ютерних систем, котрі використовують технології дублювання інформації показав:

використання дублювання, хоч і збільшує загальну кількість інформації, котру необхідно захищати, але сумарні витрати за захист змінюються не суттєво (рис.1);

поряд з тим, завдяки створенню резервних копій суттєво збільшуються показники цілісності і доступності інформації.

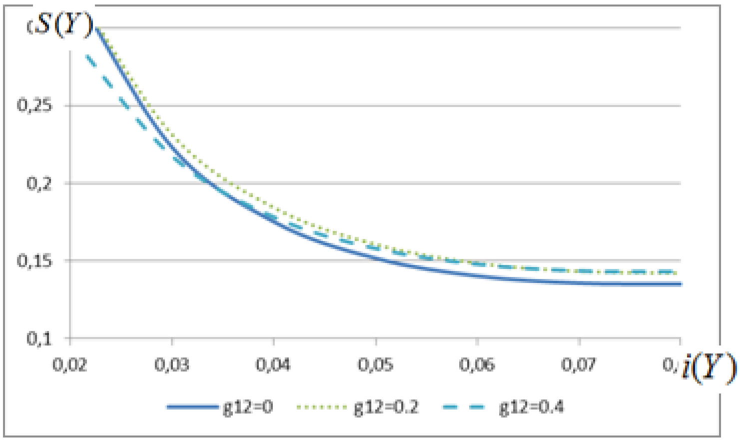


Рисунок1. Сумарні витрати на захист інформації при різних частках дубльованої інформації

Часткове або повне дублювання інформації приводить до зростання обсягу інформації, котру необхідно захищати і, як результат, — до збільшення необхідної кількості ресурсів захисту. Оптимальна кількість ресурсів і їх розподіл між об'єктами залежать від структури інформаційної системи, її параметрів, режиму протистояння, кількості ресурсів нападу, їх розподілу між об'єктами і рівня дублювання. Врахування цих факторів дозволяє оптимальним чином розподілити обсяги інформації і ресурси захисту між об'єктами. Критерієм оптимальності є досягнення мінімальних значень втрат, котрі включають втрати від витоку інформації і витрати на її захист, при якомога меншій чутливості результуючих показників до рівня дублювання. Коригування розподілу ресурсів між об'єктами при введенні дублювання дає можливість мінімізувати зростання необхідної кількості ресурсів при одночасному збільшенні надійності системи.

Література:

1.Шаньгин В. Защитаинформации в компьютерных системах и сетях. — Litres. — 2013. — 592 с.

2.Левченко Є.Г., Рабчун А.О. Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації. — 2010. — №1(1). — С.16-24

Кіракосян Н.А.
Студентка навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ДЕСТРУКТИВНІІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВПЛИВИ, ЯК ЗАСІБ РЕАЛІЗАЦІЇ ГЕОПОЛІТИЧНИХ ТА ІНШИХ ІНТЕРЕСІВ ДЕРЖАВ У XXI СТОЛІТТІ

XXI століття - епоха інформаційних технологій та глобальних інтеграційних процесів. Інформаційні технології застосовуються майже у всіх сферах суспільного життя, що робить суспільство і кожного конкретного індивіда все більш залежним від інформації. Все частіше інформаційні технології використовуються для маніпулювання масовою свідомістю, впливу та управління людьми. Комунікаційними каналами виступають мас-медіа та всесвітня мережа Internet, які створюють так звану «викривлену реальність», у якій відбувається формування «підпорядкованості» свідомості ідеям, які пропагуються ЗМІ, що робить людину відкритою і беззахисною перед маніпулятивними технологіями. Інформаціястаєзброєю.

Економічна, політична, інформаційна незалежність відповідає інтересам будь-якої держави. Саме вони обумовлюють свободу й розвиток особистості, суспільства й держави в цілому та забезпечують їх життєздатність. Інтенсивний розвиток новітніх технологій у сфері комунікацій, глобальні інтеграційні процеси, становлення інформаційного суспільства обумовлюють необхідність найприскіпливішої уваги до можливостей впливу на індивідуальну та масову свідомість, ставлять питання щодо інформаційної безпеки, у т.ч. в межах теоретико-практичних засад ведення інформаційно-психологічних операції для досягнення політичних, економічних та інших переваг над супротивником чи як особливої форми війни у геополітичному просторі сучасного світу. Застосування інформаційно-психологічних прийомів задля відстоювання особистих інтересів, збереження власних ресурсів чи здобуття додаткових у протиборстві з протилежною стороною, відомі людству з незапам’ятних часів.[1]

Інформаційно-психологічний вплив (ІПВ) - вплив на свідомість особи і населення з метою внесення змін у їх поведінку та (або) світогляд. Базовими методами ІПВ є переконання і навіювання.

Переконання звернене до власного критичного сприйняття дійсності. Воно має власні алгоритми впливу:

логіка переконання повинна бути доступною інтелекту об'єкта впливу;

переконання необхідно здійснювати, спираючись на факти, відомі об'єкту;

переконуюча інформація повинна містити узагальнюючі пропозиції;

переконання має складатися з логічно-несуперечливих тез;

факти, що повідомляються, повинні бути відповідним чином емоційно забарвлені.

Навіювання навпаки спрямовано на суб'єкти, що некритично сприймають інформацію. Його особливостями є:

цілеспрямованість і плановість застосування;

конкретність визначення об'єкта навіювання (селективний вплив на визначені групи населення, що враховує основні соціально-психологічні, національні й інші особливості цих груп);

некритичне сприйняття інформації об'єктом навіювання (навіювання засновано на ефекті сприйняття переданої інформації як інструкції до дії без її логічного аналізу);

визначеність, конкретність поведінки, що ініціюється (об'єкту необхідно дати інструкцію щодо здійснення конкретних його реакцій і вчинків, що відповідають меті впливу).[2]

Для реалізації інформаційно-психологічного впливу на індивідуальну, групову і масову свідомість використовуються такі канали поширення й технології (засоби):

засоби масової інформації й спеціальні засоби інформаційно-пропагандистської спрямованості;

глобальні комп’ютерні мережі й програмні засоби швидкого поширення в мережі пропагандистських інформаційних матеріалів;

засоби, що нелегально модифікують інформаційне середовище, на підставі якого людина приймає рішення;

засоби створення віртуальної реальності;

засоби підпорогового психосемантичного впливу;

засоби генерування акустичних й електромагнітних полів.

До спеціалізованих засобів інформаційно-пропагандистської спрямованості належать мобільні, радіомовні і телевізійні центри, пропагандистські пересувні гучномовці, плакати, листівки. Технології їх застосування відпрацьовані й подальший їх розвитокпов'язаний насамперед з методами прихованого впливу на підсвідомість людини.[3]

ІПВ спрямовується на індивідуальну або суспільну свідомість інформаційно-психологічними або іншими засобами, що викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів особистості з метою вплинути на її діяльність і поведінку. Кінцевою його метою є досягнення певної реакції, поведінки (дії або бездіяльності) особистості, яка відповідає цілям ІПВ.

Література:

1.http://vybory.org/articles/485.html

2.http://pidruchniki.com/19311113/psihologiya/osnovni_ponyattya_manipulyativnogo_vplivu

3.http://studopedia.com.ua/1_44863_dzherela-kanali-poshirennya-i-tehnologii-informatsiyno-psihologichnogo-vplivu.html

Шевченко Г.В.
Ст. викладач каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ТАРГЕТИНГОВОГО РОЗМІЩЕННЯ РЕКЛАМИ ПРИ НЕПЕРЕРВНОМУ РЕКЛАМУВАННІ

Розглядається задача відбору оптимальної кількості реклами на різних інтернет-ресурсах. Відображено необхідність знаходження об’єму рекламних повідомлень, який потрібно розмістити на різних майданчиках в межах допустимого бюджету, з метою максимізувати досяжність до цільової аудиторії. Тут в якості майданчиків були розглянуті різні інтернет ресурси і різні формати реклами. Цінові (затратні) аспекти для різних форматів рекламних оголошень були визначені шляхом спостережень. Задача сформульована як задача цільового програмування з багатокритеріальними випадковими обмеженнями.

Реклама, яка на початку свого існування розглядалась як необхідні витрати на інформування покупців, тепер набуває функції генератора прибутку. Ефективність реклами визначається аналізом співвідношення між прибутком і рекламними витратами [1], [2]. Таким чином, поняття «інвестиція» більш точно висловлює економічну складову реклами. Дуже важливо, щоб реклама досягала потенційних споживачів і не охоплювала аудиторію, яка не купуватиме продукцію [3]. Крім того важливою є оптимізація розподілу рекламного бюджету компанії з метою максимізації досяжності до цільової аудиторії.

Таргетинг (адресність реклами) – маркетинговий механізм, використання якого дозволяє виділяти з загальної аудиторії цільову категорію (потенційних споживачів) і демонструвати їй рекламні повідомлення [4].

Математичну модель таргетингового розміщення реклами представлена у вигляді оптимізаційної задачі з мінімізацією цільової функції та сукупністю обмежень. Оскільки параметри обмежень задачі, та параметри цільової функції є випадковими величинами (містять випадкові компоненти) то оптимізаційна задача є задачею ймовірнісного характеру і розв’язується за допомогою методів стохастичного програмування. Імовірнісний характер завдань планування часто пояснюється неповнотою інформації про їх умови або для точного вирішення складної детермінованої задачі, потрібний занадто великий обсяг обчислень.

Тоді доцільно звести задачу до імовірнісної, хоча вся інформація відома. Обсяг обчислень при цьому істотно скорочується.

Застосовується двоетапна лінійна модель стохастичного програмування. Особа, яка приймає рішення на першому етапі виконує певні дії (встановлюється певний оптимальний план, задача є детермінованою і її результатом є вектор з детермінованими компонентами), після яких відбуваються випадкові події, що впливають на результат рішення першого етапу. На другому етапі може бути прийнято корегуюче рішення, що компенсує будь-які небажані наслідки рішення першого етапу у відповідності до реальних умов. Оптимальним розв'язком такої моделі є єдине рішення першого етапу і множина коригуючих рішень, що визначають, дію, яку необхідно виконати на другому етапі у відповідь на кожний випадковий результат.

Модель цільового програмування (ЦП)дозволяє брати до уваги одночасно декілька критеріїв в задачах про вибір найбільш прийнятного рішення у множині допустимих рішень. Тобто, ЦП розроблено таким чином, щоб знайти розв'язок, який мінімізує відхилення між рівнем досягнення критеріїв і цілей, встановлених для них. У випадку перевищення критерія відхилення вважається додатнім (позитивним), у випадку недосягнення мети відхилення вважається від'ємним (негативним). Модель формулюється таким чином, що реклама повинна досягти тих, хто є потенційним споживачем продукту і не досягати тих, хто ними не є. Задача моделюється як задача цільового програмування з випадковими обмеженнями, оскільки параметри досяжності (до цільової групи) розглядаються як випадкові величини. Передбачається, що випадкові величини, які відповідають досяжності, є величинами з відомими математичним сподіванням і середнім квадратичним відхиленням. Параметр, що відповідає досяжності, може бути визначеним шляхом знаходження ідеального розв'язку та закону за яким змінюються значення параметра.

Розроблено стратегії оптимального розміщення реклами в інтернеті на основі моделі ЦП, яка б дозволяла максимізувати досяжність до цільової аудиторії. У зв'язку з цим вирішується задача вимірювання ефективності реклами на різних носіях. У випадку розміщення реклами в інтернеті можна точно виміряти появу реклами і відгук на неї. Як наслідок, можна визначити кількість інвестицій в рекламу і прибуток від неї.

Литература:

1. Charnes A., Cooper W.W., Ferguson R. Optimal estimation of executive compensation by linear programming / A. Charnes, W.W. Cooper, R. Ferguson // Management Sciences 1,1955.-P. 138–151.

2. Charnes A., Cooper W.W., DeVoe J.K., Learner D.B., Reinecke W. A goal programming model for media planning / A. Charnes, W.W. Cooper, J.K.DeVoe, D.B. Learner // Management Science 14, 1968.-P. 422–430.

3.ЦиганокВ.В. Комбінаторний алгоритм парних порівнянь зі зворотним зв'язком з експертом / В.В. Циганок// Реєстрація, зберіганняіоброб. даних. — 2000. — Т. 2, № 2. — С. 92–102.

4. De Kluyver C.A. Hard and soft constraints in media scheduling / C.A. De Kluyver // Journal of Advertisement Research 18, 1978.-P. 27–31.

ЩебланінЮ.М.
К.т.н., с.н.с., доценткаф.Управлінняінформаційноюбезпекою
Державний університет телекомунікацій
м.Київ
Пивовар О.П.
С.н.с. Центру воєнно-стратегічних досліджень
Національного університету обориниУкраїни
м .Київ

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ERP-СИСТЕМ

В якості базового інструменту, який використовується підприємствами для автоматизації своїх бізнес процесів все частіше використовуються так звані ERP-системи (ERP – Enterprise Resource Planning), тобто системи планування ресурсів підприємства.

Оскільки ERP-система в більшості випадків виступає як головна інформаційна система компанії, вона містить в собі великий обсяг інформації необхідної для забезпечення повсякденної роботи всіх підрозділів організації. Ця інформація містить також і цілий ряд конфіденційних даних, втрата або спотворення яких можуть обернутися істотними збитками для компанії, причому як фінансовими, так і збитків від втрати репутації.

Таким чином успішність впровадження та подальшої експлуатації ERP-системи напряму залежить від того, наскільки вона захищена від можливих загроз інформаційній безпеці, які можуть бути пов'язані з порушенням конфіденційності, цілісності та доступності інформаційних ресурсів.

Перш, ніж визначитися із засобами забезпечення інформаційної безпеки ERP-систем, необхідно зрозуміти, які саме компоненти або взаємозв'язки повинні бути об'єктами подібного захисту.

В цілому, виділяють три групи об'єктів:

1. Дані, що передаються між окремими компонентами системи.
2. Дані, які зберігаються безпосередньо в базі даних (БД) системи.
3. Сервери ERP-систем.

При передачі інформації між окремими елементами ERP-системи може відбутися порушення її конфіденційності методом перехоплення і подальшого аналізу трафіку мережі; для запобігання подібних ситуацій використовуються засоби шифрування інформації, що передається. Також в процесі передачі інформації може відбутися її навмисне перекручування і порушення цілісності переданих даних - щоб уникнути подібних випадків застосовуються вбудовані інструменти захисту від несанкціонованого втручання в процеси передачі даних.

Несанкціонований доступ до даних в базі даних ERP-систем може здійснюватися як безпосередньо з консолі управління БД, так і віддалено. Метою його може бути ознайомлення з вмістом бази даних або ж несанкціонована зміна інформації, що зберігається в БД.

Загрозу серверам БД ERP-систем становлять інформаційні атаки, що реалізуються методом використання програмного - апаратних засобів самої системи.

Саме об'єкти захисту та можливі загрози обумовлюють засоби забезпечення інформаційної безпеки ERP-систем, які можна поділити на наступні групи:

1. Засоби, що забезпечують безпеку мережевої інфраструктури. Серед основних засобів є шифрування трафіку, необхідно визначитися тільки з застосуванням криптографічних протоколів. Оскільки в сучасних ERP-система, система взаємодії побудована на базі використання веб-стандартів то для захисту трафіку в середині системи доцільно застосовувати протокол HTTPS. Операційні системи на базі яких створюються ERP-системи, в своїй більшості, містять вбудовані засоби на основі міжнародних криптографічних алгоритмів для застосування HTTPS протоколу, проте з юридичної точки зору необхідно застосовувати сертифіковані криптоалгоритми відповідно до вимог ДСТУ.

В той же час зазначені алгоритми не входять в базовий комплект більшості ERP-систем, а їх впровадження вимагає додаткових ресурсів.

2. Засоби для захисту БД, які включають в себе фізичне ізолювання сервера з БД ERP-системи в окремому приміщенні і налаштування операційної системи, яка не дає користувачам прямого доступу до БД, доступ повинен здійснюватися через сервер додатків.

3. Засоби захисту серверів ERP-систем. До них відносяться: система ідентифікації користувачів, розмежування прав доступу, автентифікація за допомогою цифрових сертифікатів і т.д.

4. Засоби оцінки захищеності, призначені для своєчасного виявлення та усунення вразливостей програмного забезпечення ERP-системи.

5. Заходи захист від витоку конфіденційної інформації, призначені для контролю доступу користувачів.

6. Пакет нормативно-методичних документів, що дозволяють регламентувати експлуатацію і супровід комплексу захисту ERP-системи (політики інформаційної безпеки ERP-системи верхнього середнього та нижнього рівнів).

Перераховані групи складають основу інформаційної безпеки, а їх реалізація забезпечить ефективний захист ERP-системи від зовнішніх і внутрішніх інформаційних атак.

Платоненко А. В.
Аспірант, асистент каф. Систем захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПРИСТРОЇВ У КОРПОРАТИВНИХ МЕРЕЖАХ

В наші часи загрози інформаційної безпеки можуть з'являтись дуже часто, адже кожного дня зловмисники знаходять нові вразливості, завдяки яким можуть нанести шкоду для компаній чи державних установ.

За даними компанії, що являється одним з світових лідерів антивірусного захисту, Україна зайняла 5 місце у світовому рейтингу з ризику зіткнення з веб-загрозами. За третій квартал 2015 року третина(33,7%) користувачів антивірусного продукту зіткнулась із загрозами, які розповсюджується через інтернет. Проблемою є відсутність оновлення програмного забезпечення та використання піратських програм. Біля 17% зараження було здійснено на користувачів застарілої WindowsXP. Також проблемою є програми, які вимагають гроші, та шифрувальні програми, які блокують доступ до системи, шифрують файли, доступ до яких не можливий без спеціального ключа, за який треба заплатити. Окрім цього великою проблемою є соціальна інженерія.Зловмисники завдяки соціальним мережам, фішинговим та зловмисним сайтам розповсюджують свої програми. Таким чином може постраждати не тільки користувач особисто, а і компанія, працівником якої він є.

За статистичною інформацією компанії «Microsoft»:

- 243 дні атакуючий знаходиться в мережі компанії, до того як його буде виявлено;
- 76% вдалих атак на мережу здійснюється через зламані облікові записи користувачів;
- 500 млрд. $ становить матеріальний збиток від кіберзлочинництва в зальносвітовому масштабі;
- 3,5 млн.$ становить середній збиток від злому для компанії.

Саме тому за останні два роки вдвічі більше фахівців різних компаній приділяють перше місце по важливості питанню інформаційної безпеки.

Оскільки велика кількість компаній завдяки соціальним мережам спілкуються зі своїми клієнтами, то необхідно забезпечити певний рівень захисту користувачів від можливих загроз. Якщо раніше просто блокувались такі сайти, щоб працівники не відволікались від роботи, то зараз їх використання є необхідністю і на допомогу цьому приходять NGFW (NextGenerationFirewall– мережеві екрани нового покоління), завдяки яким можливо обмежити трафік по категоріям та відслідковувати поведінку користувачів, надати доступ необхідним пристроям до певних сайтів, файлів, програм та оцінити можливі ризики від них.

Гололобов Д.О.
Доцент каф. Обчислювальної техніки
Державний університет телекомунікацій
м. Київ, Україна

WEB 3.0: ЗАГАЛЬНІТЕНДЕНЦІЇ ТА ПРОБЛЕМИ РОЗВИТКУ

Однією із головних складностей розгляду окресленого питання є відсутність серед web-спеціалістів відносно чіткого та певного розуміння того, що саме розуміти під Web 3.0.Головним чином, це пояснюється відсутністю однієї чіткої тенденції розвитку Web. Натомість існує декілька напрямів. Одним із них є семантичний web (SemanticWeb), який полягає в створенні метамови, на якій будуть будуватися так звані семантичні версії сайтів, які міститимуть інформацію про сайт, яка правдиво описує його контент, цінну для машин і при цьому неважливу для користувачів [1].Елементи SemanticWeb, зокрема, присутні на офіційному web-сайті Національної бібліотеки України ім. Вернадського[2]. Зрозуміло, що одним із головних напрямів семантичного web є його орієнтація на потреби пошуковиків.

Існують різні думки про те, яким повинен бути Web 3.0.Однією з них є теза про перехід Інтернету від кількісних показників (як у Web 2.0) до якісних і передавання професіоналам головної ролі в створенні контенту. [3].Іншою думкою є думка про те, що Web 3.0 повинен стати епохою комерційного web[4, с. 236].

Дивлячись у минуле, зовсім нескладно цілком чітко і впевненовідповісти на питання: що таке Web 1.0 та Web 2.0? Отже, Web 1.0 – це, головним чином, статичні web-ресурси із бідною гіпертекстовою розміткою та стильовим оформленням і наявність чатів та форумів, як засобу інтерактивного спілкування. Іншими словамиWeb 1.0 – це надання користувачу контенту. Web2.0 –соціальні мережі,або інакшеWeb 2.0 – це залучення користувачів до створення контенту.Цікаво відмітити, що термін Web 1.0 з'явився, власне, після появи того, що було назване, як Web 2.0.

Але, незважаючи ні на що, концепція Web 3.0 активно просувається і упроваджується. І той факт, що коженрозуміє її по-своєму не став на заваді цьому. Проте оскільки кожен розуміє під Web 3.0 своє, то й просувається одночасно чимала кількість досить різнорідних ідеї та технологій. Утім, не зважаючи на це, можна цілком впевнено сказати, що Web 3.0 існує і розвивається.Таким чином, не порушуючи загальності, під Web 3.0на даний момент можна розуміти основні тренди розвитку Web.Однак, зовсім не виключений і такий варіант, що Web-ом 3.0 згодом назвуть цілий ряд течій уWeb.

Із точки зору web-дизайну, як складової частини web-концепції, ситуація є дещо простішою. Цілком зрозумілим є те, що останній він повинен ґрунтуватися на найповнішому використанні нових технологій, тобто HTML5 та CSS3 і web-технологій на їхній основі або суміжних з ними. І тут у якості прикладу можна назвати декілька сайтів, що близькі до відтворення зазначеного[4, с. 237]:

http://www.flickr.com– сайт обміну фотографіями;

https://www.youtube.com – сайт обміну відеофайлами та відеоканали;

http://mozilla.org – web-сторінка компанії Mozilla;

https://www.blogger.com – сервіс блогів від Google;

http://twitter.com – платформа Twitter.

Таким чином, підсумовуючи вищесказане, можна сказати, що загальними проблемами Web3.0 є:

– відсутність єдиної парадигми, а отже, і однієї стійкої тенденції розвитку web;

– відсутність загальних підходів до того, як і ким повинен створюватися контент;

– тенденція до удорожчання технологій (як за умови створення семантичних версій сайтів, так й у випадку залучення професіоналів до створення контенту, а тим більше, за умови збільшення комерціалізації Інтернету).

Література:

1.Web 3.0. Эпоха предсказаний.// http://i-novice.net/web-30-epoxa-predskazanij.

2.Національна бібліотека України імені В. І. Вернадського. Офіційний web-сайт. // http://www.nbuv.gov.ua/

3.Web 3.0, the "official" definition.// http://calacanis.com/2007/10/03/web-3-0-the-official-definition.

4.Сырых Ю. А. Современный веб-дизайн. Эпоха Веб 3.0. Издательство: Вильямс, 2013. - 374.

Романчук Б.М.
Аспірант, М.Н.С.
Інститут газу Національної Академії Наук України
м. Київ, Україна

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ТЕРМІЧНОЇ ПЕРЕРОБКИ БІОМАСИ

В зв’язку з підвищенням вартості енергетичних палив, гостро стала проблема економії коштів. Це можна реалізувати за допомогою використання біосировини. Такою біосировиною можуть стати відходи сільського господарства, такі як солома, лушпиння соняшникового насіння, відходи деревообробки. Хоча біомасса має ряд недоліків.

Недоліки біомаси як палива:

-наявність води;

-низька питома вага;

-низька теплота згоряння;

-схильність до розкладання та самозапалення.

Істотною проблемою є транспортування такого біопалива оскільки через низьку щільності біомаса має низьку теплотвірну здатність на м^3. Тому відзначена необхідність підготовки для зменшення вартості транспортування та спалювання такого палива.

Термічна обробка дозволяє перетворити біомасу на продукт, що не містить вологи. При цьому змінюються і інші її властивості: калорійність, насипна щільність. Матеріал після такої обробки стає більш крихким, що полегшує його подрібнення.Такий процес термообробки як торифікація, і є початковою стадією пірогенетичного розпаду, характеризується утворенням пірогенетичної води, двоокису і окису вуглецю.

При торифікації з твердого палива (торф, біосировина) виділяються пари і сорбовані його поверхнею гази (CO_2, CH_4 та ін) [1, с.133]; тверда речовина палива розкладається незначно, але її поверхня стає більш активна до процесів горіння, теплота згоряння підвищується пропорційно зменшенню вологи і сорбованих газів. При температурах понад 300 ° С починається деструкція твердої маси палива, в результаті розпаду молекул з нього виділяються летючі речовини - рідкі вуглеводневі сполуки та горючі гази.

Термообробка відбувається в чотири етапи:

-підсушка (до 100^{o}С);

-догрів до температури витримки;

-витримка при заданій температурі, певний час;

-охолодження палива.

В процесі термообробки біомаси відбувається: вихід летких, підсушка палива [2, с.272], зміни в структурних і міжмолекулярних зв'язках, зменшується кількість кисню[3. с.88] в хімічному складі речовини таким чином підвищується теплотворна здатність. Також термооброблена біомаса має значно меншу пористість в порівнянні з необробленим що дозволяє знизити затрати на транспортування.

Отриманні данні на базі експериментального дослідження можуть бути застосовані для поліпшення існуючих та створення нових технологій термічної обробки біосировини, розробити установки із застосуванням методів термообробки біосировини за рахунок теплоти згоряння газу торифікації. Так як таких методів існує невелика кількість, є потреба в розробці нових більш ефективних методів.

Література:

1. Григорьев В. А. и Зорин В. М., Тепловые и атомные электрические станции. Справочник. – М.: Энергоиздат, 1982.-617с.

2. Дитнерський Ю. И., Основные процессы и аппараты химической технологии. Пособиепопроектированию. – М.: Химия, 1991.-496с.

3. P. Rousset, L. Macedo, J.-M. Commandre, A. Moreira,Journal of Analytical and Applied Pyrolysis 96 (2012)86-91 “Biomass torrefaction under different oxygen concentrations and its effect on the composition of the solid by-product“ 2012.-91с.

Манько О.О.
Д.т.н.,професор
Одеська національна академія зв'язку ім. О.С. Попова,
Одеса, Україна
Скубак О.М.
доцент кафедри ПП
Державний університет телекомунікацій
м.Київ, Україна

ПИТАННЯ НАДІЙНОСТІ ОПТИЧНИХ ВОЛОКОН, ПОВ'ЯЗАНІ З ОСОБЛИВОСТЯМИ ПРОКЛАДАННЯ ОПТИЧНИХ КАБЕЛІВ

На цей час мають місце розробки типів оптичних волокон (ОВ), які призначені підтримувати нові технології волоконно-оптичного зв'язку. Зокрема до цих типів належать оптичні волокна, що відповідають Рекомендації ITU-T (МСЭ-Т) G.657 [1]. Вони являють собою оптичні волокна зі зменшеними втратами на малих радіусах вигину, та призначені для монтажу оптичного обладнання в обмеженому просторі – в будівлях та розподільчих шафах, а також при малому розмірі муфт та оптичних розподільчих боксів. Волокна розподілені на категорії А1, А2, В2, В3. При цьому ОВ типу G.657 А1,А2 застосовують в різних аспектах мереж доступу, як такі, що забезпечують вигин з радіусом не нижче 10 мм. В той же час ОВ типу G.657 В2,В3 призначені для мереж доступу як такі, що забезпечують вигин з радіусом не нижче 7,5 мм. Такий невеликий допустимий радіус вигину призводить до порівняно значних деформацій оптичного волокна та до виникнення механічних напруг в ньому. При цьому деформації оптичного волокна та механічні напруги є причиною появи в ньому мікротріщин та повільному збільшенні їх розмірів, що кінець кінцем викликає повний розрив волокна [2]. Таким чином надійність та довговічність оптичного волокна залежить його деформації, яка однозначно пов'язана з механічною напругою в ньому та, відповідно, з надійністю та часом функціонування волокна. Враховуючи необхідність виконання вигинів оптичного волокна під час монтажу оптичних муфт, оптичних боксів та прокладання його всередині приміщень представляється необхідним провести оцінку його надійності в залежності від радіусу вигину та надати необхідні рекомендації щодо його обмежень.

Як показують результати досліджень, надійність оптичного волокна, що описується ймовірністю його відмови, залежить від навантаження, яке діяло на нього, а також від постійно діючого в процесі експлуатації навантаження на оптичне волокно [2]. Згідно з [2], надійність та безвідмовність оптичного волокна, що знаходиться під натягом, визначається теорією росту мікротріщин, які мають місце у волокні. Враховуючи це, все волокно при виготовленні проходить випробування на натяг для виявлення тріщин та інших пошкоджень. Цей тест називається Proof test (випробування на міцність), і означає що волокно підлягає певному натягу на протязі приблизно однієї секунди [3]. При цьому тріщини у волокні можуть викликати його відмову (обривщини , та фактор критичного навантаження.

При проектуванні та прокладанні мереж доступу необхідно вибирати радіус вигину оптичних кабелів та волокон з урахуванням не тільки їх допустимого радіусу вигину, але й терміну експлуатації. Особливу увагу треба в цьому випадку приділити оптичним волокнам, що відповідають Рекомендації МСЕ G.657, оскільки допустимий радіус вигину в них помітно менший за такий, що забезпечує задовільний термін експлуатації.

ньому.

При проектуванні оптичних кабельних мереж для внутрішнього прокладання необхідно враховувати такий фактор, як радіус вигину оптичного кабелю та оптичного волокна в стаціонарних умовах експлуатації. Особливу увагу треба звернути на нові типи волокна, для яких допустимий, згідно зі стандартами МСЕ, понижений радіус вигину. При цьому треба перевірити відповідність проектного радіусу вигину вимогам до терміну функціонування оптичної мережі та за необхідності скоректувати його значення.

Література:

1. Characteristics of a bending-loss insensitive single-mode optical fibre and cable for the access network // ITU-T Recommendation G.657.

2. Yutaka Mitsunaga, Yutaka Katsuyama, Hirokazu Kobayashi, Yukinori Ishida // Journal of Applied Physics. – 1982. – Vol.53, №7. – P.4847-4853.

3. Definitions and test methods for linear, deterministic attributes of single-mode fibre and cable // ITU-T Recommendation G.650.1

Масесов М.О.

Начальник науково-дослідного відділу к.т.н.,с.н.с.

Саула О.А.

Провідний науковий співробітник науково-дослідного відділу

Науковий центр зв’язку та інформатизації

Військового інституту телекомунікацій та інформатизації

м. Київ, Україна

АНАЛІЗ ВИКОРИСТАННЯ ТА ПОДАЛЬШОГО РОЗВИТКУ ЗАСОБІВ ТРОПОСФЕРНОГО ЗВ’ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Аналіз організації та забезпечення зв’язку у ході виконання завдань в антитерористичній операції на сході України підрозділами та військовими частинами Збройних Сил України показав нові тенденції у поглядах щодо планування та розгортання системи зв’язку військового призначення.

Принциповими відмінностями у організації зв’язку є відмова від побудови багатоінтервальних радіорелейних і тропосферних ліній зв’язку, прокладання польових кабельних ліній зв’язку на великі відстані, практична відсутність польової опорної мережі зв’язку Збройних Сил України. Зазначені відмінності викликані проблемними питаннями щодо забезпечення охорони та оборони радіорелейних станцій ретрансляції та польових кабельних ліній в умовах дій незаконних збройних формувань, диверсійно-розвідувальних груп противника та ворожо налаштованого населення у районах виконання завдань.

Тому цілком очевидним стає факт широкого використання ліній прив’язки до телекомунікаційних мереж операторів телекомунікацій України, а також ліній прямого зв’язку між пунктами управління тактичної, оперативної та стратегічної ланок.

Лінії прив’язки використовуються при підключенні до телекомунікаційних вузлів у населених пунктах. В польових умовах, з урахуванням набутого досвіду в АТО, найчастіше використовуються лінії прямого зв’язку. Для організації ліній прямого зв’язку найбільш доцільним є використання супутникових та тропосферних засобів зв’язку. На теперішній час супутникові засоби зв’язку, з причини відсутності національного супутника, арендуються. Вартість аренди ресурсів супутникового зв’язку складає кілька сотен тисяч гривень щомісяця. Тому використання тропосферних засобів зв’язку є актуальним.

В свою чергу, існуючі засоби тропосферного зв’язку не забезпечують передавання Ethernet-трафіку. Таким чином, створення нових та модернізація існуючих станцій тропосферного зв’язку є важливим науковим та практичним завданням.

Щодо створення нових станцій тропосферного зв’язку найбільш доцільним є впровадження малогабаритних возимих та носимих засобів. Розвиток сучасних технологій дозволяє використовувати твердотільні підсилювачі з невеликими масогабаритними показниками. Підприємствами вітчизняної промисловості вже виконані відповідні наукові дослідження та варіанти практичної реалізації зазначеного підходу.

Другий варіант – модернізація існуючих тропосферних станцій – передбачає використання цифрових модемів разом з існуючим обладнанням станцій тропосферного зв’язку. Такий підхід є значно меншим за вартістю у порівнянні із створенням нових засобів. Проведені науково-практичні дослідження підтверджують можливість реалізації такого підходу з використанням цифрових модемів вітчизняного виробництва. Разом із використанням просторового рознесення антен та існуючих методів обробки сигналів можливо досягти швидкостей порядка від 512 кбіт/сек до 5 Мбіт/сек на станціях тропосферного зв’зку типу Р-412, Р-417, Р-423.

Подальшими напрямками досліджень є розробка та впровадження перспективних методів цифрової обробки сигналів у цифровому сегменті станцій тропосферного зв’язку. Використання технологій багатоантенного рознесення (MIMO), ортогональної і неортогональної частотної дискретної модуляції (OFDM та N-OFDM) дозволить підвищити якість зв’язку та пропускну спроможність тропосферних каналів без збільшення потужності випромінювання та заміни антенного обладнання. Актуальним залишається питання створення радіорелейно-тропосферних станцій зв’язку, що можуть працювати в умовах прямої видимості (радіорелейних режим) із збільшенням пропускної спроможності.

Жданова Ю.Д
Доцент каф.Інформаційної та кібернетичної безпеки
Делікатний А.О
Студент навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

МЕТОДИ ТА ЗАСОБИ ОБРОБКИ ЗОБРАЖЕНЬДЛЯ ПІДВИЩЕННЯ ДОСТУПНОСТІ ТА ЦІЛІСНОСТІ ІНФОРМАЦІЙНОГО РЕСУРСУ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ

Впровадження новітніх інформаційних систем і технологій в системи управління державних органів влади, бізнес-структури, установ освіти і медицини впливає на якість управління, своєчасність прийняття рішень та їх доведення. Зниження ефективності обробки та підвищення часових затримок, викликані процесами передачі та обробки відеоінформації вреальному часі, призводять до порушення безпеки інформації.[1,2]

У системах управління спеціального призначення (Збройні Сили, МВС) в даний час широко застосовуються системи відеоконференцзв'язку (ВКЗ). Дані системи є базовою компонентою організації управління і забезпечення об'єктивного контролю.

Інформаційний ресурс систем ВКЗ дуже чутливий до втрат пакетів, часових затримок, а також до помилок, що виникають в інфокомунікаційних системах в процесі обробки, збереження і передачі.

В даний час в інфокомунікаційних системах спеціального призначення реалізовані методи, які орієнтовані в основному на забезпечення захисту інформації, в першу чергу її конфіденційності, вирішення завдань розмежування та контролю доступу до відеоінформаційного ресурсу.

Неоднорідність структури існуючих інфокомунікаційних систем, обмежені характеристики продуктивності реалізованих технологій передачі та обробки інформації призводять до спотворень і порушень оброблюваної відеоінформації, до порушення таких категорій безпеки інформації, як її доступність і цілісність.[3,4]

Один з напрямків вирішення даної задачі - застосування технологій компресії відеоінформації.

Це дозволить:

а) розробити позиційне кодування трансформант перетворення. У результаті такого кодування скорочується комбінаторна надмірність у трансформанта, що забезпечує підвищення ефекту стиснення і зменшує втрати інформації через брак розрядів в машинному слові;

б) ввести можливість диференційованої обробки зображень, яка дозволяє: адаптувати надмірність зображення під клас семантичної структури; зберегти, з одного боку, семантику зображень, а з іншого - забезпечити необхідний рівень стиснення і як наслідок доступності відеозображень;

в) Розробити двокаскадні схеми маскування зображень, які дозволяють підвищити якість маскування і скоротити сумарний час обробки, усунути недоліки окремо використовуваних методів маскування із збереженням переваг технології маскування в цілому.

г) Розробити метод інтелектуальної диференційованої обробки відеозображень для їх компактного представлення з метою підвищення безпеки відеоінформації, а саме її доступності та цілісності, заснований на:

1.Застосуванні каскадної схеми детектування і локалізації семантичної інформації (контурів об'єктів) в відеозображенні із заданою якістю;

2.Виконанні аналізу відеозображення та класифікації його фрагментів за ступенем насиченості контурами;

3.Визначенні базових компонент технології та параметрів методу компресії в залежності від ступеня семантичної насиченості;

4.Компресії відеоданих з збереженням семантично значимої інформації та контролем якості компактного представлення.

Література:

1.Горбулін В.П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В.П. Горбулін, М.М. Биченок, П.М. Копка

2.Богуш В.М. Інформаційнабезпекадержави /В.М. Богуш, О.К. Юдин. К.: МК–Прес, 2005. 432 с. 5

3.Ватолин В.И. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В.И. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. М.: ДИАЛОГ – МИФИ, 2002

4.Власов А.В. Анализ методов обнаружения границ объектов на изображениях и их классификация / А.В. Власов, В.В. Баранник, А.В. Яковенко // Сучаснаспеціальнатехніка. 2012. Вип. 3 (30).

Курченко О.А.
Доцент каф.Управління інформаційною безпекою
Державний університет телекомунікацій
м. Київ, Україна
Храпач Г.С.
Молодший науковий співробітник Центру воєнно-стратегічних досліджень
Національного університету оборони України імені Івана Черняховського
м. Київ, Україна

ПОБУДОВА ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Виявлення вторгнень залишається областю активних досліджень вже протягом трьох десятиліть. Вважається, що такий напрям започаткував Джеймс Андерсон в 1980 році статтею "Моніторинг погроз комп'ютерній безпеці". В 1987 році цей напрям був розвинений публікацією статті "Про модель виявлення вторгнення" Дороті Деннінг. Вона забезпечила методологічний підхід, що надихнув багато дослідників і що заклав основу для створення комерційних продуктів в області виявлення вторгнень [1].

Питання реалізації та забезпечення інформаційної безпеки (ІБ) прямо входять в сферу відповідальності керівника ІТ-департаменту (якщо компанія велика) або ІТ-відділу або ІТ-служби. Економія на інформаційній безпеці може виражатися в різних формах, крайніми з яких є: прийняття тільки найзагальніших організаційних заходів забезпечення безпеки інформації в інформаційній системі (ІС), використання тільки простих додаткових засобів захисту інформації (ЗЗІ). У першому випадку, як правило, розробляються численні інструкції, накази та положення, покликані в критичну хвилину перекласти відповідальність з людей, які видають ці документи, на конкретних виконавців. Природно, що вимоги таких документів (за відсутності відповідної технічної підтримки) ускладнюють повсякденну діяльність співробітників організації і, як показує досвід, не виконуються. У другому випадку купуються і встановлюються додаткові засоби захисту. Застосування ЗЗІ без відповідної організаційної підтримки та планового навчання також неефективно у зв'язку з тим, що без встановлених жорстких правил обробки інформації в ІС і доступу до даних використання будь-яких ЗЗІ тільки підсилює існуючий безлад.

Як показує досвід практичної роботи, для ефективного захисту ІС організації необхідно вирішити ряд організаційних завдань:

створити спеціальний підрозділ, що забезпечує розробку правил експлуатації корпоративної ІС, що визначає повноваження користувачів по доступу до ресурсів цієї системи та здійснює адміністративну підтримку засобів захисту;

розробити технологію забезпечення ІБ, що передбачає порядок взаємодії підрозділів організації з питань безпеки при експлуатації ІС та модернізації її програмних і апаратних засобів;

впровадити технологію захисту інформації шляхом розробки та затвердження необхідних нормативно-методичних та організаційно-розпорядчих документів (концепцій, положень, інструкцій і т. п.), а також організувати навчання всіх співробітників, які є адміністраторами та користувачами ІС.

При створенні підрозділу ІБ треба враховувати, що для експлуатації простих засобів захисту потрібен мінімальний штат співробітників, що здійснюють підтримку функціонування ЗЗІ. У той же час розробка і впровадження технології забезпечення ІБ вимагає значно більшого часу, великих трудовитрат і залучення кваліфікованих фахівців, потреба в яких після її впровадження в експлуатацію відпадає. Крім того, розробка і впровадження такої технології повинні проводитися в стислі терміни, щоб не відстати від розвитку самої корпоративної ІС організації.

Застосування додаткових ЗЗІ зачіпає інтереси багатьох структурних підрозділів організації - не стільки тих, в яких працюють кінцеві користувачі ІС, скільки підрозділів, які відповідають за розробку, впровадження та супровід прикладних задач, за обслуговування та експлуатацію засобів обчислювальної техніки.

Для мінімізації витрат на розробку та ефективне впровадження технології забезпечення ІБ доцільно залучати сторонніх фахівців, що мають досвід у проведенні подібного роду робіт. При цьому, у кожному разі, відповідальність за розробку, впровадження та ефективність роботи захисних систем несе вище керівництво компанії.

Технологія побудови ІБ повинна забезпечувати:

диференційований підхід до захисту різних АРМ і підсистем;

максимальну уніфікацію ЗЗІ з однаковими вимогами до безпеки;

реалізацію дозвільної системи доступу до ресурсів ІС;

мінімізацію рутинних операцій та узгодженість дій різних підрозділів, щодо реалізації вимог розроблених положень та інструкцій, не створюючи великих незручностей при вирішенні співробітниками своїх основних завдань;

облік динаміки розвитку ІС, регламентацію не тільки стаціонарного процесу експлуатації захищених підсистем, але і процесів їх модернізації, пов'язаних з численними змінами апаратно-програмної конфігурації АРМ;

мінімізацію необхідного числа фахівців відділу, що займаються захистом інформації.

Зазвичай системи захисту мережі та антивірусні програми будуються за таким принципом: інформація про нові віруси заноситься в базу даних (сигнатур) такої системи. Але часу реагування на загрозу в такому випадку недостатньо. Поки дані про новий вірус будуть редагуватись - велику кількість комп’ютерів вже буде заражено [2].

У залежності від масштабу компанії можна виділити три основні класи мереж: центральна мережа міжнародної розподіленої компанії, яка може нараховувати сотні і тисячі вузлів; мережа регіональної філії, що налічує кілька десятків або сотень вузлів; мережі невеликих філій або домашні (мобільні) комп'ютери, що підключаються до центральної мережі.

Можна також виділити три основні сценарії забезпечення інформаційної безпеки для цих класів мереж, що розрізняються різними вимогами щодо забезпечення захисту інформації.

Перший сценарій забезпечує мінімальний рівень захищеності за рахунок можливостей мережевого обладнання. Залежно від масштабів мережі, що захищається, ці можливості (захист від підміни адрес, мінімальна фільтрація трафіку, доступ до устаткування по паролю і т. д.) реалізуються в магістральних маршрутизаторах - наприклад, Cisco 7500 або Nortel BCN, маршрутизаторах регіональних підрозділів - наприклад, Cisco 2500 або Nortel ASN, і маршрутизаторах віддаленого доступу - наприклад, Cisco 1600 або 3ComOfficeConnect. Великих додаткових фінансових витрат цей сценарій не вимагає.

Другий сценарій, що забезпечує середній рівень захищеності, реалізується вже за допомогою додатково придбаних засобів захисту, до яких можуть бути віднесені нескладні міжмережеві екрани, системи виявлення атак і т. п. У центральній мережі може бути встановлений міжмережевий екран (наприклад, CheckPoint Firewall - 1), на маршрутизаторах можуть бути налаштовані найпростіші захисні функції, що забезпечують першу лінію оборони (списки контролю доступу і виявлення деяких атак), весь вхідний трафік перевіряється на наявність вірусів і т. д. Регіональні офіси можуть захищатися більш простими моделями міжмережевих екранів. При відсутності в регіонах кваліфікованих фахівців рекомендується встановлювати програмно-апаратні комплекси, які централізовано керуються і не потребують складної процедури введення в експлуатацію (наприклад, CheckPoint VPN - 1 Appliance на базі Nokia IP330).

Третій сценарій, що дозволяє досягти максимального рівня захищеності, призначений для серверів e-Commerce, Internet-банків і т. д. У цьому сценарії застосовуються високоефективні і багатофункціональні міжмережеві екрани, сервери аутентифікації, системи виявлення атак і системи аналізу захищеності.

Для виявлення вразливих місць, які можуть бути використані для реалізації атак, можуть бути застосовані системи аналізу захищеності (наприклад, сімейство SAFE - suite компанії Internet Security Systems). Аутентифікація зовнішніх і внутрішніх користувачів здійснюється за допомогою серверів аутентифікації (наприклад, CiscoSecure ACS). Ну і, нарешті, доступ домашніх (мобільних) користувачів до ресурсів центральної та регіональних мереж забезпечується по захищеному VPN-з'єднання. Віртуальні приватні мережі (Virtual Private Network - VPN) також використовуються для забезпечення захищеної взаємодії центрального та регіональних офісів. Функції VPN можуть бути реалізовані як за допомогою міжмережевих екранів (наприклад, CheckPoint VPN - 1), так і за допомогою спеціальних засобів побудови VPN.

Авторизоване навчання та підтримка допоможуть швидко ввести систему захисту в експлуатацію і налаштувати її на технологію обробки інформації, прийняту в організації. Орієнтовна вартість оновлення складає близько 15-20% вартості програмного забезпечення. Вартість річної підтримки з боку виробника, яка, як правило, вже включає в себе оновлення ПЗ, становить близько 20-30% вартості системи захисту. Таким чином, щороку потрібно витрачати не менше 20-30% вартості ПЗ на продовження технічної підтримки ЗЗІ.

Стандартний набір засобів комплексного захисту інформації у складі сучасної ІС зазвичай містить наступні компоненти:

засоби забезпечення надійного зберігання інформації з використанням технології захисту на файловому рівні (FileEncryption System - FES);

засоби авторизації і розмежування доступу до інформаційних ресурсів, а також захист від несанкціонованого доступу до інформації з використанням систем біометричної авторизації і технології токенів (смарт-карти, touch-memory, ключі для USB-портів і т.п.);

засоби захисту від зовнішніх загроз при підключенні до загальнодоступних мереж зв'язку (Internet), а також засоби управління доступом з Internet з використанням технології міжмережевих екранів (Firewall) і змістовної фільтрації (Content Inspection);

засоби захисту від вірусів з використанням спеціалізованих комплексів антивірусної профілактики;

засоби забезпечення конфіденційності, цілісності, доступності та автентичності інформації, переданої по відкритих каналах зв'язку з використанням технології захищених віртуальних приватних мереж (VPN);

засоби забезпечення активного дослідження захищеності інформаційних ресурсів з використанням технології виявлення атак (Intrusion Detection);

засоби забезпечення централізованого управління системою інформаційної безпеки відповідно до погодженої та затвердженої Політики інформаційної безпеки компанії.

У залежності від масштабу діяльності компанії методи і засоби забезпечення ІБ можуть різнитися, але необхідно чітко розуміти, що дотримання необхідних вимог щодо захисту інформації неминуче призводить до ускладнення процедури модифікації ІС. Тому проявляються суперечності між забезпеченням безпеки та розвитком і вдосконаленням ІС. Отже, технологія забезпечення інформаційної безпеки повинна бути досить гнучкою і передбачати особливі випадки екстреного внесення змін до програмно-апаратних засобів, які захищають ІС.

Література:

1. Аграновский А. Статистические методы обнаружения аномального поведения трафика.// Информационные технологии – 2005 – №1
2. Домарев В. Безопасность информационных технологий. Системный подход. – К.: ООО „ТИД ДС”, 2009 – 992с.

Краснянський М.С.
Студент ФТК групи ТСД-41
Державний університеттелекомунікацій
м. Київ, Україна

ВПЛИВ НАВМИСНИХ ЗАВАД НА ПРОПУСКНУ СПРОМОЖНІСТЬ ЗАСОБІВ РАДІОЗВ'ЯЗКУ З ТЕХНОЛОГІЄЮMIMO-OFDM

Значний вклад у розвиток сучасних та перспективних систем радіо доступу внісмобільний WiMax (WorldwideInteroperabilityforMicrowave Access – всесвітній доступ для взаємодії мікрохвильових мереж) на основі стандарту IEEE 802.16e (m).

У стандарті IEEE 802.16e (m) визначені два рівні: фізичний і доступу до середовища (MAC-рівень). Такий підхід задовольняв технології безпровідних мереж Ethernet, які використовували протоколи IETF, зокрема, протоколи TCP/IP, SIP, VoIP. Архітектура мобільного WiMax побудована на платформі All-IP (Все-IP), тобто прийнята технологія заснована на передачі і комутації пакетів без використання каналів традиційної телефонії. Такий підхід припускає, що будуть зменшені витрати на всіх етапах "життєвого циклу" (проектування, розгортання, експлуатація) мережі. Переваги принципу All-IP засновані на прогнозах росту мережі за законом Мура, згідно з яким розвиток технологій обробки інформації на основі комп'ютерних систем іде швидше, ніж розвиток засобів телекомунікацій, що відбувається через те, що обробка інформації не обмежена установкою і модернізацією апаратури, як це має місце в мережах з комутацією каналів. Вибір принципу пакетної комутації припускає низьку вартість, високий ступінь нарощування, швидкий розвиток функціональних можливостей, тобто всі переваги систем, заснованих на використанні програмного забезпечення.

Стандарт IEEE 802.16e (m) на фізичному рівні застосовує технології ортогональночастотного мультиплексування OFDM (Orthogonalfrequency-divisionmultiplexing) та багатоантенної техніки „багато входів - багато виходів" (Multiple-inputmultiple-output MIMO) [1]. В літературі це називаєтьсяMIMO-OFDM.

В області сучасних систем відомчого радіозв'язку особливу увагу приділяють програмованим радіостанціям (SDR-softwaredefinedradio), принцип побудови яких заснований на апаратно-програмній реалізації . Програмовані радіостанції наступних поколінь будуть застосовувати декілька режимів роботи: робота з сучасними транкінговимирадіо засобами, КХ/УКХ-радіостанціями та мобільними радіо засобами покоління 3G та 4G, які будуть застосовувати мобільнийWiMax.

Однією з основних умов роботи відомчих засобів радіозв'язку є робота в умовах впливу навмисних завад, тобто завад, які створюються станціями радіоелектронної протидії. При використанні у програмованій радіостанції демодулятора з “м’яким” виходом на етапі проектування використовуються моделі дискретно-неперервного каналу зв’язку [2].

У каналі зв’язку переданий OFDM-сигнал x(t) спотворюється мультиплікативнимита адитивними завадами. Мультиплікативні завади представляються матрицею передачіканалу H. В роботі передбачається, що всі елементи матриці H дорівнюють одиниці. Якадитивні завади розглядаються флуктуаційний шум $n(t)$ та завади $j(t)$.

Вплив навмисних завад на канали програмованихрадіостанцій з технологією MIMO-OFDM істотно знижує їх пропускну спроможність.

Ідея технології MIMO подібна відомому принципу рознесеного прийому, коли в системі зв’язку створюються декілька некорельованих(незалежних) копій сигналу на прийомі. В таких системах реалізується просторове мультиплексування: потік даних на передачі розбивається на два або більше потоків, кожний з яких передається одночасно з іншимизадопомогоюрізниххантен.УтехнологіїMIMOпоєднаніпросторово-часовіметоди приймання з використанням адаптивних антен і методи просторово-часового кодування й просторово-часового розділення сигналів [3].

Підвищити пропускну спроможність каналів програмованих радіостанцій з технологією MIMO-OFDM можна за рахунок збільшення субканалів сигналів OFDM та каналівMIMO.

Література:

1.Khan F. LTE for 4G MobileBroadband. AirInterface Technologies andPerformance / Khan F. – Cam- bridge: CambridgeUniversityPress, 2009. – 509p.

2.А.с. 17007 Україна. Имитационная модель системырадиосвязи с псевдослучайнойперестройкойрабочейчастоты, помехоустойчивымтурбокодированием и функционирующая в условияхрадиоэ-лектронногопротиводействия / С. Зайцев, С. Лівенцев, Б. Горлинський, А. Артюх. – заявл. 19.04.06; опубл. 2006, Бюл. №10.

3.Ergen M. MobileBroadband. IncludingWimaxand LTE / Ergen M. –Berkeley: SpringerSci- ence+BusinessMedia, 2009. – 515p.

Фомін О.О.

Студент каф.Систем технічного захисту інформації

Державний університет телекомунікацій

м. Київ, Україна

МЕТОДИКА ПОБУДОВИ ЗАХИСТУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Сучасні автоматизовані системи (АС), корпоративні і державні, повинні забезпечувати цілісність, конфіденційності і доступність інформаційних та інших ресурсів. Для виконання даних вимог потрібно проаналізувати всі можливі загрози, яки впливатимуть на систему, в АС повинна бути організована політика безпеки та комплексна система захисту інформації (КСЗІ).

Для запобігання можливості реалізації загроз ресурсам АС необхідна розробка і використання в АС комплексної системи захисту інформації. Вимоги до такої системи передбачають централізоване управління засобами та механізмами захисту на основі певної політики інформаційної безпеки. Контроль за дотриманням вимог політики інформаційної безпеки в АС здійснюється Службою захисту інформації та реалізується в плані.

Комплексна система захисту інформації це сукупність організаційно-правових та інженерних заходів, а також програмно-апаратних засобів, які забезпечують захист інформації в АС. Саме на неї нормативними документами покладається завдання забезпечення безпеки функціональних властивостей захищених АС. Це завдання вирішується як технічними, так і програмними засобами базового і прикладного програмного забезпечення (ПЗ), а також з використанням спеціально розроблюваних програмних і апаратних засобів ТЗІ.

Організаційно-правовими заходами реалізується комплекс відповідних нормативних, адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу та визначення порядку функціонування засобів забезпечення безпеки інформаційної діяльності та засобів ТЗІ, а також шляхом створення служб (або призначення адміністраторів безпеки), відповідальних за їх реалізацію.

До таких заходів належать також визначення контрольованих зон і організація контролю доступу в ці зони. Для реалізації заходів цієї групи в більшості випадків не потребує використання додаткових коштів.

Основним завданням інженерних заходів є забезпечення фізичної та інформаційної безпеки.

Головним завданням технічних засобів захисту інформації є запобігання навмисного чи випадкового несанкціонованого доступу (НСД) до інформації та ресурсів АС (з метою ознайомлення, використання, модифікації або знищення інформації) з боку авторизованих користувачів або сторонніх осіб, які знаходяться в межах зон безпеки інформації АС, незалежно від способу доступу до цих зон.

Найбільш значущими для захисту АС є програмні засоби захисту, що дозволяють створювати модель захищеної АС з побудовою правил розмежування доступу, централізовано управляти процесами захисту, інтегрувати різні механізми та засоби захисту в єдину систему, створювати досить зручний, інтуїтивно-доступний користувачу інтерфейс адміністратора безпеки. З урахуванням складності автоматизованої системи, а також необхідності саме комплексного і ефективного використання всіх заходів безпеки, забезпечення високої керованості цими заходами, значна частина повинна приділятись автономній частині АС - її специфічній функціональній компоненті - систему (або, точніше, підсистему) захисту інформації (СЗІ).

При цьому підсистема захисту інформації, як одна з основних в системі технічного захисту інформації, повинна забезпечувати збереження основних функціональних властивостей захищених автоматизованих систем - цілісності, конфіденційності та доступності.

Оцінка здатності АС забезпечувати кожне з цих функціональних властивостей проводиться за сформульованими в нормативних документах з питань ТЗІ системі критеріїв оцінки захищеності системи.

Правове забезпечення комплексних систем інформаційної безпеки України включає в себе наступні основні документи:

НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

Література:

1. Коне І.Р., Бєляєв А.В., Інформаційна безпека підприємства. БХВ-Петербург, 2003.

2. Вертузаев М.С., Юрченко О.М., Захист інформації в комп'ютерних системах від несанкціонованого доступу.

3. Петраков А.В. Основи практичної захисту інформації. Навчальний посібник для вузів., Радіо і зв'язок. 2001.

4. Державна служба спеціального зв`язку та захисту інформації Україниhttp://dstszi.kmu.gov.ua

Спасітєлєва С.О.
К.-ф.-м.н. доцент каф. Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна

ЗАСТОСУВАННЯ АСПЕКТІВ ДЛЯ РЕАЛІЗАЦІЇ ЗАХИСТУ ПРИКЛАДНИХ ПРОГРАМ З ВИКОРИСТАННЯМ ASPECTC++

Пакет AspectC++ [1] є простим та практичним розширенням мови С++, яка дозволяє додавати можливості аспектно-орієнтованого програмування (АОП) в рамках об’єктно-орієнтованої мови С++. Цей пакет може вбудовуватися в систему розробки Visual Studio 2013.

Visual Studio 2013 забезпечує надійні та безпечні обчислення (trustworthy computing), дозволяє проектувати, реалізовувати і тестувати реалізацію підсистеми безпеки на кожному етапі життєвого циклу програми з підтримкою принципів розробки безпечного коду, а саме мінімізації атакованої поверхні програми (minimizing the attack surface), мінімальних привілеїв (least privilege), забезпечення безпеки за дизайном, за замовчанням, при розгортанні (secure by design, by default, by deployment)[2, с. 26]. У середовищі Visual Studio 2013 є зручна розвинена підтримка trustworthy computing - корекція коду при його введенні і діагностування його недоліків, контроль компілятором багатьох проблем надійності і безпеки, аналізатор коду проекту на типові помилки дизайну.Використання аспектно-орієнтованого програмування в середовищі Visual Studio 2013 дозволяє реалізувати підсистему безпеки у вигляді окремих компонентів і повторно використовувати їх в різних додатках.

Програмну систему можна розглядати як сукупність різних компонентів. Кожен компонент відповідає за визначену функціональність. Можна виділити певні частини, або аспекти, що відповідають за функціональність, реалізація якої розосереджена в коді програми і складається із схожих фрагментів коду. Таку функціональність називають наскрізною функціональність(cross - cutting concerns)[3, с. 89]. AspectC++ дозволяє виділити і реалізувати наскрізну функціональність в окремих модулях, які називаються аспектами. Аспекти вмонтовуються в точки приєднання цільової програмної системи за допомогою компонувальника аспектів (weaver) з використанням правил впровадження. Прикладами наскрізної функціональності є протоколювання (logging), безпека виконання програми у багатопотоковому обчислювальному середовищі (MT - safety), обробка помилок, реалізація підсистеми безпеки (security).

Пакет АОП AspectC++ може використовуватися для безшовної інтеграції наскрізної функціональності в додатки і здійснює впровадження аспектів в цільову зборку на рівні бінарного коду без модифікації початкового коду цільової програмної системи, що дозволяє систематично додавати і модифікувати нову функціональність.

Aspect є основною одиницею модульності AspectC++. В аспектах задаються зрізи точок виконання (Pointcut) та інструкції, які виконуються в точках виконання (Advice). JoinPoint — строго визначена точка виконання програми, яка пов’язана з контекстом виконання, наприклад, викликом функції, конструктора, обробника виключень. Pointcut — набір (зріз) точок JoinPoint, які задовольняють заданій умові. Advice — набір інструкцій мовиC++, якій виконуються до, післяабо замістькожної із точок виконання (JoinPoint) заданого зрізу (Pointcut).Introduction — спроможність аспекту змінювати структуру або ієрархію класу. Pointcut і Advice визначають правила інтеграції. Аспект є елементом, який нагадує клас в об’єктно-орієнтованому програмуванні, він об’єднує елементи pointcut і елементи advice, і формує модуль на зрізі системи.При розробці за допомогою AspectC++виконуються три кроки:

Аспектна декомпозиція — визначення загальної і наскрізної функціональності. При цьому потрібно визначити функціональність для модульного рівня із наскрізної функціональності системного рівня.

Реалізація функціональності.

Компоновка аспектів. Аспектний інтегратор визначає правила для створення аспектів у вигляді окремих модулів. За допомогою аспектних модулів можна впливати на існуючу схему успадкування При цьому аспект є сервісом для зв’язування компонентів системи.

В роботі пропонується реалізація авторизованого доступу до серверу даних. Ідентифікація принципала є однією із головних задач засобів захисту даних. Для прийняття рішення на доступ до певних елементів система повинна обов'язково встановити особу принципала. Функціональність авторизації і аутентифікації має бути вбудована в функції, які потребують захисту, що однозначно приведе до перемішування вимог в коді і втраті модульності компонентів бізнес-логіки.

При використанні AspectC++ на етапі проектування системи подібну наскрізну функціональність потрібно винести в аспектний модуь. Наприклад, в абстрактному аспекті AbstractAuthenticAspect визначається логіка аутентифікації та авторизації. Визначається набір інструкцій мови для ідентифікації before():authOperations(), який вставляється до коду, який має бути захищеним, і виконує закриту функцію даного аспекту — authenticate(). В аспекті визначається набір інструкцій авторизації Object around(): authOperations(), який викликається замість коду, який захищається. Код який захищається виконується у випадку успішного виконання коду служби авторизації. В абстрактному аспекті AbstractAuthenticAspect також визначено принципал authenticatedSubject, для якого в конкретному аспекті визначені права за допомогою виклику заміщеної функції getPermission(). В конкретному аспекті визначається набір точок інтеграції аспектного коду authOperations. Такими точками є головні функції для виконання операцій з даними. У всі ці функції інтегрується функціональність, яка визначена в аспектному модулі. При цьому самі компоненти будуть містити тільки базовий код без наскрізної функціональності, що значно покращує модульність системи.

Аспектно-орієнтоване програмування, яке є розвитком об’єктно-орієнтованого програмування і реалізовано в пакеті AspectC++ дозволяє знизити час, вартість і складність розробки програмного продукту, підвисити його надійність та безпеку за рахунок реалізації наскрізної функціональності в окремих модулях-аспектах. Уся наскрізна функціональність реалізується в аспектному модулі і може бути використана повторно в інших програмних системахшляхом успадкування аспектів.

Література:

1.AspectC++ [Електроний ресурс] // – Режим доступу : http://www.aspectc.org(2.10.2015).

2.Сафонов В. О. Современные технологии разработки надежных и безопасных программ (Trustworthy Computing). //Компьютерные инструменты в образовании.–2010.–JN2 6.–С. 25-33.

3.Нгуен Ван Доан Средства аспектно-ориентированного программирования для разработки Web-приложений в системе Aspect.NET/ Сафонов В. О.// Вестн. С.-Петерб. ун-та. Сер. 10. –2011. –Вып. 1. –С. 85-105.

Зариленко Е.С.

Студент каф. Информационных Технологий

Государственный Университет Телекоммуникаций

г.Киев, Украина

ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ МОБИЛЬНОЙ ТЕЛЕМЕДИЦИНЫ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ LTE

Основная идея состоит в предоставлении широкополосного беспроводного доступа для обеспечения мультимедийных услуг в области мобильной телемедицины. При передаче медицинских данных по сетям мобильной связи требуется обеспечить высокую пропускную способность, надежность коммуникаций и целостность и конфиденциальность данных. Сети 3G удовлетворяют этим требованиям лишь частично. Технология LTE значительно расширяет возможности телемедицины. Например, она позволяет использовать с более высоким качеством такие приложения как видеоконференцсвязь между доктором и пациентом.

В настоящее время существует множество технологий безпроводного доступа, таких как LTE, Wi-Fi, WiMAX. Каждая технология обладает определёнными характеристиками, которые определяют её область применения. Применительно к беспроводным сетям масштаба города WMAN технология LTE имеет следующие ключевые преимущества по сравнению сдругими системами:

Производительность. Характеристики радиопокрытия, спектральной эффективности и емкости сети LTE значительно выше характеристик WiMax, HSPA+.

Масштабы рынка. Глобальность сотового рынка не может быть сравнима с нишевым характером рынка сетей ШБД, в частности WiMax.

Экосистема производителей. Однотипность технологий LTE FDD и TDD и возможность переиспользования технических решений большого сотового рынка FDD для рынка ШБД гарантируют доступность как сетевой инфраструктуры, так и терминального оборудования TD-LTE.

Значительное превосходство технологии радиодоступа стандарта LTE над технологиями 3GPP предыдущих поколений безусловно является существенным аргументом в пользу революционного сценария развития беспроводных сетей передачи данных в будущем.При таком подходе, спектр использования технологии LTE охватывает множество областей: здравоохранение, правоохранительне органы, службы санитарной авиации и т.п.

Литература:

1. Медведев О.С., Кербиков О.Б. Телемедицина: технология будущего или возможность повысить уровень медицинского обслуживания уже сегодня. 1997 г., стр. 88-89

2. Телемедицина и компания Telecom Finland. Компьютерные технологии в медицине. 1997 г., стр. 95

Свередюк К.А.
Магістр групи СЗДМ – 61
Державний університет телекомунікацій
м.Київ, Україна

ІДЕНТИФІКАЦІЯ РИЗИКІВ

Більшість організацій постійно піддаються нескінченній кількості нових або модифікованих загроз і вразливостей, які можуть вплинути на їх роботу або виконання деяких завдань. Ідентифікація, аналіз і оцінка цих загроз і вразливостей є єдиним способом зрозуміти і виміряти вплив ризику,а отже, прийняти рішення про відповідні заходи.

Ідентифікація ризиків − це фаза, де загрози, вразливості і пов'язані з ними ризики ідентифіковані. Цей процес має бути систематичним і досить повним, щоб гарантувати, що немає несвідомо виключеного ризику. Дуже важливо, що на цьому етапі всі ризики були виявлені і зафіксовані, незалежно від того, що деякі з них, можливо, вже відомі та, ймовірно, контрольовані організацією.Перший крок полягає у створенні повного список джерел загроз, ризиків і подій, які можуть вплинути на досягнення кожної з цілей. Ці події можуть запобігти, погіршити, затримати або сприяти досягненню цих цілей.

Ідентифікаціяризиків заснована на аналізі статистичнихданих про небезпечні явища та результати їх взаємодії з антропосферою (стихійні лиха, аварії, катастрофи,економічні і політичні кризи), а також на аналізі механізмівможливого впливу їх негативних факторів на різнігрупи населення і суб'єкти діяльності у разі реалізації небезпек.[1, с. 135]

Для прийняттяобгрунтованогорішенняважливовиявитивсіможливіризики. Загалом, ризик може характеризуватися:

Походженням;
Певною діяльністю, подією;
Наслідками;
Причиною виникнення;
Часом та місцем виникнення; [3]

Можна запропонувати безліч критеріїв для виділення етапів процесу ідентифікації ризиків. Найбільш поширеним є ступінь докладності дослідження ризику. Відповідно до нього можна виділити наступні етапи:

Осмислення ризику;

Аналіз конкретних причин виникнення несприятливих подій та їх негативних наслідків.

Комплексний аналіз ризиків.[2, с. 43]

Отже, завжди слід пам'ятати , що від передбачуваного ризику можна застрахуватися, а невиявлений або проігнорований ризик може призвести до краху організації.

Література:

1.Общаятеориярисков : учеб. пособие для студ. высш. учеб.заведений / Я.Д.Вишняков, Н.Н.Радаев. — 2-е изд., испр. —М. : Издательский центр «Академия», 2008. — 368 с.

2.Иванов А.А., Олейников С.Я., Бочаров С.А. РИСК-МЕНЕДЖМЕНТ. Учебнометодический комплекс. – М.: Изд. центр ЕАОИ, 2008. – 193 с.

Електроний ресурс: https://www.enisa.europa.eu/

Берназ Н.М.
Старший викладач каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна
Саланда І.П.
Аспірант
Східноєвропейський національний університет ім. Лесі Українки
м. Луцьк, Україна

МЕТОД ОЦІНЮВАННЯ ПОКАЗНИКА ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ РОЗГАЛУЖЕНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

У сучасних умовах на розгалужені інформаційні мережі (РІМ) впливають внутрішні (відмови, збої, помилки) і зовнішні (активний або пасивний вплив зовнішнього середовища) фактори. Тому, актуальною є задача побудови функціонально стійкої інформаційної мережі [1], яка використовує альтернативні маршрути для передачі інформації. Вирішенню проблеми забезпечення стійкості функціонування складних технічних систем присвячено низку наукових праць [2-3]. Однак широке їх використання в практичних задачах оцінки ФС інформаційних мереж ускладнене по багатьох причинах, однією з яких є складність і громіздкість обчислень. Тому, становить інтерес знайти найпростіший спосіб визначення ймовірності зв'язності мережі, який допоміг би оперативно і вручну проводити на стадії проектування оцінку різних варіантів побудови.

В якості математичної моделі розгалуженої інформаційної мережі візьмемо неорієнтований випадковий граф $G(V, L)$ без петель і кратних ребер, де V – множина вершин ($|V|$=n), L – множина ребер ($|L|= m$).Метод двочастинних графів ґрунтується на використані властивостей стягнутого двочастинного графа (СДГ).

Під двочастинним графом (ДГ) будемо розуміти граф $Г_i$, який складається із об'єднання двох множин вершин $V_1=\{v_i\}$ і $V_2=\{v_j\}$, що не перетинаються, і підмножини ребер $L=\{l_{ij}\}$ таких, що вершини будь-якого ребра належать різним підмножинам V_1 и V_2. Якщо вершини однієї з його частин, наприклад V_1, стягнути в одну точку, то отримаємо стягнутий двочастинний граф (СДГ) $Г'_i$.

Послідовно приєднане ребро $l_{i,j}\in L$ та інцидентна йому вершина $v_j\in V_2$виконують функцію зв'язування компонент $Д_1$ і $Д_2$, на які розіб'є вихідний граф вилучення підмножин L і V_2. Назвемо цю конструкцію зв'язуючою ланкою та позначимо її символом $\eta_\xi=\{l_{i,j}v_j\}$. В будь-якому СДГ можна виділити $m=m_2$ зв'язуючих ланок, які утворять деяку підмножину виду $H=\{\eta_\xi\}$.Позначимо символом n кількість справних зв'язуючих ланок в r-му СДГ, а символами n_1і n_2– кількість зв'язуючих ланок, що знаходяться в несправному стані через несправність або вершини $\bar{v}_j\in\bar{\eta}_\xi$, або ребра $\bar{l}_{ij}\in\bar{\eta}_\xi$.

Всього можливих справних станів r-го СДГ може бути рівно $N_1=\sum_{i=0}^{m-1}C_m^i\cdot 2^i$, тому імовірність $p(H_r)$ його справного стану обчислюється так:

$$p(\mathrm{H}_{r\in N_1})=\sum_{n_1=0}^{m-1}\sum_{z=1}^{C_m^{n_1}}\sum_{\substack{\sigma=1\\ j\in(\xi\in z)}}^{n_1}q(\mathrm{v}_{j_\sigma})\sum_{n_2=0}^{m-(1+\mathrm{n}_1)}\times \tag{1}$$

$$\times\sum_{\gamma=1}^{C_{m-n_1}^{n_2}}\sum_{\substack{\xi=1\\ (\mathrm{i,j})\in(\xi\in\gamma)}}^{n_2}[\mathrm{q}(\mathrm{l,j}_\xi)\mathrm{p}(\mathrm{v}_{j_\xi})]\prod_{\substack{\varphi=1\\ (\mathrm{i,j})\notin(\mathrm{z},\gamma)}}^{n=m-(\mathrm{n}_1+\mathrm{n}_2)}[\mathrm{p}(\mathrm{l}_{i,j_\varphi})\mathrm{p}(\mathrm{v}_{j_\varphi})]$$

Тут символом $r\in N_1$ при H умовно показано, що імовірність справного стану зв'язуючих ланок однієї з гіпотез, при якій можливе формуванняk-го СДГ, якщо виконати $V'_{1_{k=r+1}}=(V'_{2_r}=\{v_j\in\bar{\bar{\eta}}_\xi\})$. Якшо врахувати ненадійність лише ребер або лише вершин, то n_1=0 або n_2=0. Тоді співвідношення (1) набере вигляду:

$$p(\mathrm{H}_{r\in N_1}) = \sum_{n_2=0}^{m-1} \sum_{\gamma=1}^{C_m^{n_2}} \sum_{\substack{\xi=1 \\ (\mathrm{i,j})\in(\xi\in\gamma)}}^{n_2} q(\mathrm{l}_{i,j_\xi}) \prod_{\substack{\varphi=1 \\ (\mathrm{i,j})\in(\xi\notin\gamma)}}^{n=m-n_2} (\varphi=1)\mathrm{p}(\mathrm{l}_{i,j_\xi}) \qquad (2)$$

$$p(\mathrm{H}_{r\in N_1}) = \sum_{n_1=0}^{m-1} \sum_{z=0}^{C_m^{n_1}} \sum_{\substack{\sigma=1 \\ j\in(\xi\in \mathrm{z})}}^{n_1} q(\mathrm{v}_{j_\sigma}) \prod_{\substack{\varphi=1 \\ j\in(\xi\notin \mathrm{z})}}^{n=m-n_1} (\varphi=1)\mathrm{p}(\mathrm{v}_{j_\xi}) \qquad (3)$$

Після побудови повної підмножини СДГ за формулами (2) і (3) визначаються імовірності зв’язності P_{xy} и $\overline{P}_{xy}$.

Висновок. Даний метод відрізняється від існуючих методів достатньо високою «швидкодією» та дозволяє обчислити імовірність незв’язності вершин за прийнятний час.

Література:

1. Кравченко Ю.В., Барабаш О.В. Функціональна стійкість – властивість складних технічних систем / Збірник наукових праць. – К.: НАОУ, 2002. – Бюл. №40. – С. 225-229.
2. Попков В.К. Математические модели связности. Ч.1. Графы и сети. – Новосибирск: РАН. Сибир. отд-ние, 2000. – 174 с.
3. Тоценко В.Г. Проблемы надежности сетей. / "Компьютэрра", 1998. №4. – С.23-29.

Абакумова А.О.

Студентка

Національний авіаційний університет

м. Київ, Україна

ПЕРСПЕКТИВА РОЗВИТКУ СУЧАСНОЇ ТРАНСПОРТНОЇ МЕРЕЖІ СТІЛЬНИКОВОГО ОПЕРАТОРА

З моменту появи і до сьогоднішнього дня мережі стільникового зв'язку пройшли великий шлях розвитку. Можливості, які відкривають стільникові технології сьогодні, вже давно вийшли за рамки голосових послуг, створюючи нові способи спілкування, обміну даними та бізнес моделі. Поширення пристроїв призвело до експоненціального зростання трафіку в мережах по всьому світу. Однак це тільки початок тієї революції, якій сприяє активний розвиток технологій, що з'єднують суспільство.

У довгостроковій перспективі такого розвитку з'явиться те, що ми називаємо 5G, тобто набір органічно інтегрованих технологій радіодоступу [1]. LTE (4G) – це еволюційний крок у розвитку технологій стільникового зв'язку, ця технологія буде домінуючою в багатьох куточках земної кулі і після 2020 року. Тому мова йде не про заміну існуючих технологій на 5G, а, скоріше, про їх розвиток та доповненні новими технологіями радіодоступу, призначеними для конкретних сценаріїв і певних цілей.

Однак на шляху втілення цієї ідеї виникає ряд складнощів, які необхідно передбачити:

1. Значне зростання обсягу трафіку (більш ніж у 1000 разів).
2. Значне зростання кількості підключених пристроїв.
3. Велике число вимог і характеристик:

- швидкість передачі даних;
- час очікування;
- енергоспоживання пристрою;
- вартість пристрою.

4. Доступність і надійність.

Останні кілька років стільниковий трафік демонструє стійке зростання, і ця тенденція продовжиться і в майбутньому. На підставі різних прогнозів [2] можна зробити висновок, що після 2020 року ємність систем повинна буде забезпечувати обробку трафіку, що перевищує нинішній в обсязі більш ніж в 1000 разів.

У мережах по всьому світу працюють більше 5 млрд стільникових пристроїв [3], більшість з яких представляють собою стільникові термінали або пристрої, що забезпечують стільниковий широкосмуговий доступ та інтегровані в переносні комп'ютери і планшети. У майбутньому очікується, що число підключених пристроїв, задіяних у розумних містах, розумних будинках та інтелектуальних енергомережах перевищить кількість пристроїв користувачів в 10-100 разів. Забезпечити безперебійну роботу 50 млрд (а можливо і 500 млрд) пристроїв – завдання непросте. Разом із зростанням кількості підключених пристроїв будуть значно зростати і вимоги до мережі.

Потокове відео, файлообмінні мережі і хмарні сервіси як і раніше будуть залишатися найбільш популярними додатками, вимагаючи все більш високих швидкостей. В офісних приміщеннях і міському середовищі, де щільність звернень до мережі найбільш висока, необхідно забезпечити швидкість передачі даних в кілька Гбіт/с. Така швидкість дозволить синхронізувати локальні сховища з хмарними і мережевими дисками, передавати відео надвисокої чіткості і підтримувати роботу додатків віртуальної і доповненої реальності.

Для втілення ідеї про необмежений доступ до інформації повинні бути доступні швидкості передачі даних, вимірювані в сотнях Мбіт/с. Крім того, з метою забезпечення «гігабітних» швидкостей, необхідних для роботи додатків віртуальної або доповненої реальності, потрібно буде і далі скорочувати час відгуку до декількох мілісекунд.

Зростання числа підключених пристроїв буде супроводжуватися появою нових способів їх застосування, що призведе до виникнення нових вимог до мереж, що варіюються залежно від пристрою і від конкретної мети використання.

Технології продовжують свій розвиток в напрямку до більш високої продуктивності і все більшому числу можливостей. На додаток до існуючих технологій радіо-доступу, з'являться також нові технології (досі невідомі), які дозволять вирішувати ті завдання, які вирішити за допомогою 3G/4G неможливо. Прозора інтеграція існуючих і нових технологій сприятиме підвищенню якості користувацького досвіду і появи цілого ряду нових послуг.

Література:

1.Ericsson, Networked Society Essentials. [pdf] Стокгольм: Ericsson. http://www.ericsson.com/res/docs/2013/networked-society-essentials-booklet.pdf

2.Ericsson, Ericsson Mobility Report – on the Pulse of the Networked Society. [pdf] Стокгольм: Ericsson.
http://www.ericsson.com/res/docs/2013/ericsson-mobilityreport-june-2013.pdf

3.Cisco, Cisco Virtual Networking Index: Global Mobile Data Traffic Forecast Update, 2014-2019. [pdf] США: Cisco.
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Ткалич О.П.
К.т.н.,доцент каф. Телекоммуникационных систем
Колодинский Д.О.
Студент каф. Телекоммуникационных систем
Национальный авиационный университет
г. Киев, Украина

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ УВЕДОМЛЕНИЙ В АЭРОПОРТАХ

В современном мире, мы уже не можем представить себе жизнь без постоянного движения, новых впечатлений и смены окружения. На сегодняшний день путешествия самолетом доступны практически всем. Мы привыкли к тому, что в кратчайшие сроки можем оказаться в любой точке планеты. Тем более, что требования современной деловой жизни предполагают высокую мобильность. Точно так же, нам необходим быстрый и легкий доступ к необходимой нам информации. Гражданская авиация и сфера IT достигли в своем развитии за последние годы невероятных успехов. Они плотно связаны друг с другом так, что одно уже не представляется возможным без другого. Мы уже не сможем отказаться от быстрого вида транспорта и от возможности быстро передавать и получать информацию.

Концепция системы уведомлений поможет персоналу, клиентам и посетителям,потому что это в первую очередь электронное меню, консультант, информер.У большинства из нас современные мобильные телефоны, способные выходить в Интернет и подключаться к беспроводным сетям. И мы постоянно пользуемся этими возможностями. В аэропорту, как вероятно больше нигде, нам необходим быстрый и простой доступ в Интернет. В крупных транспортных объектах возможна организация сервиса для отправки Push-уведомлений. Push-уведомления –сообщения, отображаемые на экране мобильного телефона. Они позволяют уведомлять клиентов аэропорта о таблоидной информацией,прибытии рейса, доставки багажа, возможности прохождения регистрации и таможни, приглашения для посещения мест отдыха,а так же,следить за интересующей информацией.Одним из аспектов выгоды использования электронных систем взаимодействия с клиентами заключаетсяне только в увеличении продуктивности труда обслуживающего персонала, и меньшей их загруженности, но и за счет рекламы, которая позволяет извлекать из этого огромную прибыль.

В построении инфраструктуры Push-уведомлений могут возникать следующиесложности:

Зависимость от платформы.

Масштабирование.

Маршрутизация.

Мониторинг и телеметрия.

Трудности возникают в основном потому, что push-уведомления доставляются устройствам посредством специфичных для каждой платформы служб. Push-уведомления доставляются с помощью инфраструктур, специфичных для платформы, называемых системы уведомления платформы (PNS). Например, для отправки push-уведомлений приложениям Windows Store нужно использовать Службу уведомлений Windows (Windows Notification Service, WNS), на Windows Phone — Службу push-уведомлений Майкрософт (Microsoft Push Notification Service, MPNS), на iOS — Службу push-уведомлений Apple (Apple Push Notification service, APNs), а на Android — Google Cloud Messaging (GCM).

Трудность масштабирования связана с нормами службы PNS, при каждом запуске приложения должны быть обновлены токены устройства. Эти приводит к потреблению большого количества трафика (и следовательно доступа к базе данных) только для поддержания обновления токенов устройства.

Службы PNS обеспечивают способ отправки сообщения в адрес устройства. Однако, для большинства приложений уведомления нацелены на пользователей и/или группы интересов (например, все работники, назначенные определенной учетной записи клиента). Как таковой, сервер приложения поддерживает реестр, который связывает группы интересов с токенами устройств с целью маршрутизации уведомлений в адрес правильных устройств. Так же возможно отправка уведомлений исходя из местоположения клиента, что позволит отображать информацию о полезных объектах находящихся поблизости. Эти затраты добавляются к общему времени расходов на маркетинг и техобслуживание приложения.

Отслеживание и статистическая обработка результатов миллионов уведомлений не является тривиальными, и обычно это становится важным компонентом любого решения, которое использует push-уведомления. Так же ограничена длина Push(для iOS устройств составляет 256 байт).

Для разработки сервиса по отправки Push -уведомлений возможно использовать решения Microsoft– WindowsAzure [1], структура которого показана на Рис.1. Основные преимущества:Простота использования (уже готовы библиотеки для платформ iOS, Android, WinPhone, Windows8); Кроссплатформенность (Разработаны мобильные приложения на iOS, Android, WinPhone, Windows8 и, соответственно, Push -уведомления запускаютсяна все платформы одновременно); Цена (~ 10 USD. берет Microsoftза 1000000 Push-ей в месяц) ;Масштабирование (Если наблюдается, что сервис не справляется с нагрузкой, то не составляет труда увеличить ресурс для отправки Push).

Сервис должен объединять следующие функциональные узлы:

Мобильный устройства пользователей; AzureNotificationHub; PlatformNotificationService; Backend; Web-Интерфейс, где администратор будет добавлять сообщения и смотреть статистику, отправленных Push;База данных MS SQL, где хранятся записи с Push-уведомлениями и датами их отправления;Служба, которая с заданной периодичностью(раз в минуту или если требуется чаще) ищет в базе запись с датой отправления равной текущей и отправляет команду в Azure

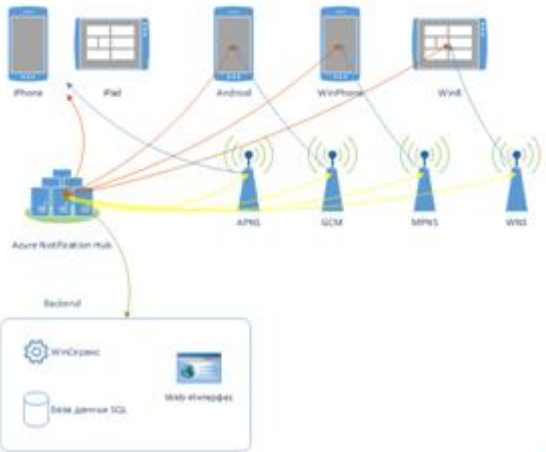


Рисунок 1 Структура сети уведомлений. Notification Hub для отправки Push.

Упрощено рассмотрим логику работы Push-уведомлений (Рис.2):После подключения к сети доступа, пользователь регистрируется в сети и автоматически получает уведомления о возможности загрузки и использования программного обеспечения содержащего перечень услуг которые доступны для данного аэропорта. Отвергая или принимая уведомления пользователь может настраивать список услуг необходимых для личного пользования. Пользователь мобильного приложения соглашается принимать Push-уведомления, происходит регистрация пользовательского устройства в службе уведомлений (Notification Service)(служба уведомлений зависит от версии операционной системы). Если регистрация прошла успешно, то ID устройства также регистрируется в Azure Notification Hub.

Рисунок 2. Процесс отправки уведомлений после подключения.

Литература:

1) https://msdn.microsoft.com/ru-ru/dn499803.aspx
2) http://www.oszone.net/24620

Ткалич О.П.
К.т.н., доцент каф. Телекоммуникационных систем
Устинов А.Ю.
Студент каф. Телекоммуникационных систем
Национальный авиационный университет
г. Киев, Украина

РАЗРАБОТКА БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ СТАНДАРТА ZIGBEE С ИСПОЛЬЗОВАНИЕМ МИКРОКОНТРОЛЛЕРА ARDUINO

Сенсорные сети представляют собой распределенное в пространстве множество датчиков и исполнительных устройств, объединенных между собой посредством радиоканала. Применяться подобные сети могут в огромном спектре приложений: домашняя и промышленная автоматизация, контроль микроклимата, охранно-пожарные системы, учет и оптимизация потребления водоэнергоресурсов и т.д. Причем область покрытия подобной сети может составлять от единиц метров до нескольких километров.

Одним из главных стандартов реализации этих сетей является стандарт IEEE 802.15.4 ZigBee, обладающий значительно большей гибкостью по сравнению со своими аналогами. Реализация стандарта ZigBee основана на трех типах устройств: координатор, маршрутизатор и оконечное устройство (сенсор или датчик)[1].

Существует несколько способов для организации беспроводной сенсорной сети, один из которых – на базе микроконтроллера Arduino [2]. Arduino – это простая в использовании открытая электронная платформа, предназначенная для быстрого создания интерактивных электронных устройств. Arduino строится на базе микроконтроллеров Atmel и используется для получения сигналов от аналоговых и цифровых датчиков, управления различными исполнительными устройствами и обмена информацией с компьютером припомощи различных интерфейсов.

Для реализации беспроводной сенсорной сети стандарта ZigBee с помощью плат Arduino, необходимо применить радиомодулиXBee.Модули XBeeработают как беспроводной последовательный порт, что позволяет для связи с ними использовать чтение и отправку последовательных данных.Модуль XBeeпередает данные на частоте 2,4 ГГц, на которой работают и многие другие устройства, например Wi-Fi-маршрутизаторы. Модули XBee соответствуют стандарту IEEE 802.15.4, который содержит перечень правил эксплуатации беспроводных персональных сетей (PAN).

Модули XBee, как правило, соединяют согласно конфигурации PAN «точка-точка» или «точка-многоточка». Схема «точка-точка» удобна, когда необходимо заменить проводную последовательную связь между двумя удаленными устройствами беспроводной. Конфигурация «точка-многоточка» часто используется для создания распределенных сетей датчиков.

Также, существуют специальные переходники – платы расширения, с помощью которых можно легко подключить модуль XBeeк плате Arduino. Большинство плат Arduino работает от источника 5 В, логические уровни также находятся в диапазоне от 0 (низкий уровень) до 5 В (высокий уровень). Напряжение питания модулей XBeeравно 3,3 В, логические уровни тоже другие. Хотя у Arduinoесть встроенный стабилизатор на 3,3 В, его ток недостаточен для питания XBee-модуля. Поэтому на большинстве XBee-переходниках установлен линейный стабилизатор для питания модуля XBee. Схема подключения и согласования между Arduinoи XBeeс помощью платы расширения Arduino-XBee изображена на Рис. 1.

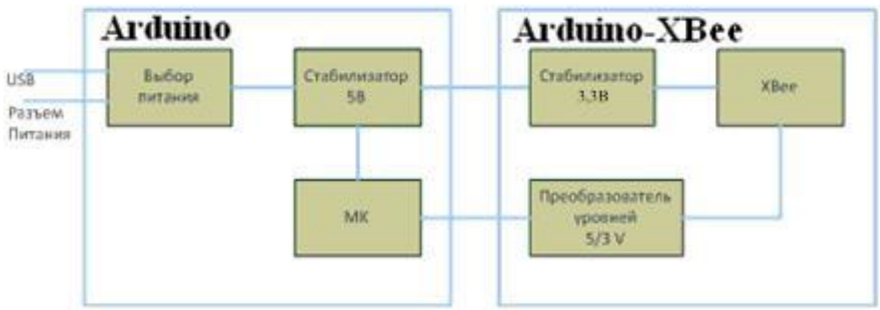


Рисунок 1. Блок-схема аппаратной платформы Arduino-XBee

Схема беспроводной сенсорной сети стандарта IEEE 802.15.4 ZigBee с помощью микроконтроллеров Arduinoизображена на Рис. 2.

В состав сети входят: координатор, который управляет беспроводной сетью стандарта IEEE 802.15.4 ZigBee; маршрутизаторы, управляющие потоками информации между разного рода устройствами; сенсоры, собирающие информацию с окружающей среды и передающие ее в сеть; платы Arduino-XBee, состоящие из платы Arduino, платы расширения Arduino-XBee и радиомодуляXBee. МикроконтроллерыArduino выполняют обработку информации, агрегацию данных от оконечных узлов сети и управление другими узлами беспроводной сенсорной сети с помощью APIинтерфейса, чем значительно снижают нагрузку с координатора, который в этом случае выполняет только поддерживающие, сервисные функции: мониторинг, конфигурирование, настройку и т.д.

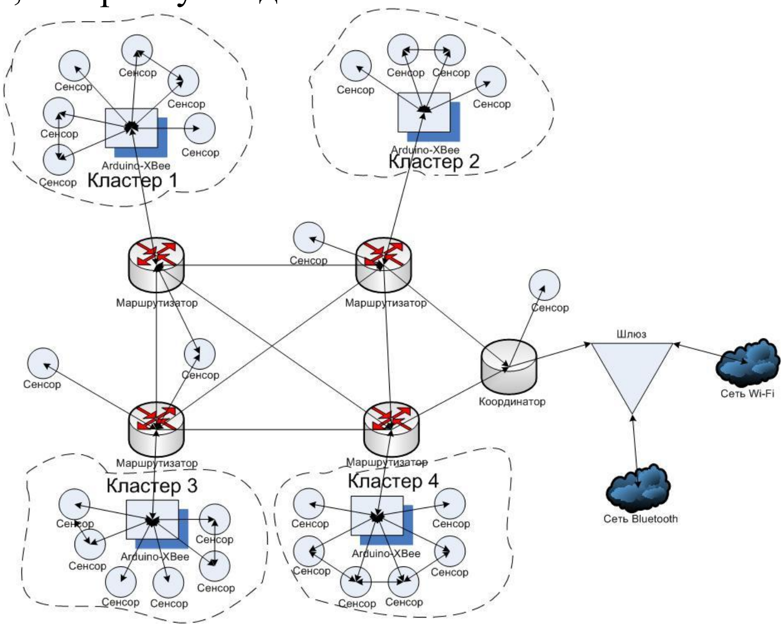


Рисунок 2. Беспроводная сенсорная сеть, реализованная с помощью микроконтроллеров Arduino

Кластеры сенсорной сети могут формироваться исходя из типов назначения датчиков. Например, в кластере 1 могут быть объединены датчики температуры и датчики влажности, в кластере 2 – датчики видеонаблюдения, в кластере 3 – датчики открытия дверей, а в кластере 4 – датчики освещения. Топология сети является ячеистой, то есть при передаче данных будут существовать альтернативные маршруты. Беспроводная сенсорная сеть является сегментом корпоративной сети, которая также включает в себя беспроводную сеть стандарта Wi-Fiи беспроводную сеть стандарта Bluetooth. Взаимодействие между тремя разнородными беспроводными сетями осуществляется через шлюз.

Литература:

1.Побудова сенсорної мережі аеропорту та її інтеграція з бездротовою мережею аеропорту стандарту 802.11/ О.П. Ткаліч, Р.С. Одарченко, О.Ю. Устинов, Д.О. Колодинський // Materiály XI mezinárodnívědecko - praktickákonference«Aktuálnívymoženostivědy – 2015»,Praha, PublishingHouse «EducationandScience» s.r.o - 96 stran

2.Изучаем Arduino: инструменты и методы технического волшебства/ Д. Блум// БХВ-Петербург, 2015 – 336 с.

Долінський Р.О.
Аспірант каф. Телекомунікаційних систем
Державний університет телекомунікацій
м. Київ, Україна

РОЗРОБКА АЛГОРИТМІВ ОПТИМАЛЬНОГО ПРИЙОМУ ДЛЯ МЕРЕЖ РАДІОДОСТУПУ LTE

У сучасних багатоканальних модемах за деякими винятками використовується когерентний прийом. Існують дві причини для такого рішення.

Першою з них є та, що обробка сигналу при когерентному прийомі використовувала фазоманіпульований сигнал. В той самий час у багатоканальних модемах з ортогональними піднесучими використовувалися проекціі початкових сигналів на ортогональні відносно одна одної опорні коливання, що мають довільну початкову фазу [5, с. 32,321].

Іншою є та, що реалізація когерентного прийому в багатоканальному модемі на базі середньої інтеграції була складною і, як наслідок, не мала популярності серед вендорів-виробників устаткування. З появою сучасних систем, що використовують SoftwareDefinedRadio (SDR) та мікропроцесори сімейства x86, які мають широкі можливості для вільного програмування алгоритмів обробки сигналу[4, с. 383], на відміну від апаратно реалізованих, жорстко спеціалізованих цифрових процесорів сигналу DSP (Digital Signal Processors), з’явилася можливість реалізувати будь-які алгоритми обробки і модуляції сигналу [6, с. 4].

Існують алгоритми когерентної обробки сигналу, що призначені виключно для обробки 16-ти позиціних сигналів з використанням квадратурної амплітудної модуляції QAM-16.

Розглянувши ці алгоритми, можна виділити наступні їх особливості.

По-перше, отримана на прийомі величина не захищена від нелінійних перетворень, тому вона має більш низькі характеристики оцінок відносно максимально правдоподібного оцінювання. Тому цей алгоритм не є максимально ефективним.

Другою особливістю є те, що використовувані алгоритми розраховані для обробки лише однієї жорстко закріпленої конструкції сигналу.

В умовах, коли в мережах операторів зв’язку існує жорстке обмеження за частотою, і потрібно отримати достатні енергетичні характеристики сигналу, використовують як амплітудно-фазову (АФМ), так і амплітудно-фазорізницеву модуляцію (АФРМ).

В сучасних системах пакетних мереж мобільного зв’язку найбільш широкого використання набули 16-ти позиційні система АФМ та 64-х позиційна система АФМ, що відповідає чотирикратній і шестикратній маніпуляції з сигналом відповідно, а також 4-х і 8-ми позиційна система ФРМ. Для цих систем передається 4 або 6 біт за символ для кожного маніпульованого сигналу для АФМ і 2 та 3 для ФРМ. Але чим більша кратність маніпуляції сигналу, тим більші вимоги висуваються до якості середи, в якій передається сигнал. АФРМ у порівнянні з ФРМ має більш завадостійкіст при збільшенні кількості позицій сигналу більше 8-ми, у разі використання більш ніж одного когла на схемі сигнальних станів, або квадратів на схемі сигнальної решітки.

Багатопозиційну амплітудно-фазову модуляцію називають ще квадратурно-амплітудної модуляцією (QAM, Quadrature Amplitude Modulation), для якої змінним і інфомаційним параметром є фаза, незміна частота і змінна амплітуда сигналу, що використовується для збільшення завадостійкості сигналу через збільшення скалярної відстані між варіантами посилок сигналу. Однак застосування багатотопозиційної QAM в чистому вигляді стикається з серйозними проблемами, пов'язаними з недостатньою завадостійкістю кодування[3, с. 35].

При фазорізницевій модуляції (DPSK, Differential Phase Shift Keying) параметром елемента, що змінюеться в залежності від номера посилки, є фаза сигналу при незмінних амплітуді і частоті. При цьому згадана фаза сигналу має не абсолютне значення фази, а різницю фаз у порівнянні з попередньою посилкою. Використання фазорізницевої модуляції є виправданим, оскільки, як ми знаємо з теорії інформації, фазова модуляція є найбільш інформативною.

Під різницею фаз, що є інформаційним параметром, мається на увазі, що рішення про прийнятий варіант сигналу приймається відповідно до різниці фази n і n-1 посилки, що була передана в лінії зв’язку:

$\Delta^1\varphi_n = \varphi_n - \varphi_{n-1}$,

а при різниці фаз другого порядку рішення приймається на протязі трьох посилок:

$\Delta^2\varphi_n = \Delta^1\varphi_n - \Delta^1\varphi_{n-1} = \varphi_n - 2\varphi_{n-1} + \varphi_{n-2}$

Перевагою застосування АФРМ першого порядку є те, що при використані данного типу модуляції досягається інваріантність сигналу, що передається в лінії зв’язку до початкової фази сигналу. Тобто її застосування дозволяє уникнути помилок на вході демодулятора, що виникають як наслідок того, що початкова фаза посилки сигналу є невідомою [1, с. 39].

При умові когерентного прийому сигналу може використовуватись як АФМ, так і АФРМ.

Треба зазначити, що алгоритми когерентного прийому, що використовуються на данний момент, змушені проводити синхронізацію фази шляхом використання синхросигналу[1, с. 92]. Через це використання фазорізницевої модуляції, що усуває вплив початкової фази сигналу на процес розрахунків, є доречним. В результаті розробка алгоритму, що не потребуватиме синхросигналу і матиме інваріантність до початкової фази сигналу, є актуальною.

При використанні алгоритмів некогерентного прийому для виконання безпомилкового прийому сигналу обов’язковим є те, що частота та інтервал обробки сигналу є відомими. Для цього алгоритму прийому початкова фаза сигналу може бути невідомою, що не дозволяє використовувати алгоритм прийому для сигналів, що мають за інформаційній параметр абсолютну фазу [2, с. 38]. Для фазорізницевої модуляції, котра використовує в якості інформаційного параметру різницю фаз сигналів, використання некогерентного прийому є доцільним. Особливістю алгоритму некогерентного прийому сигналу також є те, що при умові використання варіантів сигналу з рівною енергією, що означає використання схеми вузлів станів посилки з розподілом станів за одним параметром, а саме різницею фаз, його завадозахищеність наближується до завадозахищеності алгоритму когерентного прийому. Треба відмітити, що завадозахищеність систем, що використовують алгоритм некогерентного прийому, зменшується тим значніше, чим більше зсув сигналу по частоті [1, с. 162].

Обидва алгоритми прийому в класичному вигляді залежать від початкової фази сигналу. Через це використання фазорізницевої модуляції, що усуває вплив початкової фази сигналу на процесс розрахунків, є доречним. Також особливості фазорізницевої модуляції високих порядків дозволять підвищити завадозахищеність систем. Тому задача розробки алгоритмів оптимального прийому, що не потребуватиме синхросигналу для когерентного прийому, матиме інваріантність до початкової фази сигналу та інваріантність до зсувів частоти при некогерентному прийомі, є актуальною темою наукових досліджень.

Література:

1.Окунев Ю.Б. Теория фазоразностной модуляции [Текст] / Ю.Б. Окунев. – М.: Связь, 1979. – 215 с.

2.Окунев Ю.Б. Цифровая передача информации фазоманипулированными сигналами [Текст] / Ю.Б. Окунев. – М.: Радио н связь, 1991. – 296 с. – ISBN 5-256-00730-0.

3.Садомовский А.С. Радиотехнические системы передачи информации. Учебное пособие [Текст] / А.С. Садомовский, С.В. Воронов. –Ульяновск: УлГТУ, 2014. – 120 с.

4.Сорохтин Е.М. Распределенные программно-определяемые радиосистемы [Текст] / Е.М Сорохтин, С.А. Минеев // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2010. – № 5 (2). – С. 383-388.

5.Першин В.Т. Основы современной радиоєлектроники. Учебное пособие [Текст] / В.Т. Першин. – Ростовн/Д : Феникс, 2009. – 541 с. – ISBN 978-5-222-14681-1.

6.Dillinger M. Software Defined Radio: Architectures, Systems and Functions [Text] / M. Dillinger, K. Madani, N. Alonistioti. - NJ:John Wiley & Sons Ltd, 2003. – 456 p.

Артюгін О. В.
Студент ФІТ
Державнийуніверситеттелекомунікацій
м. Київ, Україна

ДОСЛІДЖЕННЯ МЕРЕЖ ДОСТУПУ ЗА ТЕХНОЛОГІЄЮ СТАНДАРТУ 802.22 ДЛЯ ЗАБЕЗПЕЧЕННЯ МУЛЬТИМЕДІЙНИХ ПОСЛУГ

В даній статті коротко розглянуті принципи функціонування стандарту IEEE 802.22 WRAN (Wi-Fi), який орієнтований на діапазон частот, що не використовується в телебаченні. Стандарт призначений для бездротових регіональних мереж WRAN.

Робоча група IEEE 802.22 WorkingGroup, заявляє, що специфікація IEEE 802.22 представляє собою проект безпровідних регіональних мереж, що складається з двох рівнів PHYi MAC з з'єднанням point-to-multipoint (багатоточковим). Власне ця група і займається розробкою і проектуванням даного стандарту.

Мережа призначена як для роботи з професійнимифіксованими базовими станціями, так і з портативними (абофіксованими) терміналами (модемами). Обмінданими по стандарту проводиться на «вільних» частотах ДВЧ/УВЧ(VHF/UHF) телевізійного мовлення, що становить смугу від 54МГц до 862МГц. За твердженням розробників, мережа в основному призначена длявикористання в малонаселених пунктах, а також сільській місцевості, денайімовірніше буде достатня кількість вільних каналів в робочійсмузі частот стандарту, які наведено в таблиці 1.

Частотний діапазон	**Границі діапазону**	**Діапазон хвилі**	**Границі діапазону**
Середні, СЧ	0,3-3 МГц	Гектометрові	1-0,1 км
Високі, ВЧ	3-30 МГц	Декаметрові	100-10 м
Дуже високі частоти, ДВЧ	30-300МГц	Метрові	10-1 м
Ультрависокі, УВЧ	0,3-3ГГц	Дециметрові	1-0,1 м
Понадвисокі, ПВЧ	3-30 ГГц	Сантиметрові	10-1 см
Вкрайвисокі, ВВЧ	30-300 ГГц	Міліметрові	10-1 мм
Гіпервисокі, ГВЧ	0,3-3 ТГц	Дециміліметрові	1-0,1 мм

В таблиці 1 наглядно представлені існуючі діапазони частот, що вказує на відмінність даного стандарту від вже існуючих таких як Wi-Fi, WiMax або LTE.Продемонстровано можливість роботи в дуже високому і ультрависокому діапазоні частот, що й дозволяє досягнути збільшеного радіусу дії.

Особливості стандарту:

Ядро:-технологія когнітивної радіопередачі, призначена для безліцензійованого використання частот телевізійного діапазону.

Призначення: – широкосмуговий бездротовий доступ до мережі Інтернет для сільської місцевості.

Топологія мережі: – багато точкова (Point-to-Multipoint).

Радіус зонипокриття: – 10-100 км (для фіксованої базової станції).

Портативність: – можна використовувати в русі до 114 км/ч.

Антени: – на базовій станції використовуються направлені (секторні) прийомо-передаючі антени, а з сторони абонента направлена антена 14 дБ. Також є ненаправлена антена для сканування частотного діапазону(когнітивний радіозв’язок).

Потужність випромінювання: – 4Вт (ефективна ізотропно випромінювана потужність, ERIP).

Гео-позиціонування: – GPS(необхідно для функціонування системи).

Специфікація стандарту IEEE 802.22 проста і легка для розуміння. Розробники винайшли найбільш оптимальну технологію обміну даними для відносно великих відстаней і прийнятних швидкостей передачі

Унікальний підхід з використанням когнітивних методів радіопередачі дозволяє ще на етапі проектування стандарту позбутися ряду проблем, в тому числі і на законодавчому рівні.

Можливо, стандарт буде скоро введений і отримає широке застосування оскільки територія України досить велика і в кожне село провести широкосмуговий доступ до Інтернет не є раціонально і дорого. Дана технологія допоможе вирішити поставлене питання швидко і за розумні кошти.

Література:

1.http://habrahabr.ru/post/125289/

2.http://gagadget.com/cellphones/5348-ieee-80222--novyij-pochti-vseobemlyuschij-standart-wi-fi-/

3.http://www.3dnews.ru/news/614830

4.https://xakep.ru/2011/11/17/57821/

Ярош В.О.
Аспірант каф.Телекомунікаційних систем
Ільницька М.А.
Студентка групи ТСДМ-61 факультету Телекомунікацій
Державнийуніверситет телекомунікацій
м. Київ, Україна

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ НАДАННЯ ПОСЛУГ ЗА ДОПОМОГОЮ МОДЕЛІ DIFF-SERV

Перехід від традиційних мереж загального користування, які використовують комутацію каналів, до мультисервісних мереж, базовою технологією для яких є комутація пакетів призвів до появи мереж зв'язку наступного покоління NGN (NextGenerationNetwork) – концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями по їх управлінню, персоналізації і створенню нових послуг за рахунок уніфікації мережевих рішень, що передбачає реалізацію універсальної транспортної мережі з розподіленою комутацією, винесення функцій надання послуг в крайові мережеві вузли і інтеграцію з традиційними мережами зв'язку.

Однією з основних цілей побудови NGN є розширення спектру послуг, що надаються:

- послуги служби телефонного зв'язку (надання місцевого телефонного з'єднання, міжміського телефонного з'єднання, міжнародного телефонного з'єднання);
- послуги служб передачі даних (надання виділеного каналу передачі даних, постійного і комутованого доступу в мережу Інтернет, віртуальних приватних мережпередачі даних);
- послуги телематичних служб ("електронна пошта ", "голосова пошта ", "доступ до інформаційних ресурсів ", телефонія по IP-протоколу, "аудіоконференція " і "відеоконференція ");
- послуги служб рухомого електрозв'язку та інші.

Отже, провівши аналіз побудови мультисервісних мереж можна висунути вимоги до якості надання послуг, а саме до к**онцепції якості послуг (QualityofService, QoS), якав**ідповідно до положень рекомендації ITU-T I.112 розділена на два типи:

-доставки (переносу) інформації (BearerService, BS);

-надання зв'язку (Teleservice, TS).

Поняття Service охоплює:

-різні види зв'язку (телефонний, передачі даних, факсимільний, пошуку документів та ін.);

-основні й додаткові послуги;

-передачу інформації з використанням різних методів комутації (КК, КП, гібридної);

-надання різних середовищ передачі (провідних, оптоволоконних, радіо й ін.);

-надання різних каналів і трактів, що відрізняються стандартизованою швидкістю (менше або рівною 64 кбіт/с, 384 кбіт/с, 2.048 Мбіт/с і вище);

-надання ресурсів на час сеансу, протягом спеціально обумовленого часу, в оренду.

Під QoS (QualityofService) слід розуміти здатність мережі (мережевої інфраструктури) забезпечити необхідний рівень сервісу мережевоготрафіка при використанні різних технологій.

Розглянемо наступні сервісні моделі QoS, які розділяються на три типи:

-BestEffortService – негарантована доставка.

В цій моделі відсутні будь-які механізми QoS. Використовуються всі доступні ресурси мережі. Відсутні механізми управління трафіком. Для поліпшення QoS використовується розширення смуги пропускання у вузьких місцях, проте це не завжди дає потрібний ефект так як існують типи трафіку, чутливі до затримок і джиттеру (наприклад VoIP).

-IntegratedService (IntServ) – інтегроване обслуговування.

Забезпечує наскрізну (End-to-End) якість обслуговування, тобто відбувається резервування ресурсів на всьому шляху проходження трафііка. Для резервування ресурсів (Resourcereservation) використовується протокол RSVP, гарантуючи необхідну пропускну спроможність. Істотним недоліком є постійне резервування ресурсу, навіть у тому випадку, якщо він не використовується або використовується не повністю.

-DifferentiatedService (DiffServ) – диференційоване обслуговування для різнотипного трафіка.

В загальному випадку DifferentiatedService є щось середнє між сервісними моделями best-effort таIntServ.DiffServоброблює тільки групи декількох інформаційних потоків та описує архітектуру мережі як сукупність прикордонних ділянок і ядра [1].

Для вирішення проблеми з масштабованістю виконання «важких» функцій покладено на периферію мережі в пограничні вузли.Розглянемо роботу пограничного маршрутизатора, структурна схема якого зображена на Рис.1.

Відповідно до цієї моделі байт ToS (TypeofService) в заголовку IP-пакета отримав іншу назву DS (DifferentiatedServices), а шість його бітів відведені під код Diff-Serv. Кожному значенню цього коду відповідає свій клас PHB (Per-Hop BehaviorForwardingClass), що визначає рівень обслуговування в кожному з мережевих вузлів. Пакети кожного класу повинні оброблятися у відповідності з певними для цього класу вимогами до якості обслуговування.

Трафік, який надходить до мережі класифікується і нормалізується прикордонними маршрутизаторами. Нормалізація трафіку передбачає вимірювання його параметрів, перевірку відповідності до заданих правил надання послуг, профілювання (при цьому пакети, які не вкладаються в рамки встановлених правил, можуть бути відсіяні) та інші операції. У ядрі магістральні маршрутизатори обробляють трафік відповідно до класу PHB, код якого зазначений у поле DS.

Переваги моделі Diff-Serv полягають у тому, що вона, по-перше, забезпечує єдине розуміння того, як повинен оброблятися трафік певного класу, а по-друге, дозволяє розділити весь трафік на відносно невелике число класів і не аналізувати кожен інформаційний потік окремо[2].

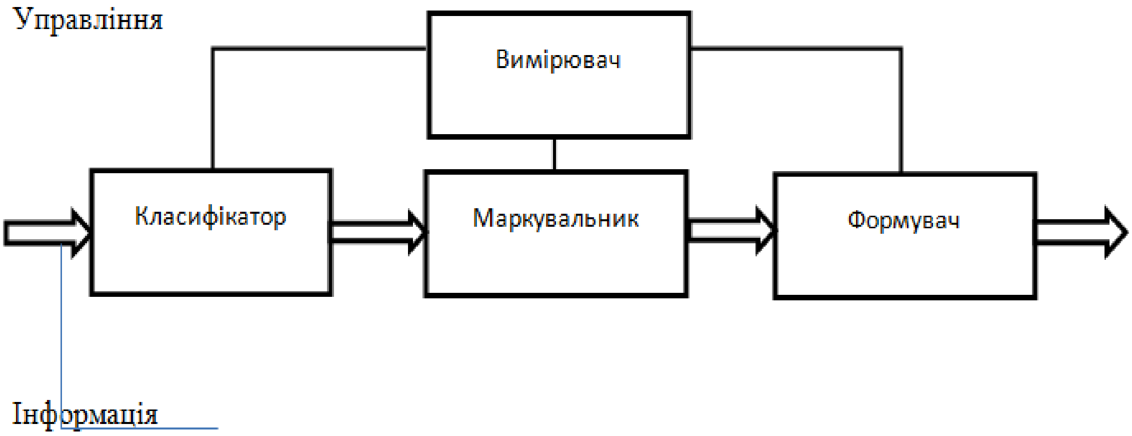


Рисунок 1. Структурна схема обробки пакетів, що надходять

До теперішнього часу для Diff-Serv визначено два класи трафіку:

-клас термінового пересилання пакетів (ExpeditedForwarding PHB Group);

-клас гарантованої пересилки пакетів (AssuredForwarding PHB Group).

Отже, модель DiffServ є оптимальним варіантом для надання потрібної якості з одного кінця мережі до іншого. Реалізація такої моделі дозволяє ліквідувати причину низької якості мультимедійних послуг на основі IP-протокола.

Сервісна модельDiffServ – це відносна простота і висока масштабованість.Виходячи з цього даній моделі відведено місце на магістральних і високошвидкісних ділянках мережі.

Провівши аналіз розглянутих сервісних моделей, які задовольняють вимоги якості надання послуг в мультисервісних мережах,зроблено наступні висновки:

При необхідності передачі великої кількості інформаційних потоків, доцільно використовувати технологію DiffServ, яка забезпечить гарантовану доставку повідомлень.Хоча ця модель і не гарантує якість обслуговування на 100%, у неї є серйозні переваги. Наприклад, немає необхідності в організації попереднього з'єднання і в резервуванні ресурсів. Так як в моделі Diff-Serv використовується невелика, фіксована кількість класів і трафік абонентів розподіляється за загальними чергами тому не потрібна висока продуктивність мережевого обладнання.

Література:

1. Дмитрий Андрушко. Качество обслуживания в сетях IP// Компьютерное Обозрение. - 2003.- №10. - С.7-10. - http://itc.ua/node/15116

2. Armitage Grenville. Quality of Service in IP Networks. - Macmillan Technical Publishing, 2000.

3. ШринивасВегешна. Качество обслуживания в сетях IP (Cisco). – 2003. – 368 С.

4. Коршун Н. В. Основні показники якості інтелектуальної мережі // Матеріали ІІІ Міжнародної науково-технічної конференції студентства та молоді «Світ інформації та телекомунікацій – 2006». – Київ. - 26-27 квітня. - 2006. – С. 76.

Овчаренко М. С.
Студентка групи ІМД-41
Овчаренко А. С.
Студентка групи ІМД-41
Ковтуненко В. О.
Студентка групи ІМД-41
Державний університет телекомунікацій
м.Київ, Україна

ВІРТУАЛЬНІ АТС: ПЕРЕВАГИ ТА МОЖЛИВОСТІ

Зараз все більше розвивається новий напрямок у ІТ сфері — створення віртуальних АТС. Набагато швидше і економічно вигідніше користуватися хмарною телефонною станцією, ніж закуповувати обладнання, встановлювати його, нести витрати по його експлуатації та ремонту.

Віртуальна АТС - сервіс (у вигляді набору програм), який дозволяє виконувати всі функції звичайної АТС, та розміщується на серверах оператора зв'язку або хостинг компанії. При використанні віртуальної АТС клієнт отримує всі функції звичайної АТС, та ряд додаткових послуг (багатоканальний прийом дзвінків, голосове привітання або меню, запис розмов, функції переадресації й розподілу викликів по групах та інше). Усі можливості реалізуються у вигляді послуг, які доступні віддалено через Інтернет.

Рисунок 1 - Принцип організації роботи віртуальної АТС

Традиційна офісна АТС та віртуальна АТС однозначно мають багато спільного, але при цьому значно відрізняються одна від одної. У таблиці 1 представлена порівняльна характеристика цих двох підходів до організації послуг зв'язку, по ряду критеріїв.

Таблиця 1. Порівняльна характеристика підходів до організації послуг зв'язку

Критерій	Віртуальна АТС	Стаціонарна АТС
Оновлення, підтримка	Автоматичне регулярне оновлення при випуску нового функціоналу; безкоштовна цілодобова підтримка	Послуги по оновленню та налаштуванню потребують інвестицій та участі кваліфікованого персоналу.
Затрати на підтримку інфраструктури	Відсутні	Постійно потребують інвестицій
Моштабованість	Велика	Апаратні обмеження: кількість ліній та кількість абонентів обмежені моделлю та ємністю АТС
Вартість володіння	Низка за рахунок необхідності оплати лише функціоналу, який реально використовується. Немає необхідності наймати персонал для її налаштування та підтримки	Висока, за рахунок необхідності обслуговування усієї АТС (як правило має великий функціонал та значну кількість портів), незалежно від повноти її функціонування.

		Значні капіталовкладення для придбання додаткового обладнання (шлюзи, кабелі та ін.). Необхідність мати у штаті компанії спеціаліста по обслуговуванню АТС.
Розширення функціоналу за рахунок впровадження нових послуг	Впровадження по кліку миші	Потребує придбання додаткового обладнання та ліцензій на використання.
Можливість підключення віддалених офісів	Необхідність лише підключення офісів до мережі Інтернет, при цьому достатньо однієї віртуальної АТС для головного офісу та всіх його віддалених філій.	Потрібна АТС для кожного віддаленого офісу.
Статистика та моніторинг викликів	Розгорнутий аналіз та контроль по усім викликам	Складний процес, обмежена кількість та можливості вбудованих засобів статистики.
Контроль даних	Данні знаходяться у провайдера, який має до них доступ.	Доступ до даних компанії має лише її персонал

Таким чином, можливо зробити висновок, що віртуальні АТС на сьогоднішній день є найбільш вигідним та багатофункціональним рішенням для організації зв'язку у невеликих офісах. Але, не зважаючи на ряд переваг, вони мають суттєві недоліки. Найбільш значна проблема, це доступ провайдера до даних компанії, що в свою чергу може призвести до залежності компанії від послуг провайдера. Найбільш проблематичним є те, що при виникненні збоїв у дата-центрі провайдера чи будь-яких нештатних ситуацій, віртуальна АТС повністю припиняє свою роботу.

Ще один недолік, який найчастіше замовчують постачальники послуг, це те, що віртуальні АТС не розрахована на дуже великі навантаження. З ростом номерної бази будуть виникати різного роду збої та погіршення зв'язку. Таке рішення ідеальне для малих офісів, але зовсім не вигідне для великих компаній. Також, слід враховувати той факт, що на практиці, чим нижче вартість послуг, тим більше потім затрати на підтримку та експлуатацію мережі.

Ряд цих недоліків можливо уникнути, якщо розгорнути приватну віртуальну АТС. Таке рішення об'єднує в собі всі переваги віртуальної та традиційної офісної АТС. Рішення являє собою віртуальну машину, розміщену на сервері хмарного провайдера з встановленим програмним забезпеченням.

З використанням приватної віртуальної АТС, власник повністю контролюєте сервер телефонії і дані на ньому. Компанія володіє всією статистикою і впевнена у збереженні конфіденційності своїх даних, при цьому сама обирає налаштування буь-якої складності в залежності від потреби.

Використовуючи приватну віртуальну АТС, ви можете при бажанні змінити хмарного провайдера або перенести проект на внутрішній сервер в офіс. Приватна віртуальна АТС може бути підключена до одного або декількох операторам зв'язку одночасно.

Література:

1. http://habrahabr.ru/post/191856/
2. http://www.skomplekt.com/solution/virtualnaya_ats_otzyvy.htm
3. https://oktell.ru/support/articles/28/

Складанний П.М.

Аспірант каф. Інформаційної та кібернетичної безпеки

Бурячок В.Л.

Д.т.н., с.н.с.,завідувач каф. Інформаційної та кібернетичної безпеки

Державний університет телекомунікацій

м. Київ, Україна

ЗАХОДИ ПРОТИДІЇ ДЕСТРУКТИВНОМУ ВПЛИВУ КІБЕРАТАК

Враховуючи, що всі відомі класи атак будуються на підставі знань про протоколи, які використовуються в мережі Інтернет й реалізуються при цьому, як правило, за типовим алгоритмом (рис.1), поступово стало можливим виділити серед них віддалені і внутрішні атаки та запропонувати типові комплекси заходів протидії їх деструктивному впливу.

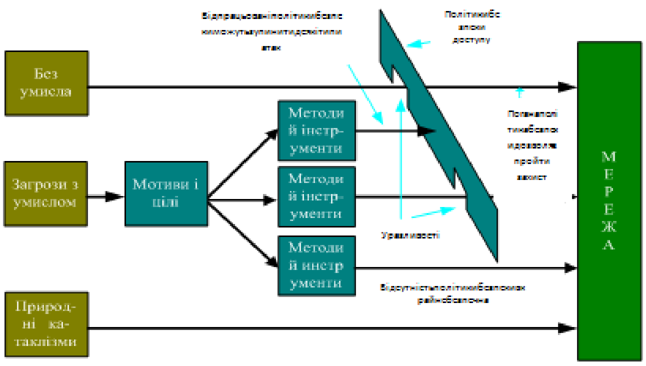


Рисунок 1. Алгоритм реалізаціїкібератаки

Так, наприклад, найвідомішими різновидами DoS атак (атак на ІКС, метою яких є зробити комп’ютерні ресурси/мережу недоступними для користувачів внаслідок: перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної можливості каналу зв’язку, рис. 2) є Flood, ICMPflood, Identificationflood, TCPSYNflood, PingofDeath, TribeFloodNetwork, Trinco, Stacheldracht, Trinity та багато інших атак.

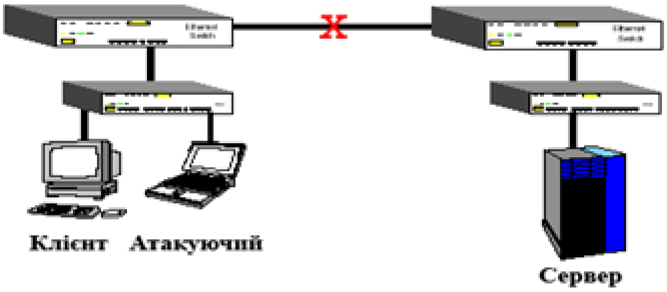


Рисунок 2.Схема DoSатаки

Послабити їх вплив можливо в результаті:

правильної конфігурації на маршрутизаторахі між мережевих екранах функцій антиспуфінга (впровадження фільтрації RFC 2827) та функцій антиDoS;

обмеження обсягу некритичного трафіка (non-criticaltraffic – визначає імовірність того, що мережа зв’язку відповідає заданому та узгодженому трафіку), що проходить мережею. Типовим прикладом такого єобмеженняобсягівтрафіка ICMP, щовикористовуєтьсятільки для діагностичнихцілей.

Найбільш відомими різновидами DDoS атак (підтипу DoS атаки, що здійснюється одночасно з великої кількості IP-адрес/ПЕОМ на систему об’єкта атаки та має за мету зробити мережу недоступною для звичайного використання) єTCPSYNflood (рис.3), TCPflood (рис. 4), SYN-та MAC-flooding(рис.5), UDP-,Smurf- та ICMPfloodатаки.

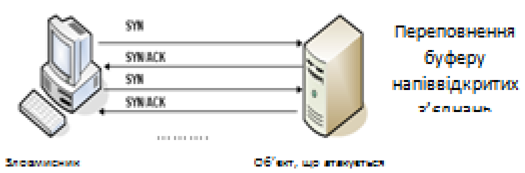


Рисунок 3. TCP SYNflood атака

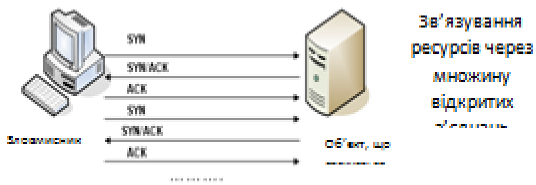


Рисунок 4. TCP flood атака

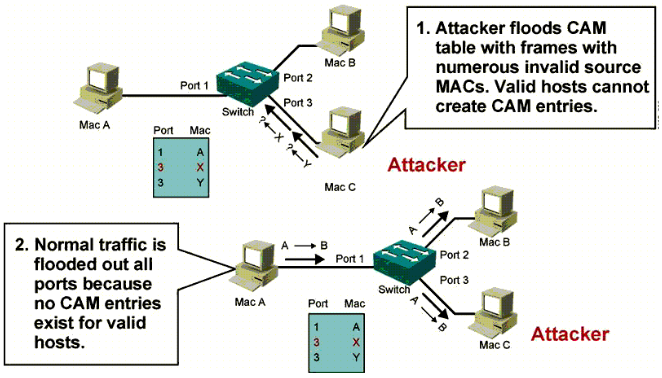


Рисунок 5. MAC-flooding атака

Стандартна схема апаратного рішення захисту від DDoS-атак подана на рис.6.

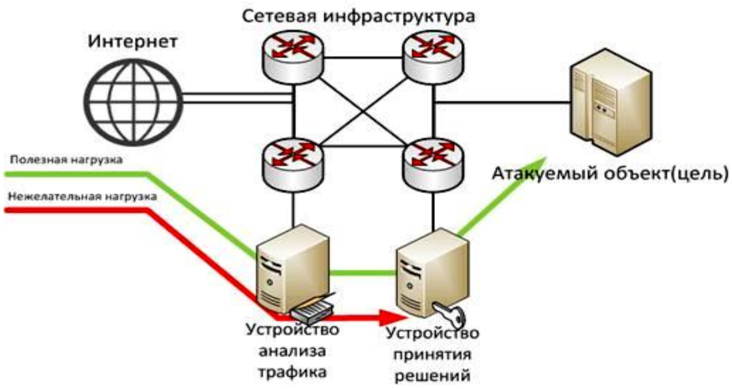


Рисунок 6. Стандартна схема апаратного рішення захисту від DDoS-атак

За звичай схема складається з двох пристроїв: пристрою аналізу на який дублюється весь трафік, що приходить у дата-центр та пристрою прийняття рішень, що блокує небажане навантаження, на основі аналізу даних отриманих пристроєм збору інформації. Іноді дані рішення сполучаються в одному пристрої як, наприклад, рішення від Cisco, що за відсутності активних атак, працює в режимі накопичення інформації про корисне навантаження, а у випадку виникнення шкідливої активності змінюється маршрутизація й починається фільтрація трафіка.Основними методами протидіїDDoS атакам є:

профілактика причин, щоспонукають тих абоіншихосіборганізовуватиDDoS атаки. Дуже часто атаки є наслідкамиособистоїобразиабополітичних, релігійнихрозбіжностей;

розосередженняабопобудоварозподілених і резервних систем, які не припинятьобслуговуватикористувачів, навітьякщодеякіїхніелементистанутьнедоступними;

фільтраціятрафіка на маршрутизаторах (міжмережевіекрани та спеціалізованіantiflood засоби фільтрації – найбільш ефективний, але й найбільш дорогий метод. За можливості їх встановлюють якнайближче до джерела flood. Наприклад, програмний засіб ADoS, який є динамічним фільтром TCP-пакетів, здатний блокувати в реальному часі доступ до Web-сервера з IP-адрес, що генерують інтенсивний потік HTTP-запитів);

розміщення (розташування) безпосередньої цілі атаки – доменного імені або IP-адреси подалі від інших ресурсів, які часто піддаються впливу разом з безпосередньою ціллю;

нарощуваннярессурсівсистеми (якщоfloodспрямований на вичерпанняресурсів, то примітивнішим способом протидіїцьому є нарощуваннявласнихресурсів, щобпротиборча сторона не змоглаїхвичерпати).

Одною з найбільш відомих компаній, які займаються розробкою комплексних рішень щодо протидії DoSi DDoS атак є компанія "NVisionGroup". Фахівці компанії використовують для цього технологіюCiscoCleanPipes, що забезпечує оперативну реакцію на DDoS атаки, легко масштабується, має високу надійність і швидкодію. Зазначена технологія припускає використання модулів CiscoAnomalyDetector і CiscoGuard, а також різні системи статистичного аналізу мережевого трафіку, засновані на даних, одержуваних з маршрутизаторів за протоколом CiscoNetflow. При цьому AnomalyDetector і системи статистичного аналізу трафіку виступають як системи виявлення DDoS атак, а CiscoGuard як засіб протидії вже виявленій атаці. У загальному випадку технологія CleanPipes припускає наявність етапу тестування (навчання), що проводиться в період відсутності DDoS атак на ресурс, що захищається. На цьому етапі пристрої виявлення визначають і запам'ятовують, який трафік для ресурсу, що захищається, є нормальним. Ситуація, за якої поточний трафік на ресурс, що захищається, різко відрізняється від нормального, уважається DDoS атакою. При виявленні DDoS, система виявлення повідомляє оператору та активує підсистему захисту CiscoGuard.

Велике значення проблемам боротьби із DDoS атаками надано нині керівництвом Південної Кореї. Зокрема, з метою запобігання масштабного виходу з ладу критично важливих IT ресурсів, корейський національний центр по боротьбі із кіберзагрозами (KrCERT) створює так звані цифрові "бункери", потужності яких планується надавати власникам корейських IT проектів, які потрапили під дію DDoS атаки. Але, враховуючі використання хакерами все більш новітніх технологій та методів здійснення впливу на ІТС та їх складові – такі засоби захисту здатні лише частково захистити чи лише виявити атаку на об'єкт, що охороняється.

Подальші дослідження слід зосередити на створенні ефективних способіввиявленняDDoS– атак, а саме розроблення програмно-апаратних рішень для придушенняDDoS - атак. Принцип роботияких має бути заснований на навчанні пристрою того, щоможе бути розпізнано як коректно-сформованийтрафік і подальшим виявленні аномалій, а при виявленні аномалій вмикати механізми захисту різного рівня.

Література:

1.Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія./ В.Л. Бурячок. – К.: НАУ.- 2013. – 432с.;

2.БурячокВ.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу // Захистінформації. — 2013. — Том 15, № 1. — С. 5-12.

Цьопа Н.В.
Аспірант каф. Радіомоніторингу та радіочастотного менеджменту
Державний університет телекомунікацій
м. Київ, Україна

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ НАДРОЗРІЗРЮВАЛЬНИХ МЕТОДІВ ПЕЛЕНГАЦІЇ

В результаті широкого розвитку різноманітних засобів радіозв'язку на сьогоднішній день радіомоніторинг радіоелектронних засобів (РЕЗ) має здійснюватися, як правило, в умовах складної електромагнітної обстановки, великої апріорної невизначеності щодо параметрів радіовипромінювань при їх багатопроменевому розповсюдженні, в умовах часу наближеного до реального. Все це стимулює розвиток засобів автоматичного радіомоніторингу (АРМ). До числа АРМ належать засоби автоматизованого пеленгування (ЗАП), які отримали широке застосування у вирішенні великої кількості задач різноманітних напрямків і є базою для реалізації технічних заходів при протидії несанкціонованому доступу до інформації, в тому числі спеціальних досліджень побічних електромагнітних випромінювань та наводок.

В задачах радіопеленгування досить часто виникає необхідність шляхом обробки досліджуваного сигналу на кінцевому інтервалі спостереження, визначити кількість джерел випромінювання (ДВ), які формують прийнятий сигнал та максимально точно оцінювати їх кутові координати. При цьому несучі частоти джерел ДВ найчастіше є майже однаковими. До таких випадків відносяться, навмисні завади, що створюються із різних точок простору певними РЕЗ.

Основний метод боротьби з навмисними завадами в радіоелектронних системах (РЕС) з цифровими антенними решітками (ЦАР) полягає у формуванні провалів діаграми спрямованості в напрямку на джерело завад.

В умовах нестаціонарної завадової обстановки вказаний метод формування провалів діаграми спрямованості ЦАР може бути реалізованим, якщо заздалегідь визначити число та кутові координати джерела завад.

Велике значення співвідношення потужності активних завад до потужності внутрішнього шуму на виході антенної системи створює сприятливі умови для пеленгації ДВ із застосуванням сучасних методів цифрового спектрального аналізу (ЦСА) [1, с. 66-68, с. 260-262]

Незважаючи на значну кількість робіт, присвячених порівняльному аналізу надрозрізнювальнихметодів ЦСА, необхідно відзначити, що в кожній з них одночасно порівнюються лише кілька методів і то за окремими показниками [2-5]. Отримані часткові результати, іноді суперечать один одному, не дозволяючи надати їм закінчену оцінку. Тому проблема порівняльного аналізу надрозрізнювальнихметодів ЦСА залишається актуальною і на теперішній час.

Для дослідження ефективності розрізнювальної здатності були взяті відомі в цифровому спектральному аналізі методи спектральні функції яких мають наступний вид [6, с. 23-39]:

$$\widehat{S}_1(\Omega) = \left(\mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega)\right)^{-1}; \quad (1)$$

$$\widehat{S}_2(\Omega) = \left(\mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}^2\cdot\mathbf{X}(\Omega)\right)^{-1}; \quad (2)$$

$$\widehat{S}_3(\Omega) = \widehat{\omega}_{mm}\left|\,\mathbf{e}_m^*\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega)\,\right|^{-2}, m\in 1,M; \quad (3)$$

$$\widehat{S}_4(\Omega) = \widehat{\omega}_{mm}\mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega)\cdot\left|\,\mathbf{e}_m^*\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega)\right|^{-2}, m\in 1,M \quad (4)$$

$$\widehat{S}_5(\Omega) = \mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega)\,\left(\mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}^2\cdot\mathbf{X}(\Omega)\right)^{-1}; \quad (5)$$

$$\widehat{S}_6(\Omega) = \mathbf{X}^*(\Omega)\cdot\widehat{\mathbf{\Psi}}\cdot\mathbf{X}(\Omega). \quad (6)$$

Спектральні функції $\widehat{S}_1(\Omega)$ характеризують метод максимальна правдоподібність Кейпона (МПК), $\widehat{S}_2(\Omega)$ - метод Тепловий шум (ТШ), $\widehat{S}_3(\Omega)$ - метод Лінійне передбачення Берга (ЛПБ), $\widehat{S}_4(\Omega)$ - метод Модифікований алгоритм Кейпона (МАК), $\widehat{S}_5(\Omega)$ - метод Борджотті-Лагунаса (БЛ), $\widehat{S}_6(\Omega)$ - метод Дискретне перетворення Фур'є (ДПФ)

Для наведених функцій використовуються такі позначення: $\mathbf{X}(\Omega) = \left\{\, x_l(\Omega)\right\}_{l=1}^{M}$ - М мірний вектор пошуку в напрямку (Ω); $\widehat{\Psi} = \left\{\,\widehat{\omega}_{ij}\right\}_{i,j=1}^{M}$ - $M\times M$ матриця, що є оцінкою максимальної правдивості кореляційної матриці процесів, які спостерігаються на виході АР; $\widehat{\omega}_{mm}$ - елемент, що знаходиться на перетині m-го стовпця та m-ї строки матриці; $\mathbf{e}_m$ - m-й $\left(m\in 1,M\right)$ стовпчик одиничної матриці, (*) - знак ермітового сполучення.

Для експериментального дослідження методів (1-6) був розроблений експериментальний вимірювальний комплекс. Умови проведення експериментального дослідження були наступні. В якості двох локальних джерел вторинного випромінювання (ЛДВВ) були взяті дві металеві кулі діаметром 3,5 см рознесені на відстань $\Delta r = 30$ см. Відстань від приймальної антени до найближчого ЛДВВ складала 3,85 метри. Максимальна девіація частоти зондувального лінійного частотно-модульованого (ЛЧМ) сигналу при кількості відліків М - мірного вектору рівному 43, за час спостереження $t_{\text{СП}} = 4$mс складала приблизно 1 ГГц, що відповідало розрізнювальній здатності за Фур'є $\Delta f_{\Phi} = 1/t_{\text{СП}} = 1/4$mс=250,00 Гц. Максимальне значення величини відношення сигнал/шум складало 35 дБ.

В результаті проведеного експерименту були виміряні значення для побудови графіків залежності частоти сигналів відбитих від 2-х ЛДВВ від амплітуда сигналу $S = f(\Omega)$. Аналіз побудованих графіків показав, що при заданих однакових умовах проведення експерименту не всі з досліджуваних методів спроможні розрізнити два ЛДВВ за критерієм Релея. При цьому найкращу розрізнювальну здатність мав метод ЛПБ: на графіках отриманих для цього методу спостерігались два максимуми, що відповідали двом розрізненим сигналам відбитим від двох металевих кульок. За таких же умов проведення експерименту методи МПК, ТШ та ДПФ мали лише один максимум і не спроможні були здійснити розрізнювання двох ЛДВВ за критерієм Реле. Застосування методів БЛ та МАК взагалі недоцільно, оскільки вони мали випадкові спектральні максимуми і не могли дати адекватну оцінку значення $S = f(\Omega)$.

Узагальнений графік нормованих значень $S = f(\Omega)$ для кожної з досліджених спектральних функцій (1-6) показав, що спектральні функції (1-3, 6) мають свої максимуми в діапазоні частот (4500 -5500) Гц, який за дальністю відповідає ділянці простору, де знаходилися два ЛДВВ.

Таким чином, проведений огляд запропонованих методів пеленгації джерел радіовипромінювань показав перевагу в застосуванні алгоритму лінійного передбачення Берга у порівнянні з іншими досліджуваними методами при вирішенні задач максимально точного знаходження координат пеленгу локальних джерел випромінювання в умовах часу наближеного до реального.

Література:

1. Марпл.-мл. С. Л. Цифровой спектральный анализ и его приложения: Пер.с англ. — М.: Мир, 1990. - 584 с.
2. Добырн В.В. Эффективность применения сверхразрешающих спектральных оценок в бортовых угломерных фазированных антенных решетках /В.В. Добырн, А.В. Немов // Радиотехника. - 1999. - №9. - С. 65-67.
3. Гершман А.Б. Адаптивное разрешение некоррелированных источников по координате. / А.Б. Гершман, А.Т. Ермолаев, А.Г. Флаксман // Изв. вузов. Радиофизика. - 1988. - №8. - С. 941-946.
4. Леховицкий Д.И. Разновидности сверхразрешающих анализаторов пространственно-временного спектра случайных сигналов на основе обеляющих адаптивных решетчатых фильтров / Д.В. Атаманский, И.Г. Кириллов. Д.И. Леховицкий // Антенны. - 2000. - №2. - С. 40-54.
5. Мюнье Ж. Делиль Ж.Ю. Пространственный анализ в пассивных локационных системах с помощью адаптивных методов // ТИИЭР. 1987. - Т. 75, № 11. - С. 21 – 37;
6. Леховицкий, Д.И. Статистический анализ сверхразрешающих методов пеленгации источников шумовых излучений в АР при конечном объеме обучающей выборки / Д.И.Леховицкий, П.М.Флексер, Д.В. Атаманский, И.Г.Кирилов // Антенны. - 2000. - Вып. 2 (45). - С. 23-39.

Жданова Ю.Д.
Доцент каф. Інформаційної та кібернетичної безпеки
Березюк А.С.
Студент навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Бурхливе розповсюдження використання інформаційно-комунікаційних систем (ІКС) та мереж значно розширюють можливості для обміну інформацією між абонентами. Сьогодні електронні документи, якщо не витісняють паперові, то є гідною їм альтернативою. Однак, в електронного документа є суттєва відмінність від паперового – його копіювання, зміна і видалення не представляють ніякихтруднощів. Тому основні проблеми, що встають перед абонентами інформаційних систем, полягають в порушенні:

конфіденційності – ознайомленні з документом осіб, що не мають на це право.

цілісності – модифікації документа особою, що не має на це право.

авторства – можливості створити електронний документ від імені іншої особи або підробки його атрибутів, наприклад, часу створення.

Ще зовсім недавно основний аспект захисту електронного документообігу (створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів), полягав у збереженні конфіденційності повідомлень, які передаються.[1]Відсутність можливості перевірки достовірності і авторства документів, що пересилаються, є істотним недоліком багатьох ІКС. Це не дозволяє використовувати такі системи для укладання операцій, що юридично визнаються або для передачі юридично підтверджуваних документів. Цю проблему можна вирішити шляхом використання електронного цифрового підпису – засобу, що дозволяє на основі криптографічних методів надійно встановити авторство і достовірність документу.[2-4]

Найбільш простий вид цифрового підпису є так званаімітовставка, яка реалізується у вигляді шифру контрольної суми по повідомленню. Імітовставкамає складну залежність від секретного ключа і всього масиву даних, тому підробити її, не знаючи ключа, неможливо. Оскільки секретний ключ відомий тільки двом (або групі) кореспондентів, то отримання повідомлення, захищеного імітовставкою, виробленою на даному ключі, підтверджує належність автора повідомлення до цієї групи.

Проте повною мірою достовірність і авторство документа встановлює електронний цифровий підпис (ЕЦП), що дозволяє замінити при безпаперовому документообігу традиційні підпис і печатку.В основі більшості алгоритмів електронного цифрового підпису лежить ідея шифрування з відкритим ключем.

Перші практичні кроки запровадження електронного документообігу і застосування електронного цифрового підпису зроблено 17 січня 2006 року, коли Центральний засвідчувальний орган вручив перше в Україні свідоцтво про акредитацію Центру сертифікації ключів електронного цифрового підпису, яким стала Науково-виробнича фірма «Українські національні інформаційні системи» (м. Дніпропетровськ). В Україні уже існують чотири таких центри. Це означає, що електронний підпис можна уже застосовувати на рівні із власноручним.

Переваги використання електронного документообігу:

перехід до більш зручного, швидкого і економного безпаперового юридично значимого документообігу;

криптографічний захист інформації (електронних документів) при передачі по відкритих каналах зв'язку;

мінімізація фінансових ризиків за рахунок підвищення конфіденційності інформаційного обміну документами;

значне скорочення процедури підписання договорів, оформлення та швидкий і надійний обмін електронними документами з партнерами, контрагентами незалежно від віддаленості адресата.

Цей перелік можна подовжувати, але наразі навіть важко уявити обсяги застосування електронного цифрового підпису у життєдіяльності держави, приватного сектору, та особистому житті громадян. Відтепер кожен громадянин, підприємець, посадова особа вже має можливість засвідчувати електронні документи своїм власним цифровим підписом, який має таку саму юридичну силу як власноручний підпис чи печатка. Для юридичних осіб передбачено використання додаткового цифрового підпису – аналога відбитку печатки. Для забезпечення такого рівня захисту використовуються посилені сертифікати ключів, що надаються акредитованими центрами сертифікації ключів. Використання посилених сертифікатів дозволяє виконувати юридично-значущий захищений електронний документообіг між будь-якими суб'єктами правових відносин: юридичними і фізичними особами, підприємцями та органами державної влади.

Література:

1.Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 №851-IV(зі змінами та доповненнями)

2.Закон України «Про електронний цифровий підпис» від 22.05.2003 №852-IV (зі змінами та доповненнями)

3.ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис що грунтується на еліптичних кривих – К.: ДКУ з питань ТР СП, 2003.

4.Гулак Г.Н., Мухачев В.А., Хорошко В.А., Основы криптографической защиты информации. – К.: Изд. ГУИКТ, 2009

Гаманюк І.М.
Ст. викладач каф. Прикладного програмування
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ МОДЕЛЮВАННЯ СИСТЕМИ УПРАВЛІННЯ В СИСТЕМІ ЗІ СКЛАДНОЮ ДИНАМІКОЮ В ІНФОКОМУНІКАЦІЯХ

Актуальною проблемою розвитку суспільства є визначення можливостей тієї, чи іншої системи до виконання визначених завдань. Нерозуміння можливостей системи призводить до неефективного управління системою, а саме постановка завдань, які система не може виконати, або які система може виконати без жодних зусиль, залучаючи до виконання мізерну частину своїх можливостей.

В сучасному суспільстві все частіше постає проблема щодо взаємодії різних систем, об'єднанню їх в тимчасові системи або роздробленню їх на дрібніші системи.

Для вирішення таких проблем та зменшення негативних наслідків реформування створюються відповідні системи моніторингу ситуації та управління процесами трансформації. Головним завданням систем трансформації є відслідковування показників систем і визначення їх відповідності вимогам.

Отже, що розумітимемо під системою.

Під системою розумітимемо множину взаємозв’язаних, взаємозалежних елементів будь-якої природи, які поєднані за деякими системотвірними ознаками, утворюють єдине ціле та підпорядковані певній спільній меті.[1, п.1.1.]

Під системою зі складною динамікою в інфокомунікаціях розумітимемо множину (яка постійно змінюється) взаємозв'язаних, взаємозалежних елементів, які поєднані за деякими системотвірними ознаками, утворюють єдине ціле та підпорядковані певній спільній меті (виконанню завдання). Бажано прийняти таке припущення, що зміна множини не є суттєвим чинником на виконання завдання, але є суттєвим чинником на процес прийняття рішення системою управління системи.

Так наприклад: Система має 4 елементи. Для вирішення певного завдання необхідно 3 елементи. Протягом часу $t_{\text{виконання завдання}}$, необхідного для виконання завдання, кількість елементів системи змінилася з 4 елементів до 3. Це не вплинуло на виконання завдання, але при виникненні аналогічного завдання в майбутньому є ймовірність, що кількість елементів зменшиться до 2 і тоді система не виконає завдання.

Головна проблема, яку необхідно вирішити: “Чи здатна система виконати поставлене перед нею завдання”.

Іншою проблемою є: “Як змінити систему, щоб отримати систему, яка здатна вирішити завдання за умови досягнення мінімального необхідного рівня можливостей”.

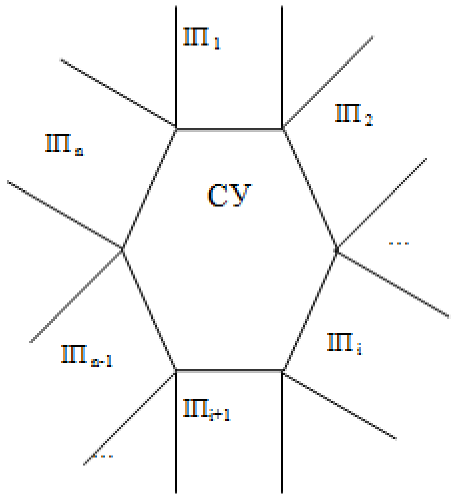
Так наприклад: Система має 6 елементів. Для виконання завдання необхідно 3 елементи. Для забезпечення стійкості роботи системи необхідно, щоб система мала від 3 до 5 елементів. Враховуючи зазначене, можна приймати рішення про скорочення системи до 5 елементів, тим самим зменшуючи витрати та підвищуючи ефективність системи.

Для вирішення проблеми щодо здатності системи необхідно визначити показники за якими характеризувати систему та критерії до них для визначення здатності системи.

Для зручності здається можливим розділити систему на систему управління та об'єкт управління. Та досліджувати їх окремо.

Також СУ можна поділити на окремі підсистеми управління і розглядати ці підсистеми, як елементарні системи управління (системи управління).

Пропонується в моделі системи управління варіант моделі прийому (передачі) інформації СУ.



Враховуючи те, що в системах управління усе частіше використовуються системи електронного документообігу, то система управління рідше стикається безпосередньо з джерелом інформації, все частіше це здійснюється опосередковано (через систему електронного документообігу).

СУ можна представити як коло до якого приєднуються інформаційні потоки інфокомунікацій.

Інформаційні потоки можуть від’єднуватися і приєднуватися.

СУ взаємодіє по черзі з усіма інформаційними потоками і отримує (передає) інформацію. Після взаємодії інформаційний потік від’єднується.

Інформація в інформаційних потоках передається як до СУ, так і від СУ.

Інформаційні потоки можуть бути як із зовнішнього середовища так і від об’єкту управління.

На отримання (передачу) інформації необхідно певний час. Цей час обмежено певною величиною $t_{\text{обмеження взаємодії}}$.

У випадку, коли потреба у часі перевищує $t_{\text{обмеження взаємодії}}$ тоді прийом (передача) інформації припиняється, запам'ятовується стан щодо отримання (передачі) інформації і здійснюється перехід до нового інформаційного потоку. Після взаємодії з іншими інформаційними потоками управління передається по колу до інформаційного потока потреба у часі, якого перевищувала $t_{\text{обмеження взаємодії}}$. На цьому інформаційному потоці відновлюється стан щодо отримання (передачі) інформації і продовжується взаємодія.

СУ має обмежену кількість одночасно приєднаних інформаційних потоків.

У випадку, коли приєднано до СУ максимальна кількість інформаційних потоків, то при намаганні приєднатися до СУ новому інформаційному потоку буде відмовлено в приєднанні.

Таким чином, при швидкому обході всіх інформаційних потоків здаватиметься, що СУ одночасно (паралельно) взаємодіє з великою кількістю інформаційних потоків.

У такій моделі застосовується принцип: інформаційний потік, що має великий об'єм інформації обслуговується довше, а інформаційний потік що має менший об'єм інформації обслуговується коротше.

СУ може характеризуватися швидкістю прийому (передачі) інформації одного потоку.

Моделюючи таким чином, можна по кількості інформаційних потоків і об'єму інформації в них, яка планується до прийому (передачі), визначити, чи буде зазначена система управління здатною прийняти (передати) вказану інформацію, і як наслідок управляти об'єктом управління.

Вирішення цієї проблеми дозволить перенаправляти неопрацьовані інформаційні потоки до інших систем управління, якщо вони здатні приймати рішення щодо інформації такого типу. У випадку нестачі таких систем управління, можна приймати рішення щодо створення нових систем управління.

У випадку недонавантаження системи управління можна піднімати питання, щодо скорочення кількості систем управління в системі, а неопрацьовані інформаційні потоки перенаправляти на інші системи управління.

Також можна змінювати внутрішню структуру системи управління з метою підвищення швидкості прийому (передачі) інформації за рахунок створення паралельних структур всередині системи управління, а також з метою зменшення витрат на систему управління, і як наслідок зменшення максимально можливої швидкості прийому (передачі) інформації, за рахунок скорочення паралельних структур.

Література:

1. Шарапов О.Д., Дербенцев В.Д., Семьонов Д.Є., Економічна кібернетика. Навч. посібник. — К.: КНЕУ, 2004. — 231 с. http://buklib.net/books/21911/.

Дуксенко Н. А.
студент
Гнатюк С. О.
К.т.н, доцент каф. Безпеки інформаційних технологій
Національний авіаційний університет
м.Київ, Україна

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ХМАРНИХ СХОВИЩ ДАНИХ

У наш час інформатизація суспільства набирає помітних обертів. Напевно, перед кожним користувачем поставала проблема надлишковості власних накопичених файлів та нестача вільного простору для їх зберігання у пам'яті пристрою. З появою високошвидкісного Інтернету це питання вирішують хмарні технології. Їх інтенсивне освоєння IT-компаніями, застосування у малому та середньому бізнесі, навчальному процесі, для управління підприємствами свідчить про черговий якісний стрибок у галузі інформаційних технологій.

Метою роботи є аналіз загроз хмарним сховищам даних та формування рекомендацій для забезпечення їх безпеки.

Хмарне сховище даних – це модель онлайн-сховища, в якому дані зберігаються на численних розподілених у мережі серверах, що надаються в користування клієнтам, в основному, третьою стороною [2, с. 78]. Перевагами використання хмарних сховищ даних являються: економія дискового простору на жорсткому диску комп'ютера; доступ до даних здійснюється з будь-якого місця та в будь-який час за наявності під'єднання до глобальної мережі Інтернет; користувач сплачує тільки за те місце у сховищі, яке фактично використовує або користується певним обсягом дискового простору хмарного сховища безкоштовно; всі процедури із збереження цілісності даних забезпечуються провайдером хмарного центру; дані можна не тільки переглядати, але і міняти редагувати; обмін файлами; спільна робота з файлами. За результатами опитування компанії Symantec у 2011 році, 44% керівників побоюються переміщати критично важливі для бізнесу програми до хмарних середовищ. При цьому 76% вважають питання безпеки основною проблемою. Проте, за підрахунками авторитетної International Data Corporation (IDC), у 2015 році до 60 % всіх даних людства зберігатиметься у хмарах [1]. Це свідчить про популяризацію та активне використання хмарних сховищ даних різними категоріями населення, але питання безпеки все ж потребує більшої уваги.

До відомих типів загроз (мережеві атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) додалися складнощі, що пов'язані з контролем середовища, трафіком між гостьовими машинами та розмежуванням прав доступу. Можливі такі атаки на хмарні середовища:

1) на елементи хмари;
2) на програмне забезпечення;
3) на клієнта («викрадення» паролів, перехоплення веб-сесії);

4) на гіпервізор (один з ключових елементів віртуальної системи, що відповідає за поділ ресурсів між віртуальними машинами, атака на який призводить до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої, а згодом і витіснити віртуальну машину з сервера);

5) на системи управління (поява віртуальних машин-невидимок, здатних блокувати одні віртуальні машини і підставляти інші).

Як засоби протидії зазначеним атакам можна запропонувати наступні:

1) контроль цілісності сторінок, правильне резервне копіювання, розмежування доступу;

2) встановити міжмережевий екран, антивірус;

3) правильна аутентифікація та використання шифрованого з'єднання з взаємною аутентифікацією;

4) використання політик складності і старіння паролів, а також стандартизацію процедур доступу до управляючих засобів хост-сервера, застосовувати вбудований брандмауер хоста віртуалізації;

5) наявність систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин;

6) ізоляція користувачів, тобто використання індивідуальної віртуальної машини і віртуальної мережі;

7) суворий контроль фізичного доступу до серверів і мережевої інфраструктури.

Отже, хмарні технології інтенсивно розвиваються і надалі будуть ставати зручнішими та універсальними. Проте питання безпеки даних користувачів потребує більшої уваги та формування нових рішень з боку компаній, що пропонують послуги та займаються розробкою хмарних сховищ. Подальші дослідження будуть присвячені детальному аналізу загроз та уразливостей сучасних сервісів доступу до хмарних сховищ даних.

Література:

1.IDC Predictions 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електроннийресурс]. - Режимдоступу : http://clck.ru/8aXZM

2.Елементи розвитку та перспективи досліджень технології хмарних обчислень / Угрин Д. І., Шевчук С. Ф. // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – Х: НТУ «ХПІ», – 2013. - № 70 (1043). – С.74-79 . – Бібліогр.: 5 назв.

Івченко М.М.
Провідний науковий співробітник науково-дослідного відділу
Мусієнко В.А.
Начальник науково-дослідного відділу
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації
м. Київ, Україна

ОБГОВОРЕННЯ ПРОБЛЕМНИХ ПИТАНЬ ТА ВИЗНАЧЕННЯ ПРІОРИТЕТНИХ НАПРЯМКІВ ПОБУДОВИ МЕРЕЖІ ВЗАЄМОДІЇ МІЖ СИЛОВИМИ ВІДОМСТВАМИ

Сучасна розстановка сил на міжнародній арені, проведення антитерористичної операції на Сході України, процес реформування Збройних Сил України, внутрішніх військ МВС України та інших силових структур зумовили кількісні та якісні зміни у їх складі, необхідність пошуку нових напрямків у підвищенні ефективності дій військ –насамперед їх взаємодії.

Успіх спільних дій військ прямо залежить від взаємної поінформованості про обстановку й умови, у яких вирішуються спільні завдання.

Створення в інформаційному просторі держави виділеної телекомунікаційної мережі спеціального призначення (далі – ТМСП) як найважливішого фактору взаємодії між силовими відомствами стало ключовим при вирішенні питань взаємодії.

Формулювання мети доповіді.Метою доповіді єаналіз побудови виділеної ТМСП, висвітлення проблемних питань при її створенні та визначення пріоритетних напрямків для її побудови на основі передових світових технологій в галузі телекомунікацій.

Результат дослідження. Мережі зв'язку спеціального призначеннязастосовують для забезпечення діяльностіорганів державного управління, оборони, безпеки й охорони правопорядку в країні та реалізації їх потреб в інформаційному обміні.

Функціонування ТМСП в Україні пропонується мати на основі створення єдиного інформаційно-телекомунікаційного середовища, із впровадженням сучасних інформаційно-телекомунікаційних технологій, протоколів обміну інформацією, комплексів і систем зв'язку спеціального призначення, що забезпечить обмін усією інформацією (голос, дані, відео) між органами й пунктами управління (всіх ланок) з відповідною пропускною спроможністю, достовірністю та надійністю [1].

Для розв'язку безлічі подібних завдань розроблена архітектура MPLS (Multiprotocol Label Switching) – технологія багатопротокольної комутації міток [2].

Головна особливість технології MPLS – відділення процесу комутації пакета від аналізу IP-адреси в його заголовку, що дозволяє здійснювати комутацію пакетів значно швидше [2].

У рамках архітектури MPLS разом з пакетом дозволено передавати не одну мітку, а цілий їх стік. Такий підхід дозволяє створювати ієрархію потоків у мережі MPLS і організовувати тунельні передачі.

ТМСП являє собою саме виділену ємність (фактично виділені порти комутаторів загального користування) у мережах передачі даних ПАТ “Укртелеком” [3].

Доступ до кінцевого обладнання абонентів у державних органах має відбуватися каналамиEthernet. Для магістральної передачі даних у ТМСП використовується технологія MPLS.Дані надходять у систему зашифрованим абонентським обладнанням з використанням стійких алгоритмів української розробки. У такий спосіб формується захищена мережа [3].

ТМСП складається з двох сегментів – SDH та IP транспорту, які мають різне сервісне і функціональне призначення, що забезпечує захист і швидке відновлення при аваріях на відповідних кільцевих сегментах [4].

Крім того, технологія MPLS дозволяє інтегрувати мережі IP і ATM (Asynchronous Transfer Mode), за рахунок чого постачальники послуг зможуть не тільки зберегти засоби, інвестовані в устаткування асинхронної передачі, але й покористуватися зі спільного використання цих протоколів.

У результаті технологія MPLS дозволяє ефективно підтримувати необхідну якість обслуговування, не порушуючи наданих користувачеві гарантій.

Можливо виділити три основні області застосування протоколу MPLS в телекомунікаційній мережі спеціального призначення. Це керування трафіком, підтримка класів та якості обслуговування й віртуальна приватні мережі (Virtual Private Network, діалі – VPN).

Висновки. Аналізуючи побудову виділеної ТМСП слід відмітити, що вона є свого роду надбудовою над інфраструктурою оператора ПАТ «Укртелеком». Але навіть якщо припустити, що фізичні оптичні волокна перейдуть у державну власність, колодязі та інші об’єкти кабельного господарства все одно залишаться в приватних руках.

Суміщення лише однієї ТМСП з вузлами зв’язку розташованими на ПАТ «Укртелеком» значно знижує живучість проводової мережі зв’язку ЗСУ, що було підтверджено на практиці під час анексії АРК Крим Російською Федерацією.

Використовуючи технологію MPLS в ТМСП можливо також здійснити балансування навантаження в мережі – рівномірно розподіляючи трафік між маршрутизаторами, у результаті цього не виникає перевантажень устаткування, не виходять із ладу маршрутизатори — ефективність мережі не знижується, що дозволить значно розширити наявні перспективи масштабування, підвищити швидкість обробки трафіка й надати величезні можливості для організації додаткових послуг [5].

Основний недолік MPLS мережі — це дороге встаткування та значні витрати на проектування й обслуговування мережі та необхідність в професійно підготовлених інженерних кадрах, що мають досвід роботи в побудові таких мереж. Однак переваг MPLS мережі значно більше, головними з яких є висока продуктивність, висока надійність, гарантована пропускна здатність каналу споживача й спільне використання із протоколами канального й мережевого рівнів.

Завдяки тому, що VPN будуються на базі архітектури MPLS, додавання нових вузлів віртуальної мережі не привносить складностей з масштабуванням [6].

При використанні технології VPN MPLS можливо ефективно забезпечити якісну передачу інформації по IP-мережам, передачу чутливого до затримок трафіка й тим самим впровадити в виділеній ТМСП такі телекомунікаційні послуги як передача в реальному масштабі часу голосу й відеозображення, з забезпеченням повноцінного використання таких сервісів, як відеотелефонія, відеоконференцзв’язок, віддалене відеоспостереження за державним кордоном та інші.

Література:

1.Замисел переоснащення системи зв’язку Збройних сил України цифровими засобами на період 2013–2017 років та шляхи його реалізації.

2.Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы/ Олифер В.Г., Олифер Н.А.: Учебник для вузов 4-е изд. – СПб.: Питер, 2010. – 944.

3.Прес-служба Держспецзв’язку. Держспецзв’язку підвищить технічні можливостінаціональної системи конфіденційного зв’язку за допомогою телекомунікаційної мережі спеціального призначення.[Електронний ресурс]. Режим доступу:

http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=116087&cat_id=112509.%20html

4.Дмитриченко С.В. Створення телекомунікаційної мережі спеціального призначення: Тези доповідей та виступівучасників ІІІ Всеукраїнської науково-практичної конференції з міжнародною участю[„Сучасні проблеми інформаційної безпеки на транспорті”] / Дмитриченко С.В. – М.: ДСТЗІ, 2013.

5.Адміністрація Державної служби спеціального зв’язку та захисту інформації України, Фонд державного майна України; Наказ № 266/739 від 19.05.2015р. „Про затвердження Порядку безоплатної передачі у державну власність виділеної телекомунікаційної мережі спеціального призначення”.

6.Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS/Захватов М.: CiscoSystems, 2007, с. 4 – 18

Сергєєва Л.А.
Доцент каф.Безпеки життєдіяльності та охорони праці
Вальченко О.І.
Доцент каф.Безпеки життєдіяльності та охорони праці
Державний університет телекомунікацій
м. Київ, Україна

БІОФІЗИЧНІ ПРОБЛЕМИ РАДІОВИПРОМІНЮВАННЯ

При узагальнені даних наукової літератури щодо впливу електромагнітних полів та випромінювань (ЕМВ) ультрависокої та надвисокої частот на тканини та організм людини в цілому визначено, що в залежності від джерела радіохвиль (комп'ютери чи мобільний телефон) їх дія визначається як загальна або локальна (відповідно вказаних джерел). У всіх сферах життєдіяльності людини на сучасному етапі широко використовується система WI-FI технологій, гігієнічне регламентування якої тільки почалося [1, с.193].

Загальний вплив радіовипромінювання невеликої (нижче теплової) інтенсивності на організм людини реалізується переважно через його рефлекторну дію на центральну нервову систему (ЦНС) [2, с.80-82]. Найбільш чутливим до впливу радіохвиль є гіпоталамус, де зосереджені вищі вегетативні центри, тому відмічаються зміни нейрогуморальної регуляції. В ЦНС при дії ЕМВ радіохвильового діапазону змінюється не тільки ультраструктура рецептора, а й ліпідні мембрани нервових клітин, вміст медіаторів ЦНС [10, с.52-53].

Встановлено, що парасимпатична частина вегетативної нервової системи (ВНС) більш чутлива до дії радіовипромінювання, ніж симпатична.

Практично всі діапазони ЕМП чинять дезактивуючий вплив на електричні процеси в корі і підкіркових утвореннях головного мозку [6, с.233]. При радіохвильовому впливі порушується передача інформації в більш складні структури мозку та психоемоційний стан людини [11, с.221].

Локальні впливи частіше обумовлені безпосередньою дією на тканини та органи (головний мозок). Дія радіовипромінювання на головний мозок реалізується складним комплексом біофізичних, фізико-хімічних, квантово-біологічних ефектів. На клітинному і субклітинному рівнях виявляються зміни калій-натрієвого градієнта в клітинах, виникає поляризація біологічних мембран з порушенням їх проникності, деформація структур водних систем, зміна активностей ферментів, порушення окислювальних процесів і т.ін.[3, с.773-779; 5, с.172].

За даними літератури локальні впливи на головний мозок радіовипромінювання від мобільних телефонів може перевищувати граничні рівні теплового ефекту (ГДР ЕМВ). При цьому: підвищується вміст білків теплового шоку; збільшується вміст біологічно активних речовин, таких як гістамін та серотонін, що змінюють ступінь проникності гематоенцефалічного бар'єру (ГЕБ) для небезпечних речовин [8, с.739-747; 9, с.14]. Деякі автори обумовлюють підвищенням ГЕБ таку симптоматику впливу ЕМВ на головний мозок як: головний біль, запаморочення, підвищена стомлюваність [12, с. 43-46], вказують на можливість проникнення в ліквор ряду ендогенних біологічно активних речовин, не бажаних для діяльності мозку.

Окрім вищезазначеного, поширено обговорюється тема резонансу частот ЕМВ на мембранах клітин та затухання радіохвиль в тканинах організму [7, с.133]. Резонансну взаємодію низькоінтенсивних мікрохвиль міліметрового випромінювання із власними когерентними коливаннями визначив в своїй науковій праці Девятков Н.Д. [4, с.127]. Відомий факт, що радіохвильовий діапазон монітора складає 20 Гц...1000 МГц, причому 20 Гц – резонансна частота серця, 8 - 300 Гц – на цих частотах визначається резонанс кровоносної системи.

Чим більше частота радіохвиль, тим більша їх біологічна дія: 10000 МГц – енергія вся поглинається в поверхневих шарах біоструктури, відбувається швидке загасання електромагнітних хвиль [7, с.135]; менше за 30 МГц – величина поглинання швидко знижується. Підшкірний жировий шар може грати роль четверть-хвильового трансформатора, що узгоджує хвильові опори шкіри та м’язової тканини, яка межує з жировим шаром. При цьому доля енергії, що проходить через тіло, може значно збільшитися. Цей ефект залежить від товщини шкіри та частоти поля та потребує перевірки.

Література:

1). Біткін С.В., Думанський В.Ю., Нікітіна Н.Г. та ін. Обґрунтування методичного підходу до вивчення та гігієнічної оцінки впливу електромагнітного випромінювання WI-FI технологій на учнів загальноосвітніх закладів // Актуальні питання гігієни та екологічної безпеки України. Збірка тез доповідей науково-практичної конференції (десяті марзєєвські читання). -2014.- Випуск 14. - С.193 – 195.

2). Булгаков Б.М., Шахбазов В.Г., Григорьева Н.Н. и соавт. Живая материя в электромагнитных полях техногенного происхождения / 13th Int. Crimean Conference “Microwave Telecommunication Technology”. 8-12 September, 2003, Sevastopol, Crimea, Ukraine // CriMiCo: IEEE Catalog Number 03EX697. - 2003 – P. 80 – 82.

3). Гудкова О.Ю., Гудков С.В. и соавт. Исследование механизмов образования активных форм кислорода в водных средах под действием импульсного электромагнитного излучения крайне высоких частот с большой пиковой мощностью // Биофизика. – 2005. – Т.50, Вып. 5. – С. 773 – 779.

4). Девятков Н.Д., Голанд М.Б., Бецкий О.В. Миллиметровые волны и их роль в процессах жизнедеятельности. – М.: Радио и связь, 1991.-168с.

5). Дідик Н.В., Томашевська Л.А. Вивчення впливу магнітного поля на біохімічні показники піддослідних тварин //Актуальні питання гігієни та екологічної безпеки України. Збірка тез доповідей науково-практичної конференції (десяті марзєєвські читання). -2014.- Випуск 14. - С.170 – 172.

6). Думанський В.Ю. Гігієнічна оцінка електромагнітного випромінювання, що створюється обладнанням стільникового мобільного зв’язку стандарту GSM – 900 // Гігієна населених місць. – К., 2004. – Вип. 43. – С. 233 – 241.

7). Емец Б.Г. О возможных причинах наблюдения «резонансного» действия электромагнитного излучения сверхвысоких частот на биообъекты // Вісник Харківського державного університету. - №410. – Біофізичний вісник. – 1998. – Вип. 1. – С.133-137.

8). Зуев В.Г., Ушаков И.Б. Микроволны и гематоэнцефалический барьер // Радиационная биология. Радиоэкология. – 1993. – Т.33, №5. – С. 739 – 747.

9). Мартынюк В.С., Темурьянц Н.А. Экспериментальная верификация электромагнитной гипотезы солнечно-биосферных связей // Ученые записки национального университета им. В.И. Вернадского.- Серия Биология, химия». – 2007. – Т. 20 (59). - №1. – С. 8 – 27.

10). Нікітіна Н.Г., Думанський Ю.Д. Електромагнітні поля як фактор впливу на здоров’я населення // Гигиена населенных мест: Сб. научн. тр. - К., 2001. – Вып. 38, Т.2. – С. 52 – 53.

11). Платонова А.Г., Яцковська Н.Я., Джурінська С.М. та ін. Психоемоційний стан школярів при роботі з портативними типами комп’ютерної техніки // Актуальні питання гігієни та екологічної безпеки України. Збірка тез доповідей науково-практичної конференції (десяті марзєєвські читання). -2014.- Випуск 14. - С.219 – 221.

12). Суворов И.М., Сушенцова Т.И. Клинические наблюдения за состоянием здоровья в зонах воздействия электромагнитных полей радиочастотного диапазона // Медицина труда и промышленная экология. – М., 2001. – №10. – С.43 – 46.

Василенко В.В.
Асистент каф. Інформаційних технологій
Бондаренко І.І.
Студентка факультету Інформаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

ТЕХНОЛОГІЯ SDN В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

SDN - Software-defined Networking SDN або програмно-конфігуруєма мережа.

SDN - це новий підхід до проектування, побудови та експлуатації мереж, який фокусується на наданні гнучкості за рахунок ефективного підключення користувачів до додатків. Він являє собою перехід від управління утворюючим мережі пристроями до управління цілими мережами.

Головна ідея SDN полягає у відділенні функцій передачі трафіку від функцій управління (включаючи контроль як самого трафіку, так і здійснюючих передачу пристроїв).

У традиційних комутаторах і маршрутизаторах ці процеси невід'ємні один від одного і реалізовані в одній «коробці»: спеціальні мікросхеми забезпечують пересилання пакетів з одного порту на інший, а вищерозміщене ПО визначає правила такої пересилки, виконує необхідний аналіз пакетів, виконує зміни які містять в них службової інформації.

Для визначення маршруту передачі або недопущення зациклення трафіку пристрої «спілкуються між собою», для чого розроблено безліч протоколів, таких як OSPF, BGP і Spanning Tree, але при цьому кожне функціонує досить автономно.

Згідно з концепцією SDN, вся логіка управління виноситься в так звані контролери, які здатні відстежувати роботу всієї мережі.

SDN має наступні ключові компоненти, а також переваги перед існуючими мережами:

Рівень управління мережним пристроєм відділений від його рівня передачі даних і логічно централізований в SDN-контролер, який забезпечує єдине абстрактне уявлення всієї мережі і її стану.

Зв'язок між мережевими пристроями і контролером SDN відбувається з використанням комунікаційних протоколів, які можуть бути відкритими, як OpenFlow, або пропрієтарними.

Контролер SDN підтримує відкритий інтерфейс програмування (API), який дозволяє програмувати його ззовні, створюючи таким чином середовище для автоматизації, контролю, а також масштабувати функціонал для майбутніх додатків. Це дає можливість застосування підходу SDN як у великих компаніях і телекомах, так і малому та середньому бізнесі.

SDN є відносно новим як поняття, але переваги вже очевидні - замовники можуть стати менш залежні від дорогих пропрієтарних мережевих комутаторів і маршрутизаторів, оскільки SDN може бути налаштована на менш дорогому обладнанні. Однак головна перевага в управлінні та гнучкості.

Враховуючи новизну технології, очевидно, що тестові і повноцінно реалізовані проекти в Україні поки одиничні, однак перспективи позитивні. І це тільки питання часу. Сьогодні у всьому світі величезний інтерес до технології SDN проявляють в першу чергу наукова сфера і провайдери хмарних послуг.

Література:

1.Барсков А. SDN: кому и зачем это надо / А. Барсков // Журнал сетевых решений LAN. — 2012. — No. 12. — С. 13–19.

2.Смелянский Р.Л. Программно-конфигурируемые сети / Р.Л. Смелянский // Открытые системы. СУБД. — 2012. — No. 9. — С. 23–26.

Сергієнко І.-В.О.
Аспірант каф. Телекомунікаційних технологій
Державний університет телекомунікацій
м. Київ, Україна

РОЗРАХУНОК ОПТИЧНИХ ХАРАКТЕРИСТИК КОМПОНЕНТНОГО КВАРЦОВОГО СКЛА В ДІАПАЗОНІ ДОВЖИН ХВИЛЬ ВОЛОКОННО-ОПТИЧНОГО ЗВ'ЯЗКУ

У виробництві оптичних компонентів волоконно-оптичних систем передачі (ВОСП) використовують високоякісні стекла на базі плавленого кварцу (хімічна формула SiO_2), леговані різними речовинами, наприклад окису бору (B_2O_3), окису германію (GeO_2), фосфорного ангідриду (P_2O_5), фтору (F) тощо. Германій чи фосфор підвищують величину n показника заломлення скла, а фтор чи бор – знижують. Для конструювання волоконно-оптичних компонентів ВОСП з покращеними оптичними характеристиками (оптичне волокно лінійного тракту, волоконні компенсатори хроматичної дисперсії, оптичні підсилювачі тощо) потрібно знати спектральну залежність $n=n(\omega)$ показника заломлення (ПЗ) в компонентному кварцовому склі, яка визначає дисперсію середовища при розповсюдженні в ньому електромагнітних хвиль.

Експериментальні результати з вимірювання спектральної залежності $n(\lambda)$ показника заломлення в об'ємних зразках компонентного кварцового скла з високою точністю апроксимуються тричленною формулою Селмейєра, [1]:

$$n^2 - 1 = \sum_{j=1}^{3} \frac{A_j \lambda^2}{\lambda^2 - l_j^2}, \qquad (1)$$

де $\lambda=2\pi c/\omega$ – довжина електромагнітної хвилі у вакуумі;

A_j та l_j – постійні для даного діелектрика коефіцієнти Селмейєра, які знаходяться підгонкою заміряних значень ПЗ в об'ємному зразку скла.

Розглянемо окремий випадок компонентного кварцового скла з використанням суміші лише двох компонентів (у найпоширеніших випадках це $SiO_2 + GeO_2$ чи SiO_2 + F). Через більшу концентрацію домішки B_2O_3, порівняно з випадком домішки F, значно підвищуються втрати енергії на поглинання та Релеєві розсіяння поширюваних в компонентному кварцовому склі електромагнітних хвиль, що є однією з причин застосування переважно домішки фтору для зниження показника заломлення кварцу SiO_2.

Таблиця 1 містить значення коефіцієнтів Селмейєра, знайдені в результаті вимірювання показника заломлення в об'ємних зразках із компонентного скла на базі плавленого кварцу (SiO_2). Значення взято із монографії [1], в якій відповідна таблиця містить не чотири, а значно більше позицій.

Табл. 1 Значення коефіцієнтів Селмейєра в залежності від концентрації легувальної домішки до кварцу SiO_2, визначені вимірюванням ПЗ в об’ємних зразках компонентного скла

№пп	Домішки, в молярн%	A_1	A_2	A_3	l_1, мкм	l_2, мкм	l_3, мкм
1	100% SiO_2	0,6961663	0,4079426	0,8974794	0,0684043	0,1162414	9,896161
2	3,1% GeO_2	0,7028554	0,4146307	0,8974540	0,0727723	0,1143085	9,8961615
3	7,9% GeO_2	0,7136824	0,4254807	0,8964226	0,0617167	0,1270814	9,896161
4	1% F	0,691116	0,399166	0,890423	0,068227	0,116460	9,993707

Після диференціювання по λ обох частин формули (1) отримаємо вираз для групового показника заломлення діелектрика

$$n_{гр}(\lambda)=\frac{v_{гр}(\lambda)}{c}=n-\lambda\frac{dn}{d\lambda}=n+\frac{\lambda^2}{n}\sum_{i=1}^{3}\frac{A_i l_i^2}{(\lambda^2-l_i^2)^2}\,, \qquad (2)$$

де $v_{гр}(\lambda)$ – групова швидкість хвильового пакету на центральній довжині хвилі.

Для розрахунку за формулою (1) спектральної залежності ПЗ в компонентному кварцовому склі потрібно знати коефіцієнти Селмейєра за довільної концентрації легуючих домішок.

Одним із способів знаходження наближених значень коефіцієнтів Селмейєра як функцій величини С концентрації домішки, $A_j(C)$, $l_j(C)$, може бути використання інтерполяційних многочленів. За вузлові точки інтерполяції беруться визначені вимірюванням ПЗ в об’ємних зразках компонентного скла значення коефіцієнтів за окремих концентрацій обраної домішки, [1]. Проведений числовий аналіз показав, що інтерполяція коефіцієнтів Селмейєра за їхніми відомими величинами для трьох окремих значень концентрацій домішки GeO_2 (три вузлові точки для кожного з 6-ти коефіцієнтів, з урахуванням чистого плавленого кварцу, а саме: 0% GeO_2, 3,1% GeO_2 та 7,9% GeO_2, – див. табл. 1), уможливлює достатню точність розрахунку за формулами (1), (2) дисперсійних характеристик компонентного скла на базі плавленого кварцу, легованого домішкою GeO_2. У діапазоні довжин хвиль ~0,82…1,65 мкм вірними виявились: 4-та – 5-та значуща цифра величин n і $n_{гр}$.

Що стосується кварцового скла з домішкою фтору, то коректною є лінійна інтерполяція коефіцієнтів Селмейєра, з використанням їхніх значень, отриманих експериментально у випадках (див. табл. 1): 1% мольної концентрації домішки F; 0% F (чистий кварц).

Література:

1. Adams M.J. An Introduction to Optical Waveguides. – Chichester, John Wiley, 1981. – 507 p.

Штонда Р.М.
С.н.с. науково-дослідної лабораторії
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації
Бабич І.В.
Начальник служби захисту інформації
Київський обласний військовий комісаріат
м. Київ, Україна

ПРИХОВУВАННЯ ПЕРЕДАЧІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЗА ДОПОМОГОЮ ДИСКРЕТНО-КОСИНУСНОГО ПЕРЕТВОРЕННЯ

Визначення проблеми. Задача захисту інформації від несанкціонованого доступу вирішується та актуальна на протязі всього часу існування людства. Сформованими є два основних напрямки рішення цієї задачі: криптографія та стеганографія. Ціллю криптографії є захист інформації методом її шифрування. У відмінності від цього, при стеганографічному захисті інформації, приховується сам факт існування таємного повідомлення.

Аналіз публікацій за напрямком дослідження. У розвиток стеганографії значний внесок зробили вчені Коханович Г.Ф. [1 с. 288], Задірака В.К. [2 с. 801], Лукічов В.В. [3] та інші. Актуальним та перспективним напрямком є дослідження дискретно-косинусних перетворень зображень в зв'язку з надійними показниками робастності та таємності вбудовування даних та розповсюдженням форматів зображень.

Формулювання мети доповіді. Описати приховування передачі інформації в комп'ютерних мережах спеціального призначення за допомогою дискретно-косинусного перетворення.

Результат дослідження. Загальновідомо, криптографія має на меті шифрування інформації, в результаті чого закрите повідомлення не доступне для осіб, що не володіють секретним ключем. Стеганографія приховує сам факт наявності повідомлення, яке певним чином вбудовується в деякий об'єкт і передається адресату, таким чином наявність прихованого зв'язку між адресатами залишається непомітною. На сьогоднішній день розроблена значна кількість методів (алгоритмів) стеганографічного захисту інформації. Аналіз вимог до стеганографічних методів (алгоритмів) показав, що жоден з них не володіє ідеальними показниками, їхня ефективність безпосередньо залежить від конкретних умов використання. Комп'ютерна стеганографія ґрунтується на вбудовуванні повідомлення в цифрові дані, найбільш популярними є методи приховування інформації в зображеннях.

Проаналізувавши всі види зовнішніх опрацювань зображення, можна зробити висновок, що найбезпечнішим з них є JPEG-стиснення. Алгоритм JPEG реалізує стиснення з втратами (ґрунтується на дискретно-косинусному перетворенні (ДКП) або вейвлет-перетворенні) та найчастіше застосовується у інформаційно-телекомунікаційних системах для зменшення об'єму зображень.

Більшість несанкціонованих змін зображень зводиться до заміщення деякої його області в область іншого цифрового зображення. Після заміщення отримане зображення зберігається знову у форматі JPEG або іншому без втрат інформації. Основна ідея ДКП полягає в приховувані інформації в коефіцієнтах ДКП [4 с. 76], вбудовування 1 біта повідомлення в блок розміром 8х8 здійснюється наступним чином: для передачі біта 0 необхідно щоб різниця абсолютних значень коефіцієнтів була більшою величини ε, а для передачі біта 1 ця різниця робиться меншою величини – ε (1):

$$\begin{aligned} &\left|c_b(j_{i,j}, k_{i,1}\right| - \left|c_b(j_{i,2}, k_{i,2}\right| > \varepsilon, \quad \text{якщо } S_i = 0, \\ &\left|c_b(j_{i,j}, k_{i,1}\right| - \left|c_b(j_{i,2}, k_{i,2}\right| < -\varepsilon, \quad \text{якщо } S_i = 1. \end{aligned} \tag{1}$$

Таким чином, зображення спотворюється за рахунок впроваджених змін в коефіцієнти ДКП, щоб переглянути повідомлення в декодері проводиться та ж операція вибору коефіцієнтів. Рішення про переданий біт приймається відповідно до правила (2):

$$\begin{aligned} &S_i = 0, \quad \text{якщо}\left|c_b(j_{i,j}, k_{i,1}\right| > \left|c_b(j_{i,2}, k_{i,2}\right|, \\ &S_i = 1, \quad \text{якщо}\left|c_b(j_{i,j}, k_{i,1}\right| < \left|c_b(j_{i,2}, k_{i,2}\right|. \end{aligned} \tag{2}$$

Загалом, існуючі методи стеганографічного захисту інформації переважно розраховані на приховування інформації без урахування особливостей спотворення зображення. За допомогою ДКП відбувається спотворення зображення в JPEG файлі, що забезпечує високу робастність та таємність повідомлення. Однозначно, вибір алгоритму реалізації для конкретних умов застосування є балансуванням між робастністю, таємністю повідомлення (забезпеченням непомітності) та максимально можливим їх об’ємом.

Висновки з дослідження. Подальші дослідження потрібно спрямувати на розробку засобів стеганографічного захисту інформації, які були б придатні для практичного використання в інтересах силових структур, в тому числі, і з використанням каналів противника. Під час розробки слід враховувати гриф обмеження доступу до інформації, архітектуру мережі, реалізацію мережевих з’єднань, використання мережевих протоколів та умови застосування мережі в цілому.

Література:

1. Коханович Г.Ф. Компьютерная стеганография. Теория и практика/ Г.Ф.Коханович, А.Ю.Пузыренко // МК-Пресс. 2006. – С. 288.

2. Задірака В.К. Аналіз стійкості стеганографічних систем в моделі пассивного противника / В.К. Задірака, Н.В.Кошкіна, О.С.Олексюк// Искусственный интеллект. 2004. - № 3. – С. 801 – 805.

3. Лукічок В.В. Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень / В.В.Лукічок, В.А.Лужецький, А.С.Васюра// ВНТУ. 2014.

4. Кох І. Цифрові водяні знаки і стеганографія / І.Кох, Д.Блум, Д.Фрідріх// Морган Кауфман. 2008. – С. 67 – 72.

Кротов В.Д.
Провідний науковий співробітник науково-дослідного відділу
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації
м. Київ, Україна

ПОРІВНЯЛЬНА ОЦІНКА АЛГОРИТМІВ (PID-, PI-IRED-РЕГУЛЯТОРІВ) ДЛЯ AQM-СИСТЕМ ПРИ ЗМІННИХ ПАРАМЕТРІВ TCP/IP МЕРЕЖ

Визначення проблеми.Для сучасних телекомунікаційних систем з комутацією пакетів характерне явище перевантаження, для боротьби з яким використовують різні методи. Серед них важливе місце займають методи управління чергою пакетів в маршрутизаторах. Існує два види управління чергою: активне і пасивне. При пасивному управлінні відбувається відкидання пакетів, які приходять у той час, коли у відповідній канальної черзі відсутні вільні місця. Це метод відкидання хвоста (TailDrop), який простий у реалізації, але має ряд істотних недоліків, з якими успішно справляються методи активного управління чергою - ActiveQueueManagement (AQM). Типовим прикладом AQM-систем є системи с PID-регулятором (proportional-integral-derivative), PI-регулятором (proportional-integral) і RED-регулятором (randomearlydetection) [0-**Ошибка! Источник ссылки не найден.**]. При використанні PID, PI і RED алгоритмів надходять у буфер пакети випадково відкидаються (маркуються) з ймовірністю, яка залежить від довжини черги.

Аналіз публікацій за напрямком дослідження. Темі присвячено досить багато досліджень,так у роботах [0-**Ошибка! Источник ссылки не найден.**] описані і проаналізовані лінеаризовані системи AQM з цими алгоритмами як системи автоматичного управління. Ці системи описані передавальними функціями з постійними параметрами, хоча реальні AQM системи є системами з випадковими, стохастичними параметрами..

Формулювання мети доповіді. Враховуючи це, метою доповіді є дослідження AQM системи з PID, PI і RED регуляторами як системи із змінними параметрами при випадковій зміні навантаження трафіку (випадковій зміні числа сесій TCP) і випадковій зміні часу проходження туди і назад (roundtriptime RTT) на основі інтерактивної системи MATLAB [0-0].

Результат дослідження.С початку розглянемоблок-схему системи активного управління чергою ActiveQueueManagement зі зворотним зв'язком і AQM законами управління (PID, PI і RED регуляторами), докладний опис якої розглянуто в роботах [0-**Ошибка! Источник ссылки не найден.**]. Динаміка об'єкта описується передатною функцією, яка являє собою відношення по Лапласу змінної "довжини черги" до змінної "ймовірності відкидання/маркування пакету" і визначена в роботах [0-**Ошибка! Источник ссылки не найден.**] для сталого режиму як:

$$G(s) = \frac{\delta q(s)}{\delta p(s)} = P(s)e^{-sR_0} = \frac{\frac{C^2}{2N}e^{-sR_0}}{(s + \frac{2N}{R_0^2 C})(s + \frac{1}{R_0})}, \qquad (1)$$

де C- ємністьзв'язку (пакети/сек), $R_0 = \frac{q}{C} + T_p$ - час слідуваннятуди і назад – roundtriptime RTT(у сек), T_p - затримка розповсюдження (у сек), N - коефіцієнт навантаження (кількість TCP сесій).

Передавальну функціюланкизапізнюваннязазвичайапоксиміруютьза допомогою функціїПаде. Для наближенняПадедругого порядкуможна записати:

$$e^{-sR_0} \approx \frac{s^2 - \frac{6}{R_0}s + \frac{12}{R_0^2}}{s^2 + \frac{6}{R_0}s + \frac{12}{R_0^2}} \qquad (2)$$

З урахуванням (2) передавальну функцію об'єкта управління (1) можна записати у вигляді:

$$G(s) = P(s)e^{-sR_0} = \frac{\frac{C^2}{2N}(s^2 - \frac{6}{R_0}s + \frac{12}{R_0^2})}{(s + \frac{2N}{R_0^2 C})(s + \frac{1}{R_0})(s^2 + \frac{6}{R_0}s + \frac{12}{R_0^2})}. \qquad (3)$$

Лінійна модель, з передавальної функцією, яка описана рівнянням (3), відрізняється від реальної моделі мережі наступним [0]:

1. Модель розглядає тільки TCP-потоки і ігнорує інші види потоків. Фактично, Інтернет - суміш різних потоків. Деякі джерела використовують механізми управління перевантаженнями як TCP, в той час як деякі відео додатки приймають постійну швидкість передачі бітів (CBR), яка байдужа до перевантажень. Далі, різні версії виконання TCP, такі як TCP Reno, TCP New-Reno, TCP Vegas і т.д., буде співіснувати в Інтернеті. Фактично, модель точно описує механізм управління перевантаженнями TCP Reno в сталому режимі роботи при постійних параметрах ємності зв'язку C, часу проходження туди і назад R_0 і коефіцієнті навантаження N.

2. Модель описує адитивне збільшення і мультиплікативне зменшення (AIMD) поведінки TCP, в той час як ігнорує стан "повільного старту" (slowstart) і перерву. Хоча модель точна у більшості умов, тому що запобігання перевантажень - первинний операційний стан TCP, спеціально для тривалих передач, таких як FTP-потоки, але у випадку нетривалих потоків таких, як Telnet або Web, часто трапляються стан повільного старту та перерва.

3. Основна відмінність моделі від реальної моделі мережі полягає у тому, що кількість активних сесій TCP (N) і час слідування туди і назад (RTT) в моделі прийняті постійними. Однак ці параметри є у високому ступені змінними в мережі.

Нижче досліджені AQM системи з PID, PI і RED регуляторами як системи із змінними параметрами при випадковій зміні навантаження трафіку (випадковій зміні числа сесій TCP і випадковій зміні часу проходження туди і назад) на основі інтерактивної системи MATLAB.

В інтерактивній системі MATLAB можна представити модель об'єкта управління з'єднанням ланок з мінливими випадковим чином параметрами $N(t)$ і $R_0(t)$. Відзначимо, що при налаштуванні цифрових PID-регулятора і RED-регулятора в інтерактивній системі MATLAB можна використовувати блок NCD (NonlinearControlDesign), який реалізує метод динамічної оптимізації для проектування систем управління. Цей інструмент, розроблений для використання з Simulink, автоматично налаштовує системні параметри, ґрунтуючись на певних обмеженнях на тимчасові характеристики (наприклад, час регулювання та перерегулювання для реакції на поетапний вплив) або межі для динамічної помилки неузгодженості.

Припустимо, що час слідування туди і назад $R_0(t)$змінюється випадковим чином в межах від 220 мсек до 300 мсек, а навантаження трафіку $N(t)$ змінюється також випадковим чином в межах від 40 до 80. Такі "впливи" на систему, можуть генерувати в інтерактивній системі MATLAB блоки UniformRandomNumber. Відзначимо, що в реальних мережах і час слідування туди і назад, і навантаження трафіку може змінюватися випадковим чином у різних межах, але для порівняння роботи розглянутих регуляторів обрані однакові "впливи".

Порівнюючи процеси вдосліджуваних системахможна укласти, що AQM система, яка скоригована RED-регулятором, має більш гірші характеристикипо точностіта швидкодії, ніж системи, які скориговані PIDiPIрегуляторами. Поточнадовжина черги повторює задану довжину черги (бажане значення черги) з великою помилкою і перехідний процессистеми,скоригованої RED-регулятором, займає майже50сек.

Література:

1.Дорф Р., Бишоп Р. Современныесистемыуправления/ Пер. с англ. - М.: ЛабораторияБазовых Знаний, 2002.- 832 с.

2.Дьяконов В.П. MATLAB 6/6.1/6.5+Simulink 4/5 в математике и моделировании. Полноеруководствопользователя. М.: СОЛОН-Пресс. – 2003. – 576 с.

3.Дьяконов В., Круглов В. Математические пакеты расширения MATLAB. Специальный справочник. - СПб.:Питер, 2001. - 480 с.

4.Куо Б. Теория и проектированиецифровых систем управления. - М.: Машиностроение, 1986. - 448с.

5.Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzy TECH.- СПб.: БХВ-Петербург, 2003.- 736 с.

6.Heying Z., Baohong L., andWenhua D. “Designof a robustactivequeuemanagementalgorithmbasedonfeedbackcompensation”. ProceedingsofACM/SIGCOMM’2003, pp. 277-285.

7.Hollot C.V., Misra V., Towsley D., Gong W.B. “A ControlTheoreticAnalysisof RED,” in Proceedingsof IEEE/INFOCOM, April, 2001, pp. 1510-1519.

8.Hollot C.V., Misra V., Towsley D., Gong W.B. “Analysisanddesignofcontrollersfor AQM routerssupporting TCP flows”. IEEE/ACM TransactionsonAutomaticControl, vol. 47, no.6, pp. 945-959, June 2002.

9.Hollot C.V., Misra V., Towsley D., Gong W.B., “OnDesigningImprovedControllersforRoutersSupporting TCP Flows”, inProceedingsof IEEE INFOCOM’2001, April 2001, 1726-1734.

Поліщук Ю.Я.
Студентка каф. БІТ
Національного авіаційного університету
м. Київ, Україна

МЕДІАВІРУС ЯК ОСНОВНА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА ЗБРОЯ В УМОВАХ ІНФОРМАТИЗАЦІЇ

XX, сторіччязарекламувало себе появою нової зброї. Мова йде про так звану інформаційну зброю. І, якщо розглядати минуле сторіччя як початок розробки новітньої зброї, то XXI століття можна сміливо назвати його піком, адже сьогодні методи впливу на людську свідомість стали різноманітнішими і дієвішими за рахунок створення спеціальних технологій спілкування між людьми.

Одним із таких методів є медіавірус. Медіавірус (англ. mediavirus) - термін, введений американським фахівцем в галузі засобів масової інформації Д.Рашкоффом для позначення медіаподії, що викликають прямо або побічно певні зміни в житті суспільства[1, с. 156]. На думку Д. Рашкоффа, разом з розвитком технологій засобів масової інформації у світовій культурі з'явилося ціле покоління «ікс», яке виросло в тісному контакті з мас-медіа, вільно знайоме з інформаційними технологіями і по-справжньому функціонує в світовому «ефірі» (який Рашкофф вважає синонімом «медіа») - інфосфері, або «медіапросторі» (англ. mediasphere), прообраз віртуальної реальності. Окремі представники цього покоління, що володіють розумінням психології, соціології, маркетингу, знайомі з прийомами нейролінгвістичного програмування та психології впливу, створюють організовані групи, метою яких ставиться проведення «медіадиверсій», здатних підірвати карту реальності, створювану ЗМІ, - найчастіше спрощену модель світу. І якщо раніше «медіапростір» більшістю людей сприймалося як медіум, посередник, інформуючий людей про реальність, то зараз все більше людей ставиться до інфосфери, як до окремого феномену, існуючому за своїми законами.

Сьогодні однією зі сфер розповсюдження медіавірусів є Інтернет. Деякі дослідники дотримуються гіпотези, що Інтернет може в недалекому майбутньому служити плацдармом для революцій.

Можна виділити три види медіавірусів:

Навмисно створені медіавіруси. Свідомо кимось запускаються, щоб сприяти поширенню будь-якого товару чи ідеології. Прикладами таких вірусів є акції медіаактивістів та рекламні трюки (наприклад, піар).

«Кооптовані» віруси, або «віруси-тягачі», які можуть виникнути спонтанно, але миттєво утилізовані зацікавленими групами з метою поширення власних концепцій. Приклади включають скандал навколо В.Аллена і М. Ферроу (використовувався республіканцями для критики концепцій демократів), епідемію СНІДу (була використана консерваторами для звинувачення гомосексуалістів) та ін.

Повністю самозароджуючі віруси - медіавіруси, що викликають інтерес і поширюються самі по собі. Прикладами можуть служити нові технології або наукові відкриття.

Варто пам'ятати, що медіавіруси породжують нові питання і ніколи не дають готові відповіді. Найпростіший спосіб відрізнити медіавірус від іншого роду трюків засобів масової комунікації - це визначити, спрощує він питання, дає на нього відповідь, або ж, навпаки, робить його надзвичайно складним і ускладнює його розуміння. Вірус завжди змушує соціальну систему або систему поглядів, на які нападає, виглядати заплутаною і незбагненною для людини, якою вона і є насправді [2, с. 53].

Люди живуть в інформаційному полі і щодня черпають інформацію з преси, радіопередач, з екранів телевізорів. Перебуваючи часто в світі відірваних від реальності символів, вони можуть йти навіть проти своїх власних інтересів. Реальність може відходити на другий план, грати підлеглу роль. У цьому сенсі людина не є вільним, тим більше, що відпрацьовано ряд способів ефективного інформаційного впливу. Для них існує термін «брейн уошінг» («Brainwashing») - промивання мізків. За допомогою «Brainwashing» може здійснюватися зомбування людей, створення пасивного слухняного людини, перетворення народу в легко керовану масу[3, с. 94].

Засоби масової комунікації формують «масову» людину нашого часу. У той же час вони роз'єднують людей, витісняють традиційні безпосередні контакти, замінюючи їх телебаченням і комп'ютерами.

День сьогоднішній, з його телекомунікаційними обчислювальними системами, психотехнологіями кардинально змінив навколишній простір. Окремі інформаційні струмочки перетворилися на суцільний потік. Якщо раніше влада мала можливість регулювати інформаційні потоки, то сьогодні, з розвитком засобів масової комунікації це стає практично неможливим. Час на інформаційну взаємодію між найвіддаленішими точками наблизилося до нуля. У результаті проблема захисту інформації, яка раніше була як ніколи актуальна, перекинулася подібно монеті, що викликало до життя її протилежність - захист від інформації.Завдання медіавірусів полягає не в знищенні живої сили, але в підриві цілей, поглядів і світогляду населення, в руйнуванні соціуму.

Одним із серйозних переваг інформаційної зброї - відносна дешевизна в порівнянні з іншим видом озброєння. За критерієм ефективність / вартість воно значно виграє у будь-якого іншого виду зброї.

Це відбувається, тому що в нього не треба вкладати «енергію» для знищення супротивника. Спочатку передбачається, що противник володіє всіма необхідними засобами для власного знищення. Завдання застосування інформаційної зброї полягає в тому, щоб допомогти противнику направити наявні у нього кошти, в тому числі технічні, проти самого себе.

Аналізуючи вищесказане, можна зробити висновок, що в епоху інформатизації, коли соціальне середовище перенасичена інформацією і напряму залежить від її подання, безпека системи вже починає визначатися не тільки тими знаннями, які ця система отримує про противника, а й, може бути тими знаннями, від сприйняття яких їй вдалося ухилитися.

Якби головним завданням цієї зброї було знищення аналогічного зброї противника, зіткнення в будь-якій області стало б початком битви, що поширюється, як степова пожежа, що призвело б до глобального обміну ударами найвищої потужності, а отже, до загибелі. Тому зброя не повинна вступати між собою в безпосередні зіткнення, воно повинна тільки взаємно чередуватися, а якщо і знищувати, то підступно, як мікроби, а не як бомби.

Література:

1.Рашкофф Д. Медиавирус! Тайныепослания в популярнойкультуре. – М.: Ультра. Культура, 2003. – 368 с.

2.Манойло А.В., Петренко А.И. Информационно-психологическая безопасность современного информационного общества // Стратегическаястабильность. – 2003. - №3.

3.Прокофьев В.Ф. Тайное оружие информационной войны. - М., Эксмо, 2009.

Одарченко Р.С.

Доцент каф. Телекомунікаційних систем, заступник директора Навчально-наукового Інституту аеронавігації

Поліщук В.В.

Магістрант

Національний авіаційний університет

М. Київ, Україна

ДОСЛІДЖЕННЯ ПЕРЕВАГ ТА НЕДОЛІКІВ КОНЦЕПЦІЇ SDN

Сьогодні комп’ютерні мережі (КМ) є необхідною частиною будь-якого підприємства, навчального закладу, державної організації тощо. Сучасні КМ не позбавлені недоліків, таких як: складність управління мережею, висока вартість мережевого обладнання, недостатньо ефективне використання каналу зв’язку через передавання великої кількості інформації для керування мережею замість корисного трафіку тощо. Тому з’явився принципово новий клас мереж. Програмно-конфігурована мережа (SDN – Software-DefinedNetworking) сьогодні є однією з найперспективніших технологій у галузі комп’ютерних мереж [1]. Модель SDN має ряд переваг над традиційними мережами, серед яких розробники виділяють наступні: підвищення ефективності мережевого обладнання на 25-30%; зниження на 30% витрат на експлуатацію мереж; надання користувачам можливості програмно створювати нові сервіси і оперативно завантажувати їх в мережеве обладнання [2]. Така концепція побудови комп'ютерної мережі надає цілий ряд можливостей, більшість яких неможливо реалізувати при використанні традиційноїархітектури. Далі проведено аналіз основних можливостей, які надає концепція програмно-конфігурованих мереж [2].

1. Централізоване управління ресурсами мережі.
2. Уніфікація управління.
3. Програмування додатків API.
4. Розширення можливостей обладнання.
5. Маршрутизація в SDN. Підвищення швидкості передачі.
6. Віртуальні мережі SDN.
7. Засоби безпеки.
8. Динамічна переконфігурація.
9. Можливість проводити будь-які експерименти на окремій віртуальній мережі, використовуючи обладнання, що обслуговує основну мережу, не порушуючи її роботу.
10. Можливість організації нових послуг, оскільки знімаються фізичні обмеження, що накладаються обмеженим числом виробників обладнання.

Проте не зважаючи на свої численні переваги, архітектура SDN має також свої недоліки[3]. Для ефективного впровадження SDN-мережі необхідно розуміти її слабкі сторони, щоб розробити методи їх усунення. Дослідження основних недоліків концепції наведено далі.

1) Проблеми, пов'язані з недолікамитехнології:

- Зупинкароботимережі при виході з ладу контролера.
- Можливістьпомилки при програмуваннідодатків.
- Затримка при отриманніінформації контролером про вихід з ладу чизавантаженість каналу.
- Складністьпобудовимережі, щомаєбільше одного власника через неможливістьділитиміж собою функції одного контролера.

2) Проблеми, пов'язані з новизноютехнології.

Вихід з ладу контролера. Найочевидніший недолік SDN витікає з її централізованості – при виході з ладу контролера зупиниться вся мережа. Це може бути спричинено зовнішнім втручанням (адже контролер буде найуразливішою точкою мережі і може стати ціллю направлених атак) або внутрішніми несправностями (фізичними пошкодженнями, браком обладнання).

Цю проблему можнавирішити наступним чином:

1. Резервуванням контролера. Запасний контролер маєпостійнопрацювати у «холостому» режимі для можливостізаміни основного контролера.Іншийваріант, якщофункціональність буде поділенаміж контролерами. Якщоконтролерирознесенігеографічно, то кожний з них відповідатиме за ту частинумережі, затримкадоякої є найменшою. При цьомукожен з контролерівмає бути готовийприйняти всю функціональність на себе у випадкузбою.

2. Побудовоюгібридноїмережі «SDN + традиційна мережа». Тоді у разівиходу з ладу центральногоелементууправління, комутаторипереходять в автономний режим обчисленнямаршрутів і починаютьпрацювати за старою технологією – хоч і повільніше, але без розривуз'єднання.

3. Застосуваннямновихпрограмнихзасобівбезпеки, щозахищають контролер відзовнішніх атак. Приклади таких засобівнаведенівище.

4. Комбінацієюцихметодів.

Помилка в програмуваннідодатків API. Помилка в програмуванні контролера можепризвести до серйозних проблем на всіймережі, яку вінобслуговує. Приклад: декількаодночаснопрацюючихпрограмбудутьконкурувати за мережевіресурси, при великому навантаженніможевиникнутиситуація, коли одна програмамонополізуєїх, через щоіншідодаткиперестанутьфункціонувати.

Можливівирішення:

- Використаннялишеперевіренихдодатків та їхкомбінацій.
- Проведеннятестуванняновихпрограмнавіртуальніймережі перед введеннямїх до експлуатації.

Затримка при отриманні інформації контролером про вихід з ладу чи завантаженість каналу. Протокол IP орієнтований на те, щоб маршрутизатори самостійно стежили за завантаженням і працездатністю пов'язаних з пристроєм каналів, а в SDN за станом мережі стежить контролер, який отримує дані про вихід з ладу каналів і їх завантаженості «зі сторони», тобто є затримка в отриманні інформації та прийнятті рішення. Це не сприяє збільшенню надійності.

Складність побудови мережі, щомаєбільше одного власника через неможливість ділити між собою функції одного контролера. Два оператори не зможутьділитиміж собою функції одного контролера, тому надійнупрограмно-конфігуровану мережу можна побудувати тільки, якщо вся мережа має одного власника. Зазначимо, що складність виникає лише у випадку використання одного логічного контролера.

Можливимви рішенням є віртуалізація та ізоляція трафіку двох провайдерів на рівніVLAN’ів. Така мережа, однак є більш складною для управління та налагодження, через необхідність застосування алгоритмів для такого розподілу мережевих ресурсів, щозадовольнить потреби обохоператорів ISP.

Нетехнологічніпроблеми:

- Необхідність перебудови існуючих мереж.
- Необхідність перекваліфікації адміністраторів мереж.
- Малакількість «чистих» Open Flow-комутаторів на ринку. Здебільшого, Open Flow присутній у мережевому обладнанні лише як додаткова функціональність. Це призводить до удорожчання обладнання, аотже на впровадженняпрограмно-конфігурованої мережі необхідні більші грошові витрати.
- Невелика кількість програм для контролера з відкритим програмним кодом.

Всі ці проблеми будуть усунені з часом, хочакомпанії з великими фінансовими можливостями та кваліфікованими спеціалістами вже зараз можуть вирішитиїх.

Таким чином, в роботібуло проведено аналізархітектури SDN. Були встановлені відмінності від традиційних мереж, проведено аналіз можливостей, які надає даний підхід до реалізації комп'ютерних мереж, було також досліджено недоліки SDN-мереж.

Також була обґрунтована перспективність впровадження мереж SDN, спираючись як на технологічний, так і на фінансовий аспекти розвитку технології. Перспективність впровадження таких мереж доводить актуальність теми дослідження.

В результаті проведених досліджень були встановлені недоліки концепції SDN, а отже існує можливість і необхідність оптимізації SDN-мереж для провайдерів ISP. Тому в подальших наукових дослідженнях планується вирішення наведенихвище проблем.

Література:

1. Смелянский Р. Программно-конфигурируемые сети / Руслан Смелянский // Открытыесистемы. – 2012. – № 09.
2. SDN и другие / Сергей Орлов // Журнал сетевыхрешений/LAN. – 2014. – № 06.
3. Черняк Л. SDN – от замысла до рынка / Леонид Черняк // Открытыесистемы. – 2012. – № 09.
6. Детскиеболезни SDN / ВалерийКоржов // Открытыесистемы. – 2013. – № 06.

Креденцар С.М.
К.т.н, доцент каф. Аеронавігаційних систем
Національний авіаційний університет
м. Київ, Україна

СТВОРЕННЯ ЦИФРОВОЇ КАРТИ НИЖНЬОГО ПОВІТРЯНОГО ПРОСТОРУ УКРАЇНІ

Бурхливий розвиток інформаційних технологій та їх використання в авіації викликає необхідність викорстання спеціальних програмних засобів обробки оперативної аеронавігаційної інформації. Геоінформаційні технології успішно використовуються для моделювання повітряного простору, планування повітряного руху, а також для дизайну маршрутів повітряного простору в реальному часі, що дає змогу приймати більш точні, надійні та безпечні рішення щодо керування повітряним простором.

Актуальність створення цифрових аеронавігаційних карт обумовлена необхідністю сучасних аеронавігаційних систем найбільш детально відображати аеронавігаційну інформацію. Відповідно до вимог ICAO сучасні аеронавігаційні системи повинні мати геоінформаційну складову, просторову інформацію у вигляді цифрової карти.

В роботі побудована цифрова карта нижнього повітряного простору України на базі ГІС MapInfo, представляє собою базу аеронавігаційних атрибутивних даних та векторне відображення цих даних у вигляді умовних позначень [1, с.24, с.128, 2, с.64].

Створена цифрова карта складається з 10 прошарків, що включають:

Кордони 24 адміністративних областей України.

Кордони районів польотної інформації на території України – 5 районів (FlightInformationRegion – FIR).

Кордони небезпечних зон – 7 зон (DangerousArea).

Кордони зон обмеження польотів – 29 зон (ProhibitedArea).

Кордони заборонених зон – 188 зон (RestrictedArea). Позначення всіх аеропортів та аеродромів Україні - 62 летовища на території України.

Відмітки основних польотних маршрутів - 370 маршрутів, що з'єднують важливі точки для аеронавігації.

Точки обов'язкового донесення аеронавігаційної інформації - 124 точки.

Точки необов'язкового донесення аеронавігаційної інформації - 76 точок.

Розміщення ненаправлених радіомаяків (Non-directionalradiobeacons) –33 ненаправлених радіомаяки (Non-directionalradiobeacons).

Розміщення сумісних VOR/DME аеронавігаційних засобів - 7 сумісних VOR/DME.

Загальний вигляд карти нижнього повітряного простору території України наведена нижче (рис. 1).

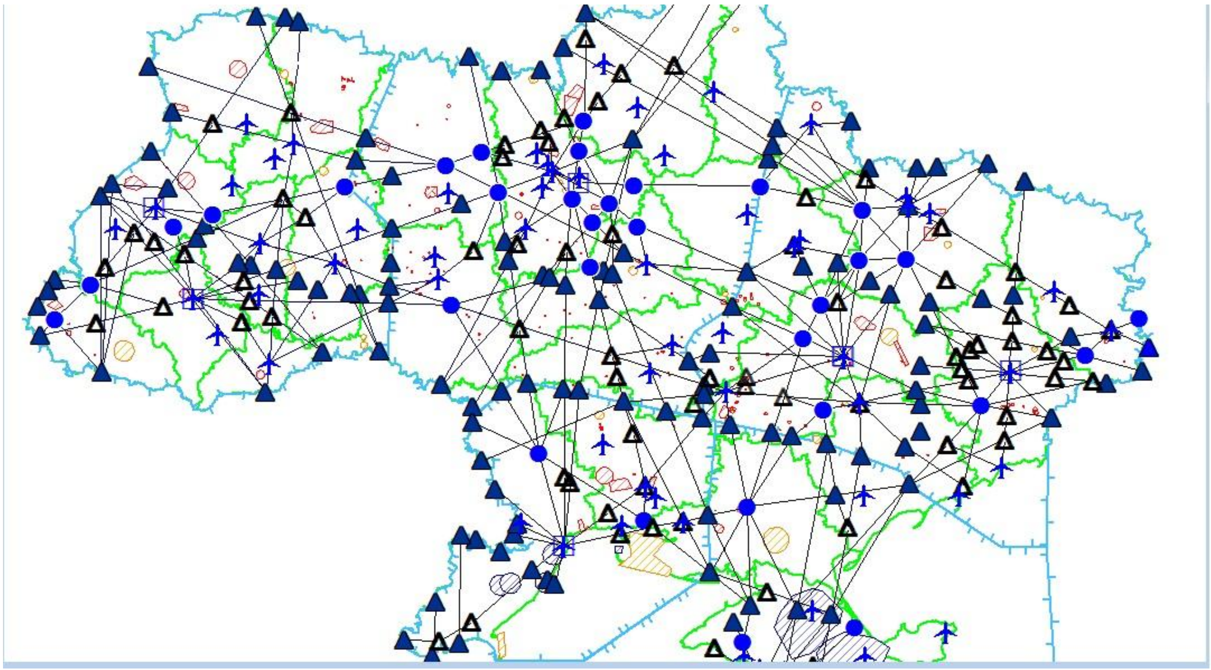


Рисунок 1 Загальний вигляд довершеної цифрової карти нижнього повітряного простору України з відображеними векторними даними.

Висновки

В результаті роботи були проаналізовані вимоги до представлення аеронавігаційної інформації відповідно до міжнародних стандартів та визначено структуру цифрової карти нижнього повітряного простору. За результатами аналізу побудовано цифрову карту нижнього повітряного простору України(до FL295) на основі маршрутної карти ICAO з перетворенням всіх об’єктів растрового зображення у векторні. Перевагою створеної карти є доступність опису кожного об’єкту карти, що дає можливість легкого подальшого редагування та удосконалення карти.

Практична цінність роботи полягає у можливості використання даної цифрової карти сучасними аеронавігаційними системами для управління повітряним простором. Також створена карта може бути використана під час підготовки спеціалістів з обслуговування повітряного руху та операторів наземних засобів керування безпілотним літальним апаратом.

Література:

1.Журкин І. Г., Шайтура С. В. Геоінформаційні системи. — Москва: Кудиц-пресс, 2009. — 272с.

2.M. Bogunenko Actual GIS systems analysisfor solving air navigation problems / M. Bogunenko, S. Kredentsar, E. Znakovskaya // ВісникНАУ. – 2011. – № 3(48).– С.63-74.

Marachovsky L.F.
D.C.S, professor
of the Economic-Technological
Transportation State University
m. Kyiv, Ukraine

BASIC CONCEPTS TO BUILD THE NEXT GENERATION OF RECONFIGURABLE COMPUTING SYSTEMS

Introduction to a new interdisciplinary computer science research. The author proposes to use the new multi-functional and multi-level memory circuits to work around the limitations of legacy systems.

Author revised and enhanced the theorem of structural completeness of the elementary memory of automata [1, p.14]

Every automata system, made of an elementary multifunctional digital circuits of memory (MFDC) with a complete set of transitional signals, output signals and functions of saving the system state (wherein the number of such functions are at least two) along with any functionally complete set of logical elements is a structurally complete system.

Marachovsky’s theory of automata with multifunctional properties.

It examines the operation of MFDC in contiguous time, while the input signals $x(t)$ and $e(\Delta)$ affect the automata’s state within a machine cycle T [2, p. 72].

For the automata Mealy and Moore (1st and 2nd type), informational input signal x(t) set the state of MFDC within a clock period t, while preserving input signal e(Δ) confirms this state within a clock period (T = t + Δ).

The special properties of the automata M (Marakhovsky's theory of automata) allow the input signal e(Δ) to generate an enhanced transition to a new state a(Δ) along with the function of the output signal y(Δ).

The following equations describe the functionality of the abstract Marachovsky's automata of different types [3, p. 68–69]:

1st type]

$$\begin{cases} a(t) = \delta_0(a(\Delta-1), x(t)); \\ a(\Delta) = \delta_e(a(t), e(\Delta)); \\ y_L^1(t) = \lambda_1(a(\Delta-1), x(t)), \\ a(t), a(\Delta) \in \pi_j;\ i = 0, 1, 2, \ldots;\ \Delta = 0, 1, 2, \ldots. \end{cases} \quad (1)$$

2nd type

$$\begin{cases} a(t) = \delta_0(a(\Delta-1), x(t)); \\ a(\Delta) = \delta_e(a(t), e(\Delta)); \\ y_L^2(T) = \lambda_2(a(t), a(\Delta)), \\ a(t), a(\Delta) \in \pi_j;\ i = 0, 1, 2, \ldots;\ \Delta = 0, 1, 2, \ldots. \end{cases} \quad (2)$$

3rd type

$$\begin{cases} a(t) = \delta_0(a(\Delta-1), x(t)); \\ a(\Delta) = \delta_y(a(t), e(\Delta)); \\ y_L^3(\Delta) = \lambda_3(a(\Delta), e(\Delta)), \\ a(t) \notin \pi_j, a(\Delta) \in \pi_j;\ i = 0, 1, 2, \ldots;\ \Delta = 0, 1, 2, \ldots. \end{cases} \quad (3)$$

The above equations completely describe the consolidated multifunctional abstract M-automata [3, p. 64].

The deterministic automata 1st and 2nd types are producing unambiguous state transitions [2, p. 74], while automata 3rd type could produce enhanced state transitions [2, p. 75]. These automats are capable of probability [2, p. 77] and fuzzy [2, p. 78] transitions, and also able to handle hierarchical information simultaneously.

The multifunctional digital circuits of memory (MFDC)

Perspective direction of development of mono-functional binary charts of memory is creation of multi-function charts (MFCM) that were basis of new element base. They have an array pattern of memorizing of information and also have open structure (table 1).

Table 1The matrix states IFAP.

	μ_1	μ_2	.....	μ_n
π_0	a_{10}	a_{20}	...	a_{n0}
π_1	a_{11}	a_{21}	...	a_{n1}
π_2	a_{12}	a_{22}	...	a_{n2}
...	...	...	...	...
π_m	a_{1m}	a_{2m}	...	a_{nm}

MFDC's internal structure allows to used at least two logical AND-NOT (OR-NOR) in each group. MFDC could change its state while is affected by two subsequent input signals x and e [3. p. 179].

The theory of MFDC offers the principles and methods of building two classes of such schemes: Class L and Class L^m

The multilevel digital circuits of memory (MLDC)

The automata of strategy (AoS or controller) is used to generate preserving input signals e(Δ) for MFDC and it could be in a form of a multistable flip-flop or the MLDC [3, p. 234]

Input signals x(t) - Input z_i (i= 1, 2, 3) - are affecting the AoS and the MFDC in parallel while the AoS (within MLDC) is generating the preserving input signals e(Δ).

This would allow the AoS to process general information and the MFDC to process partial information within a single automata cycle T.

Those new features allow to tune subsets of the MFDC states within the MLDC.

There were proposed two types of the MLDC of classes L_N and L_N^B. For the MLDC of the L_N^B class, the AoS is used not for the entire MFDC, but independently, for the each group.

The principle of hierarchical programmatic control (HPC).

CharlesBabbageproposed the principle ofprogram management, where the informationis broken down intodataand data management.The author proposesthe principleof hierarchicalmanagementsoftware, wheredata andinformationmanagementsystemis dividedintoahierarchyof data andcontrol hierarchy [2, p. 304]. The principle of HPC is that the general control information is used to select partial control information.

The presented principle allows changing subsets of MFDC' states simultaneously, within a single automata cycle T.

The fourth level of control.

In order to build reconfigurable computing devices based on the MFDC and MLDC, the author introduces an additional, forth miliprogrammed level of control to process general information [3, p. 302].

The forth level of control fulfills the principle of HPC and allows processing general and partial information simultaneously which is the basis to build reconfigurable computing devices based on the existing hardware components of elementary digital circuits of memory.

Standard reconfigurable devices.

The standard reconfigurable devices include: the control units, registers, counters, processors and computers [3. p. 258–322].

Conclusion

The new technology would allow developing competitive computing systems with enhanced functionalities, another word with significantly increased machine intelligence.

Literature:

1.Мараховский Л.Ф. Основы теории проектирования дискретных устройств. Логическое проектирование дискретных устройств на схемах автоматной памяти: монография. – Киев: КГЄУ, 1996.–128 с.

2.Мараховский Л. Ф. Комп’ютерна схемотехніка: навч. посібник. – К.: КНЕУ, 2008. – 360 с.

3.Мараховский Л.Ф. Основы новой информационной технологии: монография / Л.Ф. Мараховский, Н.Л. Михно. – Saarbrcken, Germany / i.melnic@lap-publishing.ru / www.lap-publishing.ru, 2013 – 369 с.

Козубцов І.М.

Провідний науковий співробітник науково-дослідного відділу

Науковий центр зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації

м. Київ, Україна

ПРО МОТИВАЦІЙНИЙ ПОРТРЕТ УЧАСНИКИ КІБЕРНЕТИЧНОГО ПРОТИСТОЯННЯ

Визначення проблеми. Одним з ключових причин виникнення проблемиу кібернетичному просторі є: наявність негативно налаштованих групувань, які бажають реалізації протиправних дій у кібернетичному просторі, шляхом порушення цілісності, доступності і конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам.

Аналіз публікацій за напрямком дослідження. Темі присвячено досить багато досліджень, які в сукупності вибудовують цілісну картину. Проте питанню опису мотиваційного портрета учасників кібернетичного протистояння приділено недостатньо уваги.

Формулювання мети доповіді. Описати мотиваційні портрети ключових гравців кібернетичного протиборства.

Результат дослідження. Визначимо ключових гравців кібернетичного простору. Автори [1 с. 156] визначили суб’єкти кібернетичного простору лише в загальному вигляді, не надавши приналежність до громадянства. А це, на нашу думку, важливо, оскільки правила поведінки ключових гравців в кібернетичному просторі визначається етичними нормами поведінки та нормативно-процесуальним законодавством країни [2]. Натомість нормативно-процесуальне законодавство країн світу має відмінності, які поступово усуваються процесами глобалізації міжнародного права. Гравців кібернетичного протиборства можна умовно згрупувати в групи: громадяни країни, люди без громадянства, іноземні громадяни табл. 1. Відповідно до цих груп можна побудувати наступні моделі: порушника інформаційно-кібернетичного простору та захисника інформаційно-кібернетичного простору.

Таблиця 1. Класифікація учасників кібернетичного простору

Учасники кібернетичного простору	Рівень мережі	Категорія користувача	Модель	
			захисника	порушник
Громадяни України	мережа внутрішня закрита	військовослужбовці Збройних Сил України; працівники Збройних Сил України; військовослужбовці інших військових (силових) формувань; працівники військових (силових) формувань	+	+ / –
	мережа внутрішня (корпоративна)	громадяни України (члени корпорації) не резиденти (члени корпорації)	+	+ / –
	мережа Інтернет	всі перелічені категорії громадяни	+	+ / –
Іноземні громадяни	мережа внутрішня закрита (в межах своєї держави)	громадяни країни, яким надано допуск та доступ до мережі	– / +	+
	мережа внутрішня (корпоративна)	громадяни однієї країни (члени корпорації) не резиденти та резиденти (члени корпорації)	– / +	+
	мережа Інтернет	всі перелічені категорії громадяни	– / +	+
особи без громадянства (що перебувають в Україні)	мережа внутрішня закрита	доступ заборонений	– / +	+
	мережа внутрішня (корпоративна)	члени транснаціональних корпорації	– / +	+
	мережа Інтернет	всі перелічені категорії громадяни	– / +	+
особи без громадянства (що перебувають за межами	мережа внутрішня закрита	доступ заборонений	– / +	+
	мережа внутрішня (корпоративна	члени транснаціональних корпорації	– / +	+

України)	)			
	мережа Інтернет	всі категорії громадяни	– / +	+
Провайдери Інтернету	провідний	матеріальна мотивація	+	+ / –
	регіональний	матеріальна мотивація	+	+ / –
	периферійний	матеріальна мотивація	+	+ / –
	дротовий	матеріальна мотивація	+	+ / –
	(бездротовий) стільниковий	матеріальна мотивація	+	+ / –

Гравці кібернетичного протиборства можуть реалізовувати вплив як із зовні, так і з середини держави. Нами розроблено умовну класифікацію мотивацій гравців кібернетичного простору (табл. 2).

Таблиця 2. Класифікація мотивацій учасників кібернетичного простору

Мотивації учасників кібернетичного простору		Додаткова класифікація	Модель	
			захисник	порушник
Мотивація				
Матеріальні		телекомунікаційні компанії	+ / –	+ / –
		провайдер Інтернету	+ / –	+ / –
		абонент – користувач	+ / –	+
Духовні		абонент – користувач	+	+ / –
Ідейні		політичні	+	+ / –
		релігійні	– / +	+ / –
		щирі патріоти	+	+
		не щирі патріоти	– / +	+ / –
		кримінал	–	+
Стійке формування мотивації, що не піддається швидкому корегуванню		допитливість	– / +	+
		ентузіасти	+	+
		ідіоти	–	+
Професійні		розвідник	+	–
		шпигун	–	+
Інсайдери		зловмисник	–	+
Типові умови та фактори впливу на мотивацію				
Підкуп		всі категорії громадяни	–	+
Шантаж		всі категорії громадяни	–	+
Бюрократія		всі категорії громадяни	+	+
Професійні		всі категорії громадяни	+	+
Хвороба		всі категорії громадяни	+	+
Особливі потреби		всі категорії громадяни	+	+
Потреби за	фізіологічні	всі категорії громадяни	– / +	+ / –
	безпека	всі категорії громадяни	– / +	+ / –

Маслоу	соціальні	всі категорії громадяни	– / +	+ / –
	поваги	всі категорії громадяни	– / +	+ / –
	самовиражен-ня	всі категорії громадяни	– / +	+ / –

Модель учасника в математичній формі матиме такого виду (1):

$$\grave{I}_{0} = \left(\hat{I}_{p}, O_{\ln}, O_{a}, \hat{I}_{pn}\right) \times M(x). \tag{1}$$

де M(x) – мотиваційна характеристика; O_p – місце розташування порушника; O_{ln} – професійний рівень знань та умінь порушника; O_a – сценарій можливого доступу; O_{pn} – первинні знання порушника про систему. Відповідно $O_p \in \{1,2,3\}$, де 1 – порушник зовнішній; 2 – порушник внутрішній; 3 – злочинна домовленість внутрішніх та зовнішніх порушників, наприклад підкуп, шантаж. Професійний рівень знань та умінь порушника $O_{ln} \in \{1,2,3\}$, де 1 – низький рівень; 2 – середній рівень; 3 – високий рівень. $M(x) \in \{0,1\}$ приймає значення: 0 – порушник кібернетичного простору; 1 – захисник кібернетичного простору.

Висновки з дослідження. На нашу думку, необхідно раціонально підходити до побудови моделі порушника та захисника кібернетичного простору з урахуванням мотиваційного портрету. В залежності від необхідного результату необхідно створювати відповідні мотиваційні характеристики у гравців кібернетичного протиборства. Ми навмисно не розглядали порушників, що імітують (створюють) технічні, обчислювальні засоби обробки інформації (комп'ютери, ноутбуки, планшети, мобільні додатки), оскільки вони поки що створені біологічною особою (індивідуумом) виходячи з власної мотиваційної характеристики. В такому разі вони працюють за певним алгоритмом. Задача може ускладнитися в майбутньому, коли штучний інтелект почне створювати власне кібернетичну загрозу.

Література:

1. Черняк О.Р. Тенденції розвитку кіберзагроз у світовому інформаційному просторі / О.Р. Черняк, О.В. Федулов // Сучасні інформаційні технології у сфері безпеки та оборони. 2014. – №1(19). – С.155 – 158.

2. Дубов Д. Проблеми чинної вітчизняної нормативно – правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка / Д. Дубов, М. Ожеван // [Електронний ресурс]. – Режим доступу URL: http://www.niss.gov.ua/articles/454.

Козубцов І.М.

Провідний науковий співробітник науково-дослідного відділу
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації
м. Київ, Україна

ОБГОВОРЕННЯ СТРУКТУРИ СТРАТЕГІЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Визначення проблеми. Доктрина інформаційної безпеки України, яка за задумом розробників є «основою для розроблення проектів концепцій, стратегій, цільових програм і планів дій» [1], виявилась не ефективною для побудови шляху від постановки завдань та формулювання мети до практичного результату. Автор у роботі [2] звертає увагу, «що таке є Доктрина, як не стратегічний, програмовий і концептуальний документ?» Досі триває підготовка закону про кібернетичну безпеку. Існує намір після його ухвалення затвердити відповідну Стратегію. Відзначимо, що даний підхід наражається на аналогічні заперечні аргументи, що закон є нормативно-правовим актом прямої дії та не потребує на своє розгортання прийняття інших документів такого рівня. Значною мірою є складнощі у прийнятті та практичній реалізації різноманітних концепцій, стратегій, доктрин, що обумовлено відсутністю усталеної системи ієрархії керівних документів державної політики та не усвідомленням відмінності від інших нормативно-правових актів. Нерозв'язаність цієї проблеми призводить до нестабільної та незбалансованої державної політики, зменшує ефективність державного-управлінського впливу, як в інформаційній сфері, так і в політиці в цілому.

Темі присвячено досить багато досліджень, які в сукупності вибудовують цілісну картину. Найбільш значущими з них є дослідження: Г. Ситник [3], А. Кузьменко [4], М.О. Мельник [5], А.В. Баровська [6]. На думку числа дослідників: О. Берданова, В. Вакуленко, В. Тертичка ці документи мають складати основу стратегічного планування, актуальність якого обумовлена, в першу чергу, його раціональністю[7]. Зазначимо, що в Україні, на практиці, користуються наступною ієрархію керівних документів державної політики [8]: Доктрина → Концепція → Стратегія → Програма → План. Водночас наукові дослідження пропонують й інші підходи до розгортання ієрархії керівних документів державної політики, зокрема: Концепція → Доктрина → Стратегія → Програма ([3]); Стратегія → Концепція → Доктрина → Програма ([4]).

І якщо на саму послідовність (ієрархію) документів існують різні погляди, то щодо її обов'язковості думка є одностайною. Оскільки загальновизнаного підпорядкування керівних документів державної політики немає, тому необхідним є нормативно-правове врегулювання цього питання, що належить сфері законодавства, яке визначає систему стратегічного планування. Проте питанню структури та змістовного наповнення автори не достатньо приділили уваги, а тому є актуальним запропонувати структуру стратегії дій учасників у кібернетичному просторі. В наступному переліку наведено перелік діючих концепцій та стратегій кібернетичної безпеки: [9 – 12].

Формулювання мети доповіді. Обґрунтування структуру стратегії дій учасників у кібернетичному просторі.

Результат дослідження. Розглянемо класичний підхід до рішення проблеми, що застосовується на державному рівні. Ієрархічна структура розкривається в наступній послідовності: доктрина, концепція, стратегія, програма [13]. Такий підхід безумовно можна застосувати як фундаментальний і для рішення нашої проблеми, а шлях реалізації, як методологію проектування системи кібернетичної безпеки. Виникає логічне і очевидне запитання: «Чому і досі не спроектована та розгорнута надійна система кібернетичної безпеки».

Відповідь на це питання ми відшукали в результаті аналізу різного роду і за призначення стратегій. Під «стратегією» розуміється (др.-греч. στρατηγία — «искусство полководца») – наука о войне, в частности наука полководца, общий, недетализированный план военной деятельности, охватывающий длительный период времени, способ достижения сложной цели, позднее вообще какой-либо деятельности человека.

Задачею стратегії є ефективне використання наявних ресурсів для досягнення основної цілі (стратегія, як спосіб дій становиться особливо необхідною в ситуації, коли для прямого досягнення основної цілі недостатньо наявних ресурсів). Тактика є інструментом реалізації стратегії підпорядкована основній цілі стратегії. Стратегія досягається основної цілі через рішення проміжних тактичних задач по осі «ресурси – ціль».

На думку Карла Клаузевица [14] «ведение войны подразумевает два совершенно различных вида деятельности: организация отдельных боев и ведение их; увязка их с общей целью войны». Ця думка пояснює чому написані десятки стратегій і досі не введені в практику. Річ у втім, що вони не розкривають механізм практичної реалізації, оскільки текст є абстрактним. За аналогією до нормативно-процесуальної законодавства пропонується наступна структура стратегії дій учасників у кібернетичному просторі. Вона складається з наступних складових: 1) Постійного розвитку системи кібернетичної безпеки та її учасників. 2) Функціональної структури системи кібернетичної безпеки. 3) Стратегічний алгоритм реагування системи кібернетичної безпеки на інциденти. 4) Тактичний алгоритм реагування системи кібернетичної безпеки на інциденти. 5) Перелік всіх учасників (моделей) кібернетичного простору. 6) Правило гри в кібернетичному просторі. 7) Порядок фінансування реалізації стратегії.

Висновки з дослідження. На нашу думку, запропонована структура стратегії кібернетичної безпеки є функціонально працездатною. Функціональна працездатність полягає в створенні стратегії в якій закладено динамічний процес та чітко визначений сектор відповідальності учасників кібернетичного простору. Крім того, стратегія враховує мотиваційні портрети порушників та захисників кібернетичного простору. В залежності від очікуваних результатів зводиться задача створення тієї чи іншої мотиваційної характеристики до моделі, а отже, трансформувавши її на групу учасників кібернетичного простору.

Література:

1. Доктрина інформаційної безпеки України: Про Доктрину інформаційної безпеки України: Указ Президента України №514/2009 [Електронний ресурс] // Верховна рада України. – Режим доступу URL: http://zakon2.rada.gov.ua/laws/show/514/2009.

2. Северин О. Доктринально говорячи / О. Северин [Електронний ресурс]. – Режим доступу URL: http://stop-x-files-ua.org/?p=1809.

3. Ситник Г.П. Державне управління у сфері забезпечення національної безпеки України: теорія і практика: Автореф. дис... д-ра наук з держ. управління: 25.00.01 / Г.П. Ситник; Нац. акад. держ. упр. при Президентові України. – К., 2004. – 36 с.

4. Кузьменко А. Проблеми відповідності стратегії та системи забезпечення безпеки України національним потребам / А. Кузьменко // Юридичний Журнал. – 2006. – №10 [Електронний ресурс]. – Режим доступу URL: http://www.justinian.com.ua/article.php?id=2432.

5. Мельник М.О. Особливості формування стратегічних документів державної політики у сфері соціального становлення та розвитку молоді в Україні / М.О. Мельник // [Електронний ресурс]. – Режим доступу URL: http://www.kbuapa.kharkov.ua/e-book/tpdu/2014-3/doc/2/05.pdf.

6. Баровська А.В. Оптимізація структури керівних документів державної політики (на прикладі інформаційної сфери) / А.В. Баровська. – К.: НІСД, 2011. – 46с.

7. Стратегічне планування. Навчальний посібник / О. Берданова, В. Вакуленко, В. Тертичка. – Л.: ЗУКЦ, 2008. – С.6.

8. Коментар до проекту Доктрини інформаційної безпеки України [Електронний ресурс]. – Режим доступу URL: http://www.rainbow.gov.ua/news/942.html.

9. Концепция стратегии кибербезопасности // Вопросы кибербезопасности №1(2) – 2014 – С. 2 – 4.

10. Государственные стратегии кибербезопасности // [Электронный ресурс]. – Режим доступа URL: http://ibst.pnzgu.ru/index.php/news/novosti-v-mire-it-i-ib/129-gosudarstvennye-strategii-kiberbezopasnosti.

11. Концепция стратегии кибербезопасности Российской Федерации [Электронный ресурс]. – Режим доступа URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

12. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Электронный ресурс]. – Режим доступа URL: http://ens.mil.ru/files/morf/Strategy.doc.

13. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування. Аналітична записка // [Електронний ресурс]. – Режим доступу URL:http://www.niss.gov.ua/articles/572/

14. Клаузевиц, Карл фон. О войне Клаузевиц К. О войне. – М.: Госвоениздат, 1934 [Электронный ресурс]. Сайт «Военная литература». – Режим доступа URL: http://militera.lib.ru/science/clausewitz/index.html.

Берназ Н.М.

Ст. викладач каф. Вищої математики

Державний університет телекомунікацій

м. Київ, Україна

АНАЛІЗ ІЄРАРХІЇ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Методи забезпечення функціональної стійкості телекомунікаційних мереж досить різноманітні і реалізовуються на основі різних принципів і підходів до організації стійкості. Можливу класифікацію підходів до реалізації програмних засобів функціональної стійкості через їх різноманіття доцільно будувати у вигляді деякої ієрархічної структури. На першому рівні ієрархії методів стійкості і їх програмної реалізації потрібно виділити наступні методи забезпечення функціональної стійкості телекомунікаційної мережі:

стійкість системи, по відношенню до суб'єкта, який здійснює вторгнення в телекомунікаційну мережу;

стійкість програмно-апаратних компонент обчислювача;

– стійкість від факторів вторгнення в телекомунікаційну мережу, які не персоналізовані з конкретним користувачем.

Засоби стійкості по відношенню до суб'єкта, який здійснює вторгнення, носять персоніфікований характер, що стосується також і програмних засобів їх реалізації. Ці засоби досить різноманітні і їх доцільно класифікувати таким чином:

особисті, персоналізовані програмні компоненти функціональної стійкості системи;

програмні засоби підтримки функціональної стійкості персоналізованих компонент системи;

не персоналізовані засоби функціональної стійкості по відношенню до користувача, як суб'єкта вторгнення;

технологічні програмні засоби функціональної стійкості системи.

Засоби функціональної стійкості програмно-апаратних компонент телекомунікаційних мереж можна класифікувати з різних точок зору. Одна з них полягає у виділенні типу компоненти, оскільки різні види компонент телекомунікаційної мережі можуть вимагати різні способи реалізації засобів функціональної стійкості. Тому розглянемо наступну класифікацію типів компонент телекомунікаційних мереж:

дані обчислювальних систем (масиви, файли даних і інші об'єкти, які не реалізують логіку функціонування системи, наприклад, таблиці, матриці і т.д.);

програмні засоби рішення прикладних задач, програмні засоби, які реалізують різні додатки (в частині реалізації логіки їх стійкості);

операційні програмні засоби, що складаються з програм операційних систем, таблиць і інших елементів системного характеру;

додаткові засоби системного забезпечення функціональної стійкості обчислювальної системи;

програмні засоби підтримки персоналізованих компонент функціональної стійкості системи.

Приведена система відображає два рівні ієрархії в класифікації можливих несанкціонованих впливів на функціональну стійкість телекомунікаційної мережі. Можна запропонувати і інші типи класифікації, але приведений тип класифікації найбільш прийнятний з точки зору задач, що розглядаються в доповіді.

Бодров С.В.
Здобувач каф. Комп'ютерних систем та мереж
Державний університет телекомунікацій
м. Київ, Україна

АЛГОРИТМ ВИЯВЛЕННЯ НЕСТІЙКИХ ВІДМОВ І ЗБОЇВ У СИСТЕМАХ ІНТЕЛЕКТУАЛЬНОГО ВІДЕОКОНТРОЛЮ

В даній доповіді розглядається система обміну даних мережі відеоконтролю на прикордонних пунктах пропуску, що відноситься до класу складних організаційних систем. В системі обмін даними відбувається на основі технології локальних обчислювальних мереж. Вона складається з вузлів комутації і каналів (ліній) зв'язку між ними. Головною вимогою, що висувається до системи обміну даних, є виконання нею основної функції – забезпечення абонентів мережі потенційною можливістю доступу до розподілених інформаційних ресурсів, об'єднаних у систему обміну даних. У сучасних умовах на систему обміну даними впливають внутрішні (відмови, збої, помилки) і зовнішні (навмисне пошкодження) фактори. Тому задача своєчасного знаходження відмов і збоїв є актуальною.

Під нестійкою відмовою в доповіді будемо розуміти відмову, яка, у деякий момент часу може перебувати в активному стані, порушуючи при цьому правильне функціонування системи інтелектуального відеоконтролю (СІВ), і в інший момент часу – в пасивному стані, дозволяючи СІВ працювати коректно. Іншими словами, нестійка відмова – це така відмова, вплив якої на поведінку СІВ має місце тільки в певні моменти часу. На відміну від постійних відмов для нестійких розрізняється їх існування в СІВ та їх активна поведінка. Простим прикладом нестійкої відмови є наявність в СІВ некоректності, яка робить вплив на правильне функціонування СІВ при певних обставинах, наприклад, при впливі різних збурюючих чинників.

Суть діагностування нестійких відмов полягає в можливому виявленні відмови за рахунок виконання перевірок, що повторюються, в моменти активної фази нестійкої відмови, накопичення і подальшого аналізу модернізованого синдрому. Особливість даного підходу полягає в тому, що процедура діагностування здійснюється одночасно з вирішенням робочих завдань і є фоновою по відношенню до них. Завдяки цьому, виключається вплив процедури діагностування на обчислювальний процес у системі інтелектуального відеоконтролю. Такий підхід може бути здійснено лише при реалізації випадкової структури діагностичних зв'язків. Якщо аналіз синдрому показує наявність суперечностей в результатах перевірок між підмножинами модулів, то в системі виникли збої, нестійкі відмови або некоректності каналів інформаційного обміну. Такі ситуації відмов прийнято називати гібридними. Саме виявленню таких відмов системи відеоконтролю прикордонних пунктів пропуску і присвячена дана доповідь.

Барабаш О.В.
Д.т.н., завідувач каф. Вищої математики
Мусієнко А.П.
к.фіз.-мат.н., доцент каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ПРОЦЕСІВ УПРАВЛІННЯ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

В доповіді розглядаються основні методики забезпечення функціональної стійкості процесів управління в телекомунікаційній мережі на основі інтелектуалізації навігаційного комплексу.

Основною особливістю функціонально-стійких систем являється їх здатність деградувати на структурному рівні до повної відмови системи, тобто виключати зі структури несправні елементи, перебудовувати структуру, настроювати параметри системи для пристосування (адаптації) до нових умов експлуатації. Основним засобом забезпечення функціональної стійкості є введення надмірності (структурної, програмної, тимчасової і т.д.) при їх проектуванні.

Разом з тим, такий підхід, що часто використовується в різних технічних системах, не може бути використаний в розподілених інтелектуалізованих системах управління, ключовим елементом яких є розподілена база знань. На відміну від технічних систем, база знань не може деградувати, виключаючи з роботи окремі свої модулі, оскільки утворилися в такому випадку розриви не забезпечать нормальне її функціонування, а висновок, зроблений на такій базі знань, не буде володіти необхідною достовірністю.

У такому випадку необхідний дещо інший підхід до визначення поняття і формування етапів забезпечення функціональної стійкості інтелектуальної системи автоматичного управління.

Під функціональною стійкістю розподіленої інтелектуалізовано телекомунікаційної мережі будемо розуміти її властивість зберігати протягом заданого часу виконання своїх основних функцій в умовах протидії зовнішніх дестабілізуючих факторів.

Основна відмінність стійкості функціонування від функціональної стійкості полягає в наступному: стійкість функціонування характеризує поведінку координат незбуреного і збуреного руху системи

$$\forall\theta > 0 \Rightarrow \delta > 0,\ \rho(z_0, z_0') < \delta \Rightarrow \rho[z(t, z_0), z(t, z')_0] < \theta, \quad \forall t \in [0, \infty),$$

де $z_0 = z(0)$ – початкові умови – координати фазового простору z_0 при незбуреному русі; $z_0' = z'(0)$ – координати фазового простору при збуреному русі; ρ – метрика простору Z ; ε, θ – задані числа, що характеризують відхилення обуреного руху від незбуреного.

Функціональна стійкість характеризує відхилення основних функцій від координат при збуреному і незбуреному русі

$$\forall\theta > 0 \Rightarrow \delta > 0,\ \rho(f(z_0), f(z_0')) < \delta \Rightarrow \rho[f(z(t, z_0)), f(z(t, z_0'))] < \theta, \quad \forall t \in [0, \infty),$$

де $f(z)$ – функція від координати руху системи, яка характеризує основні вимоги, що пред'являються до системи.

Яременко Є.П.
студент
Моторний В.М.
студент
Національний авіаційний університет
м. Київ,Україна

КЛАСИФІКАЦІЯ ТИПІВ ШИФРУВАННЯ ДЛЯ БЕЗДРОТОВИХ СИСТЕМ ЗВ’ЯЗКУ

Для того щоб забезпечити надійність захисту інформації в бездротових мережах існує декілька видів шифрування. Але в даний час не має такого типу шифрування який би не мав недоліків. Тому кожен типвикористовується в певній галузі або системі.

Метою робити є дослідження різних типів шифрування в різних галузях, визначення їхніх характеристик, переваг та недоліків. Також дослідження криптостійкості шифрувань.До основних методів шифрування можна віднести WEP TKIP та AES.

WEP-шифрування (Wired Equivalent Privacy). Аналог шифрування трафіку в провідних мережах. Використовується симетричний потоковий шифр RC4 (англ. Rivest Cipher 4), який досить швидко функціонує. На сьогоднішній день WEP і RC4 не рахуються крипостійкість. Є два основні протоколи WEP:

• 40-бітний WEP (довжина ключа 64 біта, 24 з яких - це вектор ініціалізації, який передається відкритим текстом);

• 104-бітний WEP (довжина ключа 128 біт, 24 з яких - це теж вектор ініціалізації); Вектор ініціалізації використовується алгоритмом RC4. Збільшення довжини ключа не призводить до збільшення надійності алгоритму.

Основні недоліки:

• використання для шифрування безпосередньо пароля, введеного користувачем;

• недостатня довжина ключа шифрування;

• використання функції CRC32 для контролю цілісності пакетів;

• повторне використання векторів ініціалізації та ін.

TKIP-шифрування (Temporal Key Integrity Protocol). Використовується той же симетричний потоковий шифр RC4, але є більш крипостійкий. Вектор ініціалізації становить 48 біт. Враховано основні атаки на WEP. Використовується протокол Message Integrity Check для перевірки цілісності повідомлень, який блокує станцію на 60 секунд, якщо були послані протягом 60 секунд два повідомлення не пройшли перевірку цілісності. З урахуванням всіх доопрацювань і удосконалень TKIP все одно не вважається крипостійким.

CKIP-шифрування (Cisco Key Integrity Protocol).Має схожості з протоколом TKIP. Створено компанією Cisco. Використовується протокол CMIC (англ. Cisco Message Integrity Check) для перевірки цілісності повідомлень.

WPA-шифрування. Замість уразливого RC4, використовується криптостійкий алгоритм шифрування AES (Advanced Encryption Standard). Можливе використання EAP (англ. Extensible Authentication Protocol, розширюваний протокол аутентифікації). Є два режими:

• Pre-Shared Key (WPA-PSK) - кожен вузол вводить пароль для доступу до мережі;

• Enterprise - перевірка здійснюється серверами RADIUS;

WPA2-шифрування (IEEE 802.11i).Прийнято в 2004 році, з 2006 року WPA2 повинна підтримувати всі випускається Wi-Fi обладнання. У даному протоколі застосовується RSN (англ. Robust Security Network, мережа з підвищеною безпекою). Спочатку в WPA2 використовується протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника). Основою є алгоритм AES. Для сумісності зі старим обладнанням є підтримка TKIP і EAP (Extensible Authentication Protocol) з деякими його доповненнями. Яків WPA єдварежимироботи: Pre-Shared Key і Enterprise.

WPA і WPA2 мають такі переваги:

ключі шифрування генеруються під час з'єднання, а не розподіляються статично.

для контролю цілісності переданих повідомлень використовується алгоритм Michael.

використовується вектор ініціалізації істотно більшої довжини.

На практиці крпиптостійкість кожного типу шифрування ми перевіряли за допомогою роутера D-link та програми злому AirSlax 5 pro. Ця програма включає в себе всі можливі алгоритми підбору паролю, такі як: brute forse airctack, hashcat та інші.

Таким чином після дослідження ми визначили який тип шифрування доцільніше використовувати в певній структурі, з урахуванням рівня небезпек, трафіків та затримок в мережі. Для захисту домашньої мережі або невеликого офісу краще використовувати WPA2-PSK, компанії (більше 30 абонентів) – WPA2- Enterprise. Концепція може змінюватись в залежності від плану приміщення, та захисту зовнішнього периметру.

Література:

1.Защита информации в телекоммуникационных системах Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов

2.Нечаев М. Правовые и организационные основы комплексных систем защиты информации // Корпоративные системы. – 2008. – №2. – С.54-57.

3.Подробнее информация о протоколах аутентификации WPA приведена в статье «Защита беспроводных сетей, WPA: теория и практика» на сайте IXBT.

Мужанова Т.М.

Доцент каф. Управління інформаційною безпекою

Державний університет телекомунікацій

м. Київ, Україна

УПРАВЛІННЯ МЕРЕЖЕЮ ІНТЕРНЕТ: ПОШУК КОНСЕНСУСУ НА МІЖНАРОДНОМУ РІВНІ

На думку багатьох науковців та практиків, Інтернет є найбільш значним і корисним винаходом у сфері комунікацій в історії людства. Однак, як і будь-якій інновації, Інтернету притаманні не тільки переваги, серед яких - можливість швидкого зв'язку та спілкування, доступ до інформації та послуг, але й велика кількість загроз технічного, економічного та соціально-психологічного характеру, з якими стикається користувач (від громадянина, організації, підприємства до держави, глобальної спільноти).

Багато невирішених проблем щодо функціонування Інтернету, встановлення правил, вимог та заборон щодо діяльності у глобальному мережевому просторі є сьогодні предметом бурхливих дискусій. Серед них - питання розвитку мережевої інфраструктури Інтернету, забезпечення безпеки, стабільності, відмовостійкості всесвітньої мережі, визначення меж і ефективності національного регулювання Інтернету, в т.ч. можливості його «відключення», проблеми встановлення юрисдикції в Інтернеті, а також неприпустимість його протиправного використання [3].

Як відзначають спеціалісти, саме визначення терміна «Інтернет» породжує суперечки, які виникли щодо управління Інтернетом. Наприклад, фахівці в області телекомунікацій розглядають проблему управління Інтернетом крізь призму технічної інфраструктури. Професіонали в області комп'ютерних технологій в основному приділяють увагу розробці різних стандартів, мов і додатків як засобів забезпечення впорядкованості мережі. Фахівці з комунікації роблять акцент на спрощенні обміну інформацією. Активісти боротьби за права людини розглядають управління Інтернетом з погляду свободи висловлення переконань, захисту таємниці приватного життя та інших основних прав особистості. Юристи звертають увагу на питання юрисдикції і вирішення правових суперечок. Політики по всьому світу зазвичай говорять про засоби масової інформації та про питання, що знаходять відгук у виборців, наприклад про перспективи (більше комп'ютерів – вищий рівень освіти) і загрози (безпека Інтернету, захист дітей). Дипломатів у першу чергу турбує сам процес регулювання і захист національних інтересів [1].

У результаті тривалих дискусій на міжнародному рівні запропоновано визначення, відповідно до якого управління Інтернетом (англ. - Internet Governance) – це розробка і застосування урядами, приватним сектором і громадянським суспільством, при виконанні ними своєї відповідної ролі, загальних принципів, норм, правил, процедур прийняття рішень і програм, регулюючих еволюцію і застосування Інтернету [3].

Серед основних міжнародних суб'єктів процесу впорядкування всесвітньої мережі відзначають насамперед такі, як Інтернет корпорація з присвоєння доменних імен та номерів (ICANN) та інші організації інфраструктури Інтернету; Регіональний Інтернет-регістратор (RIR), Товариство Інтернету (Internet Society), Інженерна Рада Інтернету (IETF) тощо; Міжнародний союз електрозв'язку, інші спеціалізовані установи ООН і міжурядові організації.

Дієвим інструментом організації дискусії щодо майбутнього вигляду Інтернету є міжнародні, регіональні та національні форуми з управління Інтернетом, у роботі яких беруть участь усі зацікавлені сторони, в тому числі бізнес та громадське суспільство, які зацікавлені у вирішенні проблем всесвітньої мережі з огляду на свої корпоративні чи суспільні інтереси.

У квітні 2014 року відбулася певною мірою віхова подія у процесі пошуку механізмів упорядкування всесвітньої мережі - Глобальний саміт з перспективних питань управління Інтернетом (NetMundial), який ознаменував 40 років з моменту появи першої публікації про протокол передачі даних TCP, 25 років з моменту появи глобальної мережі і викликав очікування інноваційного прориву у вирішенні проблеми управління Інтернетом.

За підсумками зустрічі за участю понад 800 делегатів, з яких 37% учасників представляли 19 держав, 23% - громадянське суспільство, 20% - приватний сектор, по 10% - технічні та академічні спільноти [2], були визначені принципи та Дорожня карта подальшого розвитку управління Інтернетом.

Серед принципів щодо утвердження стандартів прав людини в мережі визнано свободу вираження, об'єднань та інформації; недоторканність приватного життя, гарантії рівноправності в доступі і участь у розвитку Інтернету.

У Дорожній карті наголошено, що процес управління Інтернетом має здійснюватися на таких засадах:

рівноправна участь усіх зацікавлених сторін, зокрема урядів, приватного сектору, громадянського суспільства, технічних співтовариств, освітніх установ і користувачів,

відкритість та прозорість процесів прийняття рішень та діяльності інституцій,

партнерство усіх зацікавлених сторін і прийняття рішень на основі консенсусу та врахування інтересів усіх учасників, підзвітність та гнучкість політики управління Інтернетом [4].

На саміті також особливо підкреслено, що віддалена участь є способом розширення прав і можливостей залучення зацікавлених сторін у процес прийняття рішень.

Однак учасники зібрання звернули увагу на те, що:

підсумкова декларація саміту містить розпливчасті формулювання і не розглядається як обов'язкова;

недостатньо чітко визначена позиція глобального форуму щодо суворіших законодавчих обмежень стеження в Інтернеті;

у результаті лобіювання представників ІКТ-бізнесу нейтральність мережі не була включена в остаточний список принципів, а визначена тільки як питання, що буде обговорюватися;

у декларації закріплено положення, відповідно до якого поширення інформації в Інтернеті здійснюється з обмеженнями, які накладаються авторським правом, що фактично ускладнює можливості доступу до інформації для користувачів [2].

За словами експертів, Глобальний саміт засвідчив черговий виток еволюції розуміння міжнародним співтовариством і всіма зацікавленими сторонами природи Інтернету і способів вироблення домовленості щодо управління Мережею. Однак, не виправдав очікувань щодо вироблення інноваційних шляхів вирішення проблем упорядкування всесвітньої мережі, оскільки наявні суперечності між різними учасниками цього процесу, серед яких держави, які представляють свої геополітичні інтереси, бізнес, зацікавлений в комерціалізації Інтернету, громадськість, яка стоїть на сторожі прав і свобод людини і громадянина.

Література:

1.Курбалийя Й. Управление Интернетом. [Електронний ресурс]. – Режим доступу: http://www.cctld.ru/files/IG-2010-12oct.pdf

2.Матеріали про Глобальний саміт з питань управління Інтернетом: Блог Центру правової трансформації. [Електронний ресурс]. – Режим доступу: http://www.lawtrend.org/information-access/blog-information-access/marina-sokolova-netmundial-pravitelstva-nachinayut-i-vyigryvayut

3.Якушев М.В. Управление Интернетом (2014 г.): проблемы, инициативы, перспективы: доклад на региональной конференции ENOG 7 26-27 мая 2014 года. [Електронний ресурс]. – Режим доступу: http://www.enog.org/presentations/enog-7/268-ENOG-2014-05-MY.pdf

4.NETmundialMultistakeholderStatement: Підсумкова декларація Глобального саміту з питань управління Інтернетом. [Електронний ресурс]. – Режим доступу: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

Камран Хасілзаде
Магістр ФТ
Турал Мамедов
Магістр ФТ
Ілгин Еркан
Магістр ФТ
Державний університет телекомунікацій
м.Київ, Україна

ОСОБЛИВОСТІ ЗМІНИ ПОКРИТТЯ СЕКТОРА ШЛЯХОМ СУБСЕКТОРИЗАЦІЇ

Розглянута наступна структура антеної системи, що дозволяє проводити регулювання коефіцієнта посилення в секторі обслуговування в декількох напрямках.

Принцип дії такої антени полягає в тому, що весь сектор обслуговування (наприклад, 120°), розбивається на деяке число "субсектора" (у загальному випадку вони можуть бути не рівними один одному). На кожен з субсекторів працює своя антена з шириною діаграми спрямованості, рівний цьому сектору. Сигнали всіх субсекторівсинфазно складаються / поділяються в розподільнику (сплітер) з коефіцієнтами передачі, розрахованими індивідуально для кожного субсектора. На рис.1 проілюстрована ситуація, коли всі субсектори мають однакову ширину.

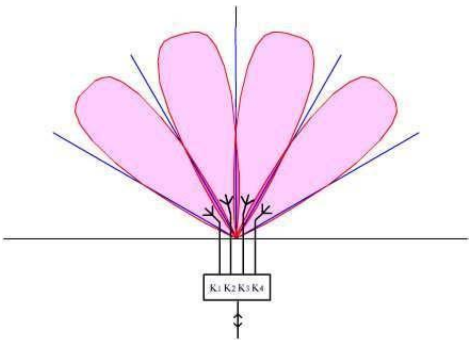


Рисунок 1 -Пелюсткидіаграмспрямованостіокремихсубсекторів

В результаті сукупна діаграма спрямованості може в певних межах змінювати свою форму (див. рис.2), що надає великі можливості для оптимізації мережі.

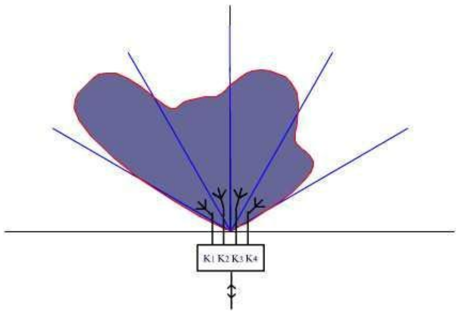


Рисунок 2- Загальна діаграма направленості субсекторизованого сектора.

У даному випадку оптимізація полягає у вирівнюванні (еквалайзінге) зон покриття окремих секторів шляхом вибору необхідних широт і направленостей окремих субсекторів і правильному налаштуванні коефіцієнтів передачі сплітера. Отриманізонипокриттяповинніскладати систему, яка максимально задовільняєнаступнівимоги:

- ширину зон перекриття слід мінімізувати до необхідої для забезпечення сталого хендофа;
- необхідно мінімізувати зони з присутністю подібних за потужності сигналів більш ніж двох секторів;
- необхідно мінімізувати внутрішні зони з недостатнім для підтримки впевненого зв'язку рівнем сигналу.

Варіантом реалізації запропонованої антеною системи може стати система, що складається зі стандартних секторних антен з вузькими діаграмами спрямованості, розташованих на одній мачті і спрямованих кожна у своєму напрямку в межах сектора обслуговування. У такому випадку необхідна діаграма реалізується вже не однією складною спеціалізованою антеною, а кількома типовими вузько направленими антенами. В даний час в асортименті ряду виробників обладнання для стільникового зв'язку (наприклад, німецької фірми Kathrein) є антени з шириною променя до 30 градусів, що дозволяє розбивати стандартний 120-градусний сектор на чотири субсектора. Більша розбиття не виправдано, оскільки, з одного боку, така точність неадекватна для розв’язування практичної задачі, а з іншого боку, антени подібного класу з ДН менше 30 градусів важко-реалізовані.

Число субсектора в секторі (тобто 2, 3 або 4) залежить від радіо обстановки в даному конкретному секторі, а також від ширини цього сектора (крім того, використання тієї чи іншої кількості субсекторів обмежено реаліями місця установки). У деяких випадках оптимальним буде розбиття сектора на нерівні частки (наприклад, 30 ° і 90 °). Може мати місце ситуація, коли взагалі не потрібно розбиття сектора, достатньо лише змінити його напрямок, нахил і, можливо, застосувати антену з іншого шириною діаграми спрямованості. Всі ці рішення приймаються в ході ітеративного оптимізаційного процесу, який проводиться на базі спеціально написаного для цієї мети програмного забезпечення CdmaOptimizer в режимі діалогу "людина-машина".

Програма CdmaOptimizer дозволяє моделювати CDMA-мережу, що використовує субсектора, розраховувати основні характеристики мережі залежно від обраної конфігурації субсектора, будувати карту покриття мережі і т.д. В якості вихідних даних для розрахунку покриття використовується інформація натурних досліджень мережі - драйв-тестів. Результатом роботи програми є конфігурація субсектора/секторів, відповідна компромісу між максимумом ємності мережі та хорошим покриттям.

Запропонований метод не вимагає розробки нового обладнання: оператор може застосовувати стандартні секторні антени, поділ сигналів може бути здійснено з використанням регульованих дільників потужності, які випускають багато виробників ВЧ-пристроїв. Зрештою, це знижує витрати оператора. Крім усього іншого, процес оптимізації мережі з використанням субсектора більш простий і наочний порівняно з випадком антен зі складною ДН, його можна робити вручну.

До недоліків рішення слід віднести деяку громіздкість антенно-фідерного обладнання, оскільки число антен зростає в число субсекторів, а розташовувати антени, з метою зниження негативних явищ ближньої зони, необхідно на якомога більшій відстані одна від одної (також бажано використовувати екрановані можливості місця установки). Цей недолік менш виражений в CDMA-системах, що працюють в діапазоні 1800 МГц

Артющик А.С.
Аспирант кафедры Комутационных систем
Государственній университет телекомуникаций

ЛОГАРИФМИЧЕСКИЕ АМПЛИТУДНО-ЧАСТОТНЫЕ ХАРАКТЕРИМТИКИ СИСТЕМЫ АКТИВНОГО УПРАВЛЕНИЯ СОВОКУПНОЙ СКОРОСТЬЮ ОЧЕРЕДИ ПАКЕТОВ В СЕТЯХ TCP/IP

Регулятор совокупной скорости **(Aggregate Rate Controller-ARC)** использует подход низкочастотных обращений для выявления перегрузок и минимизирует уровень шумов, обеспечивая более гибкую систему качества обслуживания **(QoS)** для канала по сравнению с подходами, основанными на простых очередях.

Модель **TCP/ARC** системы управления с обратной связью показана на рис.1.

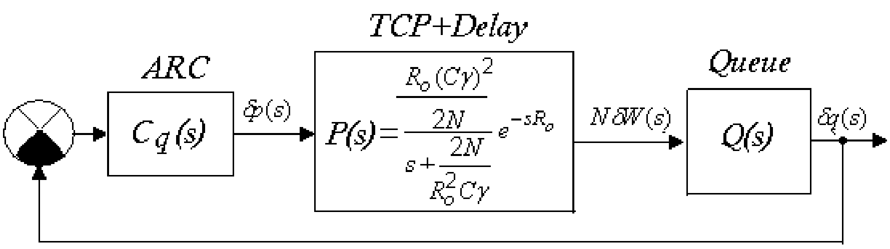


Рисунок1. Модель TCP/ARC системы управления с обратной связью, задержкой распространения, ARC-регулятором и динамикой очереди

Передаточная функцию **TCP-ARC** системы:

$$L(s)=\frac{\dfrac{\alpha(R_o\gamma C)^3(1+\gamma)}{4dN^2}\left(\dfrac{R_o}{1+\gamma}s+1\right)\left(\dfrac{R_o^2}{12}s^2-\dfrac{R_o}{2}s+1\right)}{s\left[\dfrac{R_o^3\gamma C}{2N}s^2+\left(\dfrac{R_o^2\gamma C}{2N}+R_o\right)s+1\right]\left(\dfrac{R_o^2}{12}s^2+\dfrac{R_o}{2}s+1\right)}$$

Используя пакет **Control System Toolbox 5.0** интерактивной системи **MATLAB** , определим логарифмические фазо-частотные характеристики **ЛФЧХ** (диаграммы **Bode**) системи (см. рис.1), скорректированной **ARC**-регулятором, по передаточной функции. Эти характеристики при номинальных параметрах схемы $\alpha=1{,}42\cdot10^{-5}$, $R_0=0{,}246$, 0,38 и 0,5 (сек), $\gamma=0{,}98$, C=3750 (пакетов/сек), $d=1$(сек) и числе сессий $N=100$, приведены соответственно на рис.2,3,4

Программа расчета **ЛЧХ** системы, которая скорректирована **ARC**-регулятором, может быть записана в системе **MATLAB**таким образом:

```
A=1.42*10^(-5); R= 0,246, 0,38 и 0.5; L=0.98; C=3750; d=1; N=100;
alf= A*(R*L*C)^3*(1+L)/(4*d*N^2);
f1=alf*[R/(1+L) 1]; f2=[R^2/12 (-R)/2 1];
f3=[1 0]; f4=[R^3*L*C/2/N (R^2*L*C/2/N+R) 1]; f5=[R^2/12 R/2 1];
num= conv(f1,f2); den=conv(f3,conv(f4,f5));
sys=tf(num,den); [mag,phase,w]=bode(sys);
[Gm,Pm,Wcg,Wcp]=margin(mag,phase,w); margin(sys)
```

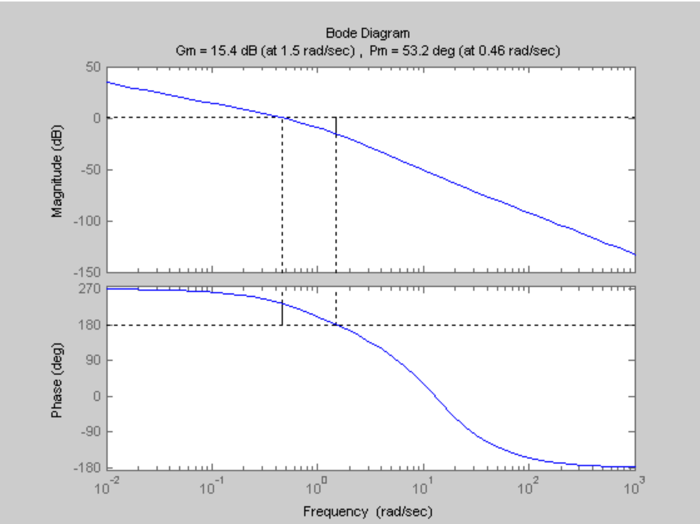


Рисунок 2 - Логарифмические фазо-частотные характеристики при R_0 = 0,246 сек для устойчивой системы

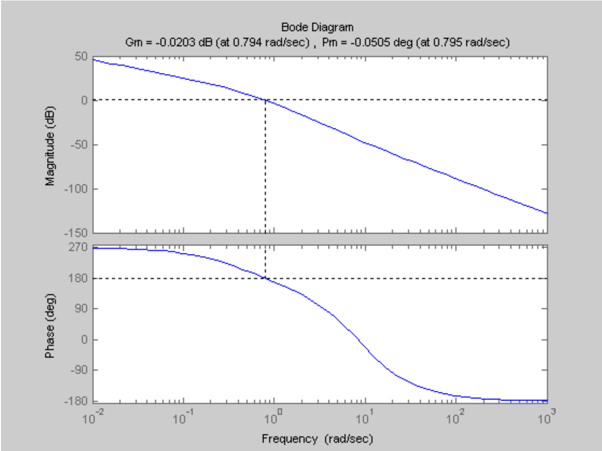


Рисунок 3 - Логарифмические фазо-частотные характеристики при R_0 = 0,38 сек для системы на границе устойчивости

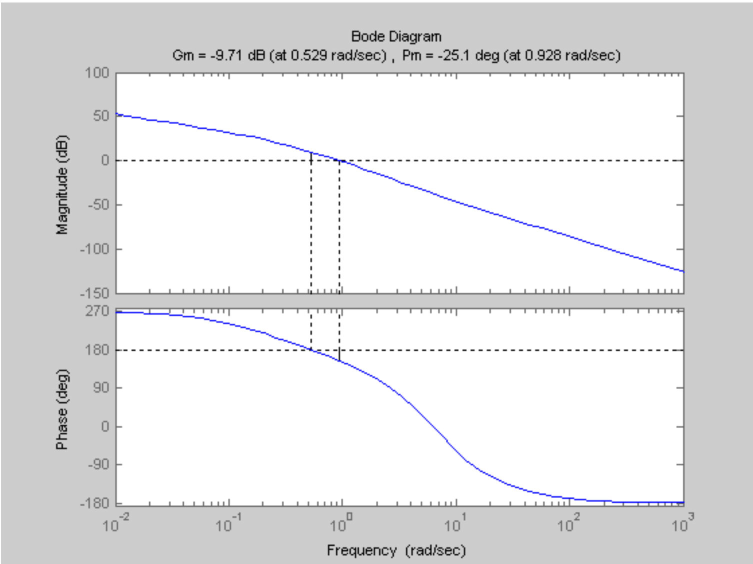


Рисунок 4 - Логарифмические фазо-частотные характеристики при R_0 =0,5 сек для неустойчивой системы

Литература:

1.Гостев В.И. Исследование AQM системы с регулятором совокупной скорости для эффективной регулировки перегрузок / В.И. Гостев, Н.И. Кунах, О.В. Невдачина, А.С. Артющик // Зв'язок. - 2013.- №2.-С. 33-37.

2.Дьяконов В.П. MATLAB 6/6.1/6.5+Simulink 4/5 в математике и моделировании. Полноеруководствопользователя. М.: СОЛОН-Пресс. – 2003. – 576 с.

3.Hollot C.V., Misra V., Towsley D., Gong W.B. “Analysis and design of controllers for AQM routers supporting TCP flows”. IEEE/ACM Transactions on Automatic Control, vol. 47, no.6, pp. 945-959, June 2002.

Андрєєва Е.П.
Ст. викладач каф. Обчислювальної техніки
Державний університет телекомунікацій
м.Київ, Україна

ЗАСТОСУВАННЯ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ПРИ ВИВЧЕННІ ГРАФІЧНИХ ДИСЦИПЛІН

Необхідність використання нових інформаційних технологій при підготовці технічних спеціалістів пов'язана з тим, що різко змінились умови праці в багатьох галузях промисловості.

Бажання кожного інженера – більше результатів при менших зусиллях – ґрунтується на прагненні звільнитися від монотонних дій, які повторюються і сконцентруватися на творчому процесі.

Висока конкурентоспроможність інженерних кадрів можлива тільки при кваліфікованій графічній підготовці та вільному спілкуванні з комп'ютером. За допомогою традиційних методів викладання неможливо підготувати сучасних високопрофесійних спеціалістів. Все це потребує нових способів навчання сучасним прийомам інженерної праці. Особливістю впровадження комп'ютерних технологій у вищу освіту є відставання методик викладання базових графічних дисциплін від рівня сучасних технічних рішень і вимог навчального процесу.

У багатьох студентів при вивченні інженерної комп'ютерної графіки виявляються труднощі в представленні просторових форм.

Поява і розвиток засобів комп'ютерної графіки відкриває для сфери навчання принципово нові графічні можливості, завдяки яким студенти можуть в процесі аналіза зображень динамічно управляти їх змістом, формою, розмірами і кольором, добиватися найбільшої наочності.

Для рішення актуальних проблем доцільно використовувати можливості останніх досягнень CAD- технологій, такі як, наочність, автоматизована побудова, робота з великими об'ємами інформації. За допомогою вдосконалення графічної підготовки при вивченні інженерної графіки пропонується використання технології тривимірного комп'ютерного моделювання з використанням CAD – систем.

При викладенні нових технологій проектування до студентів доводяться суть і перевага тривимірного твердотільного моделювання. У світі двомірного моделювання результатом проектування є креслення, з якими йде постійна робота на протязі всього циклу виробу. При тривимірному моделюванні ключовий елемент – твердотільна модель, а креслення являються лише одним із видів представлення моделі. Значно простіше уявити собі об'єкт ще до того, як він буде виготовлений.

Для тривимірного твердотільного моделювання вибрана найпрекрасніша програма AutoCad – система автоматизованого проектування, яка дозволяє в режимі діалога створювати двомірні та тривимірні моделі об’єктів, отримувати конструкторську документацію. AutoCad дозволяє успішно вирішувати актуальну задачу, яка стоїть перед викладанням графіки, із адаптації базових графічних дисциплін: нарисної геометрії і інженерної графіки – до сучасних 3D – технологій моделювання просторових об’єктів і побудови креслення.

Тривимірна графіка пакету AutoCAD володіє можливостями наочної фото-реалістичної візуалізації, дозволяючи відтворювати матеріали, моделювати світло та тіні. Створюється реалістична модель на екрані, її можна оглянути із всіх сторін, розрізати, отримати довільні розрізи, відредагувати форму. А що може бути краще динамічної об’ємної моделі, отриманої самим студентом? Уміння будувати моделі формується за два-три заняття та вдосконалюється в процесі виконання графічних завдань. Одне із самостійних графічних завдань, яке виконується на деяких спеціальностях, цікаве тим, що потрібно спочатку сконструювати деталь, яка відповідає заданим зображенням, проявивши фантазію в сполученні із просторовим мисленням та виконати побудову тривимірної твердотільної моделі(ідея використана із досвіду зарубіжних викладачів). Після створення тривимірної solid-моделі виконуються зображення - вигляди, розрізи, перерізи, необхідні для виконання креслення, майже автоматично. Системою AutoCAD необхідно керувати, щоб виконати креслення у відповідності із діючими стандартами, які вивчалися студентами раніше.

Що саме дивне полягає в тому, побудова тривимірної моделі дуже часто вимагає не більше часу, ніж розробка її плоского креслення.

Такий порядок роботи, студента дозволяє створювати твердотільні моделі різної складності. Вивчення подібного підходу проектування прищеплює майбутнім інженерам практичні навики аналіза форм об’єктів, які моделюються. Використання графіки в навчальних комп’ютерних системах не тільки збільшують швидкість передачі інформації студентам та рівень її розуміння, але і сприяти розвитку таких важливих для спеціаліста любої галузі якостей, як інтуїція, професійне ‘відчуття’, образне мислення. Ці і ряд інших можливостей комп’ютерної графіки ще слабо усвідомлені викладачами, в тому числі і розробниками інформаційних технологій навчання, що не дозволяє в повній мірі використовувати в навчальний потенціал.

Актуальним завданням навчання залишається пошук ефективних способів організації, навчально-пізнавальної діяльності студентів, використовування прогресивних та розвиткових методів та засобів навчання для реалізації планів і задач розвитку особистості, зокрема в області графіки та графічної інформації.

Дахно Н.Б.
Ст.викладач кафедри Вищої математики
Державний університет телекомунікацій
м.Київ, Україна
Барабаш О.В.
Д.т.н., завідувач каф. Вищої математики
Державний університет телекомунікацій
м.Київ, Україна

ДИНАМІЧНІ МОДЕЛІ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ КЕРУВАННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ НА ОСНОВІ ОДНОКРОКОВОГО ВАРІАЦІЙНО-ГРАДІЄНТНОГО МЕТОДА

Інтенсивний розвиток безпілотних літальних апаратів (БпЛА) за останній час привів до значного поширення переліку завдань, як у військовій, так і в цивільній сферах. Безпілотні літаки можуть бути застосовані для вирішення завдань, виконання яких недоцільно пілотованими літальними апаратами в силу різних причин. В залежності від специфіки цих завдань, вимоги до них значно відрізняються від інших.

Головна особливість БпЛА - це їх економічність при експлуатації і відсутність ризику для життя екіпажу, можливість вести спостереження і моніторинг з безлічі точок протягом короткого періоду часу. У зв'язку з тим, що запас енергії на борту легкого безпілотного літака сильно обмежений, отже, обмежено час автономного польоту, можливість використання БпЛА обмежена в цілому ряді характерних завдань.

Очевидно, що для мінімізації витрат на виконання завдань необхідно запровадження відповідної системи підтримки прийняття рішень (СППР), яка дозволяє в реальному масштабі часу розробляти оптимальну програму польоту БпЛА [3].

Основою СППР є формалізований опис - математична модель ситуації прийняття рішення. В даний час є значні успіхи в розробці і широкому практичному застосуванні математичних моделей різних класів для керування БпЛА [1]. Велике розмаїття ситуацій, що виникають при управлінні, необхідність оперативного прийняття рішень, що задовольняють різнорідним якісним вимогам, викликають необхідність комплексного використання багатого арсеналу математичних моделей і методів.

Математична модель БпЛА [2] описує рух матеріальної точки. Його рух описується системою звичайних диференційних рівнянь першого порядку або інтегро - диференційними рівняннями більш високого порядку.

Розглядаємо динамічну модель СППР для керування БпЛА, що описується диференційним виразом:

$$Au(t) = u^{(m)}(t) + c_1(t)u^{(m-1)}(t) + \dots + c_m(t)u(t) + \sum_{j=0}^{m}\int_a^b H_j(t,\xi)u^{(j)}(\xi)d\xi = f(t), \quad (1)$$

і обмеженнями:

$$U_l(u)=\sum_{j=0}^{m-1}(\alpha_{lj}u^{(j)}(a)+\beta_{lj}u^{(j)}(b))=\sigma_l,\qquad l=\overline{0,m-1},\tag{2}$$

де α_{lj} , β_{lj} , σ_l при $0\le l,j\le m-1$ сталі числа, а $c_i\in C([a,b])$, $i=\overline{1,m}$, $t\in[a,b]$

Припустимо, що оператор A є K - позитивно визначеним і K - симетричним, тобто існує оператор $K:D(K)\to L_2[a,b]$ вигляду:

$$Ku(t)=u^{(n)}(t)+a_1(t)u^{(n-1)}(t)+...+a_n(t)u(t)+\sum_{j=0}^{n}\int_a^b D_j(t,\xi)u^{(j)}(\xi)d\xi,$$

такий, що виконуються умови:

$$\exists\alpha,\beta>0\ :\ \int_a^b(Au)(t)(Ku)(t)dt\ge\alpha\int_a^b u^2(t)dt,\quad \forall u\in D(A);$$

$$\int_a^b(Ku)^2(t)dt\le\beta\int_a^b(Au)(t)(Ku)(t)dt;\ \int_a^b(Au)(t)(Kv)(t)dt=\int_a^b(Ku)(t)(Av)(t)dt,\forall u,v\in D(A)$$

Нехай існує лінійний оператор $B:D(B)\to L_2[a,b]$ і $D(B)=D(A)$:

$$Bu(t)=u^{(m)}(t)+d_1(t)u^{(m-1)}(t)+...+d_m(t)u(t)+\sum_{j=0}^{m}\int_a^b G_j(t,\xi)u^{(j)}(\xi)d\xi=g(t).\tag{3}$$

Оператор B є K - позитивно визначеним і K - симетричним і для задачі (3) просто побудувати розв`язок для довільного $g\in L_2[a,b]$, тобто існує функція Гріна для задачі $(BR_k)(t)=r_k(t),\quad t\in[a,b],\ k\ge 1.$ Тобто

$$R_k(t)=\int_a^b J(t,\xi)r_k(\xi)d\xi,\tag{4}$$

Припускаємо, що справедлива нерівність:

$$\exists\gamma,\delta>0\ :\ 0<\gamma\le\delta<\infty,\quad \forall u\in D(A),$$
$$\gamma\int_a^b(Bu)(t)(Ku)(t)dt\le\int_a^b(Au)(t)(Ku)(t)dt\le\delta\int_a^b(Bu)(t)(Ku)(t)dt.\tag{5}$$

Застосуємо до моделі (1), (2) однокроковий варіаційно-градієнтний метод [4]. Нехай $\{\varphi_i\ :\ i\ge 1\}$ система лінійно незалежних елементів. Візьмемо u_0 – довільне початкове наближення, тоді наступні шукаємо за схемою:

$$u_k(t)=u_{k-1}(t)+\tau_k R_k(t)+\sum_{i=0}^{n}\varphi_i(t)a_i^k,\quad t\in[a,b].\tag{6}$$

де τ_k деякий параметр, а $r_k=f(t)-(Au_{k-1})(t)$ – нев`язка.

Невідомі τ_k і a_i^k шукаємо з умови мінімуму функціоналу

$$F(u)=\int_a^b(Au)(t)(Ku)(t)dt-2\int_a^b f(t)(Ku)(t)dt.\tag{7}$$

Після перетворень отримуємо співвідношення:

$$\tau_k\int_a^b(AR_k)(t)(KR_k)(t)dt+\sum_{i=1}^{n}a_i^k\int_a^b(AR_k)(t)(K\varphi_i)(t)dt=\int_a^b r_k(t)(KR_k)(t)dt,\tag{8}$$

$$\tau_k \int_a^b (AR_k)(t)(K\varphi_i)(t)dt + \sum_{j=1}^{n} a_j^k \int_a^b (A\varphi_j)(t)(K\varphi_i)(t)dt = \int_a^b r_k(t)(K\varphi_i)(t)dt, i = \overline{1,n}. \quad (9)$$

З того, що оператор A є K - позитивно визначеним і K - симетричним випливає, що лінійна система (8) – (9) має єдиний розв'язок відносно τ_k і a_i^k.

Теорема: Якщо виконані умови, то варіаційно-градієнтний метод (6) – (9) збігається до розв`язку рівняння і швидкість збіжності характеризується оцінками:

$$\left\|u^* - u_k\right\|_B \le \sqrt{\frac{\eta}{\gamma}} q^{k-1} \left\|u^* - u_1\right\|_B; \quad \left\|u^* - u_k\right\|_B \le \sqrt{\frac{1}{\gamma\sigma}} \left\|B^{-1}(f - Au_k)\right\|_B, \; k \ge 2, \text{ де}$$

$$q = \frac{\eta - \sigma}{\eta + \sigma}; \quad \gamma \le \sigma \le \eta \le \delta.$$

Із схеми метода і отриманих оцінок видно, що однокроковий варіаційно-градієнтній метод має високу швидкість збіжності, стійкий і не потребують знання меж спектра оператора. Таким чином, застосування однокрокового варіаційно-градієнтного метода до динамічних СППР для задач керування БпЛА є перспективним. Це дозволить підвищити ефективність застосування безпілотних комплексів за рахунок оптимізації маршруту польоту та визначення оптимальних параметрів польоту з можливістю корегування параметрів польотного завдання в реальному масштабі часу.

Література:

1.Барабаш О.В. Модель баз знань інтелектуальної системи управління високошвидкісного рухомого об’єкта на основі її верифікації / О.В. Барабаш, Д.М. Обідін, А.П. Мусієнко //Системи обробки інформації: збірник наукових праць. – Х.: ХУПС, 2004. – № 5 (121). – С. 3 – 6.

2.Кондратьева Л.А. Обратные краевые задачи на многообразиях // Вестник Российского университета дружбы народов, Серия Математика. Информатика. Физика. 2010. №1. С.34-38.

3.Самков О.В., Сілков В.І., Гожий О.П., Мавренков О.Є. Підтримка прийняття рішень в системі управління літального апарата. // Збірник наукових праць Державного науково-дослідного інституту авіації. –2012. – Вип.8(15), С. 104-109.

4.Хорошко В.О., Дахно Н.Б. Застосування варіаційно-градієнтного методу щодо математичних моделей систем захисту інформації. //Збірник наукових праць військового інституту Київського національного університету імені Тараса Шевченка. – Київ – 2009. - Вип.19. – С.108-112.

Семенюта Н. Ф.
Почетный профессор каф. Системы передач информации
Белорусского государственного университета транспорта
г. Гомель. Беларусь

ОБОБЩЕННЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ РЕКУРРЕНТНЫХ ЧИСЕЛ

В науке, искусстве широкое использование получили рекуррентные числовые последовательности, в основе которых лежат частные последовательности чисел Фибоначчи, Люка и др. Они же, как простейшие числовые последовательности, более всего исследованы.

Начала исследований обобщенных числовых последовательностей были приведены в работепрофессора М. М. Яглома при решении задачи о разрезании квадрата [1]. В последующие годы были установлены проявления обобщенных числовых последовательностей в теории электрических цепей и др. Значительную роль обобщенные числовые последовательности играют в формировании нового направления математики – математики гармонии [2].

Целью настоящей работы является обобщение рекуррентных числовых последовательностей, которые составляют основу электрических моделей гармонических пропорций.

Обобщенная последовательность чисел. Числа формируются по рекуррентному соотношению

$$G_n = G_{n-1} + G_{n-2}. \tag{1}$$

В зависимости от значения начальных чисел G_1 и G_2 соотношение (1) порождает бесконечное множество частных числовых последовательностей, в том числе последовательности Фибоначчи, ($G_1 = F_1 = 1$, $G_2 = F_2 = 1$) и ($G_1 = F_1 =$ $=1$, $G_2 = F_2 = 2$), Люка ($G_1 = L_1 =1$, $G_2 = L_2 = 3$) и др. Если обозначить $G_1 = p$ и $G_2 = q$, тообобщенная числовая последовательность (1) примет следующий вид:

$$\begin{array}{llllllll} G_1 & G_2 & G_3 & G_4 & G_5 & G_6 & G_7 & \ldots \\ G_n(p;q) \quad p, & q, & p+q, & p+2q, & 2p+3q, & 3p+5q, & 5p+8q, & \ldots \end{array} \quad (2)$$

Из (1) следует общее правило образования последовательностей обобщенных рекуррентных чисел, в основе которых лежит основная последовательность Фибоначчи:

$$G_n(p;q) = pF_{n-2} + qF_{n-1}, \qquad n = 1, 4, 5, \ldots \tag{3}$$

где $F_n = F_{n-1} + F_{n-2}$, числа основной последовательности Фибоначчи

$$\begin{array}{l} F_n(1;1) \quad \ldots F_{-2} F_{-1} F_0 F_1 F_2 F_3 F_4 F_5 F_6 F_7 \quad F_8 F_9 \ldots, \\ \qquad\qquad\qquad -1 \quad 1 \quad 0 \quad 1\,1 \quad 2 \quad 3 \quad 5 \quad 8 \quad 13 \quad 21 \quad 34 \end{array} \quad (4)$$

Таким образом, обобщенная рекуррентная последовательность (1) состоит из двух последовательностей Фибоначчи, которые начинаются числами $G_1 = p$ и $G_2 = q$. Числа $G_1 = p$ и $G_2 = q$ своего рода гены, которые определяют значения всех последующих чисел и числовые свойства гармонических последовательностей.

В зависимости от структуры электрических моделей, последовательности обобщенных чисел можно разделить на две, с соответствующими коэффициентами:

– q-последовательность с коэффициентами q= 1, 2, 3, … и p = 1,

$$G_n(1;q) = F_{n-2} + qF_{n-1}, \qquad (5)$$

– p-последовательность с коэффициентами q= 1 и p = 1, 2, 3,…

$$G_n(p;1) = pF_{n-2} + F_{n-1}. \qquad (6)$$

Последовательностиq-чисел. В случае целочисленных значений $G_1 = p = 1$ и $G_2 = q = 1, 2, 3,\ldots$, из соотношения (5) следует:

$G_n(p;q)$ G_0 G_1 G_2 G_3 G_4 G_5 G_6 G_7 …,
$G_n(1;1) = F_n(1;1)$ p = 1 q = 1 0 1 1 2 3 5 8 13 …,
$G_n(1;2)$ p = 1 q = 2 1 1 2 3 5 8 13 21…,
$G_n(1;3)$ p = 1 q = 3 2 1 3 4 7 11 18 29 …,
$G_n(1;4)$p = 1 q = 4 3 1 4 5 9 14 23 37 …

При q = 1 образуется основная последовательность Фибоначчи $G(1;1) = F_n(1;1)$,при q = 2 – усеченная последовательность Фибоначчи $G(1;2) = F_n(1;2)$, при q = 3 –последовательность Люка $G_n(1;3) = L_n(1;3)$, при q = 4 последовательность$G_n(1;4)$ и т.д.

В рассмотренных случаях $G_1 = 1$ и $G_2 = q$ были целые числа и числа

q-последовательностей были также целыми числами. В случае, когда $G_1 = 1$, а $G_2 = q = 1/H$, т. е. дробные числа, получим последовательности:

$G_n(p;q)$ $G_0G_1G_2G_3G_4G_5G_6G_7$ …,

$G_n(1;\frac{1}{2})$ $\frac{1}{2}$(–1 2 1 3 4 7 1 1 18 29 …),

$G_n(1;\frac{1}{3})$ $\frac{1}{3}$(–2 3 1 4 5 9 14 23 37 …),

$G_n(1;\frac{1}{4})$ $\frac{1}{4}$(–3 4 1 5 6 11 17 28 45 …).

Таким образом, при дробном $G_2 = q = 1/H$ обобщенная последовательность имеет вид:

$$G_n(1;1/H)\ \frac{1}{H}\{-(H-1)\ \ H\ \ 1\ \ H+1\ \ H+2\ \ 2H+3\ \ 3H+5\ \ldots\}. \qquad (7)$$

Последовательности в скобках (7) являются p-последовательностями чисел.

Последовательности p -чисел. В случаях целочисленных значений G_2 = q= =1 и G_1 =p = 1, 2, 3, … из соотношения (6) образуются p-последовательности:

$G_n(p;q)$			G_0 G_1 G_2 G_3 G_4 G_5 G_6 G_7 …,
$G_n(1;1) = F_n(1;1)$	p = 1	q = 1	0 1 1 2 3 5 8 13 …,
$G_n(2;1)$	p = 2	q = 1	–1 2 1 3 4 7 11 18 …,
$G_n(3;1)$	p = 3	q = 1	–2 3 1 4 5 9 14 23 …,
$G_n(4;1)$	p = 4	q = 1	–3 4 1 5 6 11 17 28 …,

В случае для дробных значений p = 1/H:

$G_n(p;q)$ G_0 G_1 G_2 G_3 G_4 G_5…,

$G_n = (\frac{1}{2};1)$ $\frac{1}{2}$(1 12 35 8 …),

$G_n = (\frac{1}{3};1)$ $\frac{1}{3}$(2 1 3 47 11 …),

$G_n = (\frac{1}{4};1)$ $\frac{1}{4}$(3 1 4 59 14 …).

Таким образом, при p = 1/H и q = 1 образуется p-последовательность

$G_n(1/H;1)$ $\frac{1}{H}$ {(H–1) 1 H H+1 H+2 2H+3 3H+5 …}.

Заключение. Основным параметром, характеризующим свойства рекуррентных последовательностей чисел, являются коэффициенты q и p. Последовательность Фибоначчи (q = p = 1) – простейшие гармоническая составляющая, которая по аналогии с гармоническими последовательностями Фурье, являются основными (первая гармоника), остальные гармонические составляющие (вторая, третья, четвертая и другие гармоники и субгармоники кратны целым значениям коэффициента q и p. С числами q и p связаны также свойства последовательностей чисел, поэтому естественно их использовать для классификации рекуррентных последовательностей чисел.

Литература:

1. Яглом М. М. Как разрезать квадрат. – М.: Наука, 1968. – 112 с.

2. Семенюта Н. Ф. Обобщенные числовые последовательности типа Фибоначчи // «Академия Тринитаризма», М., Эл № 77-6567, публ.18140, 17.08.2013.

Дзядик С.Ю.
Доцент каф. Вищої математики
Жебка В.В.
Доцент каф. Вищої математики
Державний університет телекомунікацій
м. Київ, Україна

ЧИСЕЛЬНЕ ІНТЕГРУВАННЯ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ МЕТОДОМ РУНГЕ-КУТТИ

Найбільш ефективними методоми розв'язання диференціальних рівнянь першого порядку вигляду $y' = f(x,y)$ є метод Рунге-Кутти.

Існує також ряд класичних методів для визначення точних розв'язків диференціальних рівнянь $y' = f(x,y)$ при спеціальних правих частинах $f(x,y)$. Ці розв'язки можуть бути виражені елементарними або спеціальними функціями, наприклад, функціями Бесселя.

Проте практичні задачі часто приводять до диференціальних рівнянь, для яких класичні методи застосувати неможливо. Так, наприклад, в практичних задачах інколи коефіцієнти і функції, які входять в диференціальне рівняння, можуть бути задані у вигляді графіка або таблиці експериментальних даних. Метод, запропонований німецьким математиком Рунге і удосконалений Куттом, є дієвим при таких труднощах.

Метод Рунге-Кутти є однокроковим методом, тобто, знаючи наближене значення розв'язку задачі в точці$\left(x_i, y_i\right)$, визначається його значення в точці $\left(x_{i+1}, y_{i+1}\right) = \left(x_i + h, y_i + h\right)$.

Метод Рунге-Кутти узгоджується з рядом Тейлора аж до членів порядку h^n. Число *n* називається порядком методу.

При використанні методу Рунге-Кутта порядку *n* необхідно обчислювати значення функції $f(x,y)$ в *n* точках. Обчислювати значення похідних не потрібно.

Якщо права частина диференціального рівняння не залежить від *y*, тобто $y' = f(x)$, то це рівняння еквівалентне рівності $y(x) - y_0 = \int_{x_0}^{x} f(t)dt$.

При цьому виявляється, що розрахункові формули методу Рунге-Кутти збігаються з наближеними формулами обчислення певних інтегралів $\int_{x_0}^{x} f(t)dt$:

- при *n=1* (порядок методу Рунге-Кутта рівний 1) – з формулою прямокутника;
- при *n = 2* – з формулою трапецій;
- при *n = 3* – з формулою парабол (Сімпсона).

Дуже важливим при знаходженні розв'язку диференціального рівняння встановити похибку обчислень, причому зазначена похибка повинна бути мінімальною.

Розрахунок похибки методом Рунге-Кутти є дещо наближеним, оскільки значення y_{i+1} розраховуються через попередні наближені значення. Оцінку похибки було проведено за допомогою наступної формули

$$\delta_{ni} \approx \frac{\left|y_{2i} - \overline{y}_i\right|}{2^s - 1} \le \frac{\left|y_{2i} - \overline{y}_i\right|}{2^n - 1}.$$

В результаті проведених розрахунків встановлено, що частинні випадки методу Рунге-Кутти на кожному кроці розрахунку мають наступні значення похибок:

1. Метод Рунге-Кутти I порядку (метод Ейлера) – для кроку h похибка порядку не менше, ніж h^2.
2. Метод Рунге-Кутти II порядку – похибка не менше, ніж h^3.
3. Метод Рунге-Кутти III порядку – похибка не менше, ніж h^4.
4. Метод Рунге-Кутти IV порядку – похибка не менше, ніж h^5.

Метод Рунге-Кутти IV порядку найбільш часто використовується при розрахунку диференціальних рівнянь за допомогою персонального комп'ютера з використанням програмного забезпечення.

Авторами проаналізовано метод Рунге-Кутти та детально досліджено частинні випадки зазначеного методу, а саме для порядку $n = 1, 2, 3, 4$. Оцінено похибку для кожного випадку та розроблено розрахункові схеми зазначених частинних випадків методу. Розроблені лабораторні роботи, які мають на меті не лише закріпити у студентів знання з теми «Інтегрування диференціальних рівнянь методом Рунге-Кутти», а й систематизувати та алгоритмізувати зазначені знання, що допоможе студентам навчитися виділяти кроки та застосовувати знання з різних галузей при розв'язуванні технічних задач, які постають перед ними.

Ковбель М.
Студент каф.Управління інформаційною безпекою»
Державний університет телекомунікацій
м.Київ, Україна

ШЛЯХИ РОЗВИТКУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ ТА ЇХ ВПЛИВ НА ЕКОНОМІЧНИЙ РОЗВИТОК ДЕРЖАВИ

Нині формується нове уявлення про головний фактор могутності держави, згідно з яким основним чинником у XXI столітті є інформація та їїзахист. А також здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології і засоби, що дозволяють ефективно обробляти, зберігати, передавати й поширювати потрібно інформацію. Володіння державою такою здатністю - шлях до подальшого нарощування на нових засадах своєї економічної та військової міцності.

Перед Україною передусім постає завдання аналізу наявності, прогресивності передавання та захисту цієї інформації, які характеризують формування відповідної бази даних. Результати економічної діяльності зазвичай містяться в базах даних, відтворюючих реальний стан економічного розвитку держави. Такі бази даних вміщують різні обсяги інформаційних даних, які дають можливість прийняття управлінських рішень й аналізу інформаційної ресурсної бази країни. [2,с.62].

Аналіз стану інформаційної складової розвитку свідчить про безсистемність і хаотичність функціонування середовища України на даний час, яке здебільшого наповнюється недостовірною, а в окремих випадках і спотвореною інформацією.

Так, за оцінками експертів, система статистичної звітності не забезпечує отримання достовірної інформації, насамперед, це стосується сфери зовнішньоекономічної діяльності та паливно-енергетичного комплексу. Різні дані (за однаковими позиціями) щодо зовнішньої інформації оприлюднюють Державні органи України , а оцінки показників зовнішніх данних, зроблені в Україні, значно відрізняються від показників, що наводяться її зарубіжними партнерами.[6,с.91].

Відсутність безпеки та інформаційного забезпечення унеможливлює стратегічне і тактичне планування діяльності суб'єктами зовнішньо-економічної діяльності і створює умови для недобросовісної конкуренції та постійного порушення. Закритість інформаційно-економічних потоків, що циркулюють в Україні- є ще одною проблемою для стабільного розвитку. У зв'язку з відсутністю ефективних механізмів державного регулювання, багато суб'єктів господарювання працюють без знання умов ринкового середовища. Фактично галузева і відомча інформація, створена на кошти платників податків, використовується, як правило, у вузьковідомчих інтересах. Перевагу у доступі до неї отримують лише комерційні структури, утворені при багатьох державних органах, котрі безкоштовно користуються централізовано зібраною інформацією і самочинно встановлюють ціни на інформаційні послуги

Країна, яка неспроможна організувати поєднання та захист в загальну інформаційну систему надійні інформаційно-економічні потоки, що дозволяють прогнозувати і планувати складний комплекс економічного і соціального розвитку на основі досягнень науково-технічного прогресу, приречена на втрату економічної самостійності, незалежності, перетворення на сировинний придаток розвинених країн.[4,с.31]

Для розвитку та ефективного функціонування інформаційно-економічного середовища було б доцільним здійснити такий комплекс заходів:

-Організувати розробку і впровадження організаційних і правових механізмів очищення інформаційно-економічного середовища від недостовірної і спотвореної інформації.

-Визначити державні органи, їхні компетенцію і відповідальність за формування достовірної, надійної інформації для своєчасного надання її суб’єктам господарювання України.

-Забезпечити рівні умови для доступу до загальнодоступної (відкритої) економічної інформації всім суб’єктам економічних відносин, тобто до інформації, яка в розвинених країнах є суспільним надбанням

-Забезпечити захист такої інформації від зовнішніх факторів

Такі інформаційні потоки потребує застосування комплексних заходів:

-налагодження безпеки зв’язку;

налагодження надійних процедур грошових потоків, прибутків і витрат на випадок сплеску неконтрольованої інфляції;

розробка та впровадження критеріїв оцінки стану економічних об’єктів через неефективність застосування критеріїв рентабельності, які використовуються в стабільній ринковій економіці;

розв’язання проблем державного впливу на ринкові відносини в зовнішньої економічної діяльності.

Для того щоб держава могла інтегрувати у світовий ринок інформаційного забезпечення потрібно вирішити такі проблеми:

– підвищення ролі і відповідальності держави з урахуванням світового досвіду регулювання процесів інформаційно-економічної взаємодії

– впровадження комплексу правових механізмів регулювання діяльності міжнародних фінансових, економічних та інших організацій в Україні,

- вдосконалення законодавства щодо обміну технологіями,

- захисту об’єктів інтелектуальної власності.

Враховуючи світовий досвід захисту інформації, Україна повинна провести низку заходів :

– адаптувати чинне законодавство до законодавства світового досвіду;

– зняти перешкоди на шляху здійснення міжнародної інформації ;

– розвивати співпрацю з "Інформаційним суспільством" та Міждержавною координаційною радою з науково-технічної інформації;

– створити інформаційні центри при посольствах України із залученням спонсорських коштів;

організувати систему професійної підготовки з ІТ для державних службовців;

створити іномовні інформаційні ресурси про Україну;

– розповсюджувати державні видання за кордоном;

поглиблювати співпрацю з українською діаспорою;

– залучати громадські організації, незалежних експертів до обговорення проблем інтеграції України в інформаційний простір.

Впровадження вищезазначених пропозицій сприятиме задоволенню інформаційних потреб суспільства та держави, активнішому рухі України в інформаційний простір. Водночас, Україна прагнучи стати повноправним членом спільноти повинна забезпечити захист національних інтересів, зберегти власну культурну ідентичність

Таким чином, можна зробити висновок, що будь-який шлях економічного розвитку держави та практична реалізація без надійного інформаційного забезпечення та захисту цієї інформації неможливі. Гострою і актуальною проблемою сьогодення є необхідність розробки концепції державної інформаційної політики. Така концепція повинна поєднувати весь комплекс інформаційних складових в єдину цільову інформаційну систему, спрямовану на економічний і соціальний розвиток, а також забезпечення стабільності в суспільстві і державі.

Література:

1. Галатенко В.А. Основы информационнойбезопасности [Текст]/ В.А.Галатенко.– М.: Интерент-ун-т информационныхтехнологий, 2006.– 277с.
2. Иноземцев В.Л. Современноепостиндустриальноеобщество: природа, противоречия, перспективы [Текст] / В.Л.Иноземцев.– М.: Логос, 2004.– 304с.
3. Ситник Н.П. Влияниеинформации на человека/ Н.П.Ситник // Науч. и техн. библиотеки.– 2004.– №8.– С.81-84.
4. Партико З.В. Теорія масової інформації та комунікації [Текст]/ З.В.Партико.– Львів: Афіша, 2008.– 290с
5. Пономаренко В.С. навчальний посібник «Інформаційні системи в економіці» /В.С. Пономаренко// ХНЕУ.- 2001.-176с.
6. Чиж І.С. Україна: шлях до інформаційного суспільства [Текст]/ І.С.Чиж.– К.: Либідь, 2005.– 119с.

Жданова Ю.Д.
Доцент кафедри інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна
Шевчук Я. А.
Студентка навчально-наукового інституту захисту інформації
Державний університет телекомунікацій
м. Київ, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ

У сучасному світі простежується чітка тенденція розвитку платіжних систем, з кожним роком набираючи обертів, електронні гроші захоплюють сучасний ринок товарів та послуг.

Грошові розрахунки з використанням безготівкових розрахунків набагато більш вигідніз усіх точок зору. Вони значно прискорюють процес оплати, спрощують його,сприяють зниженню витрат обігу. Найбільш яскраво це видно на прикладі,коли покупець і продавець знаходяться у видаленні один від одного (у різнихмістах, країнах). Безготівкова форма розрахунків, безперечно, більш вигідна, ніжготівкова форма, але для її впровадження необхідний певний рівень розвиткутехніки, освіти, культури та багато іншого.

Обмін електронними даними (ОЕД) - це міжкомп'ютерний обмін діловими, комерційними, фінансовими електронними документами. Наприклад, замовленнями, платіжними інструкціями, контрактними пропозиціями, накладними, квитанціями і т.п.[1-3]

Окремим випадком ОЕД є електронні платежі - обмін фінансовими документами між клієнтами і банками, між банками та іншими фінансовими та комерційними організаціями.

Суть концепції електронних платежів полягає в тому, що пересилаються по лініях зв'язку повідомлення, належним чином оформлені та передані, є підставою для виконання однієї або декількох банківських операцій.

Одне з найбільш вразливих місць в системі ЕОД - пересилання платіжних та інших повідомлень між банками, або між банком і банкоматом, або між банком і клієнтом. При пересиланні платіжних та інших повідомлень виникають наступні проблеми:

- внутрішні системи організацій Одержувача і Відправника повинні бути пристосовані до отримання / відправки електронних документів та забезпечувати необхідний захист при їх обробці всередині організації (захист кінцевих систем);
- взаємодія Одержувача і Відправника документа здійснюється опосередковано - через канал зв'язку.

У свою чергу, це породжує три типи проблем:

- взаємного впізнання абонентів (проблема встановлення автентифікації при встановленні з'єднання);
- захисту документів, переданих по каналах зв'язку (забезпечення цілісності та конфіденційності документів);

Таким чином, стає актуальним питання криптографічного захисту інформації в системах електронних міжбанківських платежів. Для цього використовуються такі протоколи електронних транзакцій:

- SET(SecurityElectronicsTransaction) – протокол захищених електронних транзакцій , розроблений VisaInternational та MasterCard, спеціально призначений для захисту транзакцій в електронній комерції. Протокол SET використовує цифрові сертифікати для ідентифікації кожної сторони в електронній транзакції, включаючи покупця, продавця і банк. Захист інформації, переданої по мережі, доповнюється методами криптографії, в яких використовуються відкриті ключі.
- SSL (Secure Sockets Layer) – криптографічний протокол, який передбачає більш безпечний зв'язок. Він використовує асиметричну криптографію для автентифікації ключів обміну, симетричне шифрування для збереження конфіденційності, коди автентифікації повідомлень для цілісності повідомлень.[4]

Автоматизація та комп'ютеризація банківської діяльності (і грошового обігу в цілому) продовжує зростати. Основні зміни в банківській індустрії за останні десятиліття пов'язані саме з розвитком інформаційних технологій. Можна прогнозувати подальше зниження обороту готівки і поступовий перехід на безготівкові розрахунки з використанням пластикових карт, мережі Інтернет і віддалених терміналів управління рахунком юридичних осіб.

Література:

1. Закон України «Про платіжні системи та переказ коштів в Україні» від 05.06.2003 №906-IV(зі змінами та доповненнями)
2. Закон України «Про положення та порядок здійснення криптографічного захисту інформації в Україні» від 15.09.1998 №1019/ 98 (зі змінами та доповненнями)
3. Закон України «Про інформацію» від 02.10.1992 №48(зі змінами та доповненнями)
4. Гулак Г.Н., Мухачев В.А., Хорошко В.А., Основы криптографической защиты информации. – К.: Изд. ГУИКТ, 2009.

Пічак А.В.
Студенти ФІТ
Качайло А.Ю.
Студент ФІТ
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ НАДАННЯ ВІДЕОСЕРВІСІВ ІСНУЮЧИМИ ІНФОКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

В останні роки різко зростає попит на отримання відео інформаційних сервісів з використанням безпроводових інфокомунікаційних технологій. Існує тенденція більш високого зростання обсягу відеопотоку (в середньому на 20%), переданого з використанням безпроводових технологій відносно проводових. При цьому повноцінні можливості з надання відеоінформаційних послуг можливі для безпроводових мереж починаючи з покоління 3G.

Найбільш важливими з наведених характеристик телекомунікаційних систем в рамках надання відеоінформаційних послуг для користувачів є:

- затримка вузла доступу;
- затримка від джерела до одержувача;
- ймовірність втрат пакетів на вузлі доступу;
- завантаження вузла доступу.

Затримка при передачі статичних і динамічних зображення не повинна перевищувати 1 сек. Більш високі значення затримки призводять до помітного для користувачів погіршення якості відображуваних зображень.

Отже, існує суперечність, викликана з одного боку зростанням вимог щодо якості відеоінформаційних сервісів, а саме:

- роздільної здатності
- якості візуального сприйняття відеокадрів:
  - збільшення частоти і розмірів кадрів;
  - збільшення глибини оцифровки пікселів;
  - зниження тимчасової затримки на доставку кадрів;
  - зниження джиттера;
  - зменшення середньої затримки доставки пакетів;
  - зменшення ймовірності втрати пакетів;
  - розвиток стереододатків.

Це веде до збільшення кількості відеоінформаційних потоків; з'являються вимоги щодо мобільності відеоінформаційних послуг. З іншого боку виникають складнощі щодо надання відеоінформаційних послуг заданої якості з використанням безпроводових технологій.

Це обумовлено наступними причинами:

- відставанням темпів зростання пропускної спроможності безпровдових ІКС щодо темпів зростання інтенсивності відеотрафіка;
- недостатньою обчислювальної продуктивністю безпроводових ІКС для обробки даних;
- відносно високою ймовірністю перешкод у бітовому потоці, переданому по безпроводовому каналау зв'язку.

Це призводить до збільшення ймовірності бітових помилок і втрати пакетів у разі наявності помилок в службовій частині пакетів, що особливо посилюється для режиму передачі живого відео в реальному часі.

На основі цього можна зробити висновок, що підвищення якості надання відеоінформаційних сервісів з використанням інфокомунікаційних технологій є актуальною науково-прикладною задачею.

Стиснення відеоданих дозволяє скоротити обсяги переданих відеоданих (знизити вимоги до бітової швидкості). Це дозволяє скоротити час передачі даних у мережі, зменшити інтенсивність надходження пакетів в мережу, а отже, знизити ймовірність переповнення буфера.

При цьому порівняльний аналіз систем стиснення в різних режимах втрати якості показує, що найбільші коефіцієнти компресії досягаються для методів з втратою якості, тобто для більш низьких значень ПОСШ. З іншого боку з позиції психофізіологічних властивостей зорового апарату допускається наявність обмежених втрат якості зображень. Нижня межа спотворень відповідає рівню ПОСШ в 30дБ.

Література:

1. Чернега В.С. Сжатие информации в компьютерных сетях / В.С. Чернега. – Севастополь: Изд – во СевГТУ, 1997. – 214 с.

2. Бараннік В.В. Метод компресії трансформованих зображень у інфокомунікаціях на основі кодування векторів кортежів / В.В. Бараннік, С.В. Туренко // Наукоємні технології. – 2013. - №4. – С. 24 – 30.

3. Анисимов Б.В. Распознавание и цифровая обработка изображений: учебное пособие для студентов вузов / Б.В. Анисимов, В.Д. Курганов, В.К. Злобин. – М. : Высшая школа, 1983. – 295 с.

4. Wallace G.K. The JPEG Still Picture Compression Standard // Communication in ACM. – 1991. – V34 - №4. – P.31-34.

Гулак Г.М.
К.т.н., доцент
Професор каф. Інформаційної та кібернетичної безпеки
Складанний П.М.
Аспірант каф.Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна

ДВОСТУПЕНЕВИЙ КРИТЕРІЙ ВИЯВЛЕННЯ МЕРЕЖНИХ АНОМАЛІЙ

Виходячи з даних про щорічні темпи зростання кількості інцидентів у кібернетичному просторі можна зробити висновок про необхідність обов’язкового включення до складу комплексних систем інформаційної безпеки критичної інфраструктури автоматизованих засобів ефективного виявлення комп'ютерних атак та інших небезпечних подій, що можуть завадити кібернетичній безпеці, включаючи загрози техногенного та природного (випадкового) характеру.

Сучасні системи виявлення вторгнень СВВ (англ. *IntrusionDetectionSystems- IDS*) для досягнення цілей інформаційної безпеки здійснюють постійний моніторинг стану функціонування апаратних та програмних платформ мережевої інфраструктури та реєструють певну множину кількісних та якісних показників їх роботи $\{X_1(t), \ldots, X_N(t)\}$,де t-момент часу у який здійснюється вимірювання показника $X_k(t)$.

Зокрема, у системі *NIDES* [1] серед вимірюваних параметрів є наступні:

- використання *CPU* окремо системою та користувачем,
- час виконання процесу,
- загальний обсяг пам’яті що використана під час виконання процесу та його максимальний розмір під час виконання,
- кількість відкритих файлів під час виконання,
- кількість збоїв сторінок,
- обсяг зчитаної з диска інформації,
- кількість символів вводу/виводу під час виконання додатка,
- чи змінювалось ім’я користувача під час виконання додатка,
- час початку виконання додатка,

- кількість сигналів що отримані під час виконання додатка,
- чи виконувався додаток на віддаленої станції та ім’я цій станції,
- ім’я додатка що був використаний на віддаленої станції,
- чи виконувався додаток на локальній станції та ім’я цій станції, ім’я додатка використаного на локальній станції тощо.

Ціллю функціонування будь якої СВВ є виявлення атаки з найменшою похибкою. При цьому необхідно відповісти на наступні питання [2]:

- Що відбулось у мережі?
- Що зазнало нападу та наскільки небезпечна атака?
- Коли та звідки почалася атака?
- Хто зловмисник?
- Яким чином та внаслідок чого відбулося вторгнення?

Виклад основного матеріалу досліджень

У загальному випадку за допомогою набору показників $\{X_1(t), \ldots, X_N(t)\}$СВВ здатні виявляти деякі аномалії в роботі мережі, що ототожнюються з тими чи іншими несанкціонованими діями, та автоматично реагувати на них практично в реальному масштабі часу. При аналізі поточних подій можуть враховуватися події, які вже відбулися, що дозволяє ідентифікувати атаки, рознесені в часі, і тим самим прогнозувати майбутні події.

Ефективність роботи системи СВВ суттєво залежить від застосованого методу аналізу вихідних даних. Розрізняють наступні основні методи[1]:

- Сигнатурні методи аналізу. Цей метод заснований на тому, що більшість атак та їх сценаріїв у загальних рисах відомі. У даному підході сигнатури вторгнень визначають характерні особливості, умови, пристрої і взаємозв'язок подій, які ведуть до спроб або власне до вторгнення. Найпростішим методом реалізації сигнатурного аналізу є підтримання системою безпеки бази даних сигнатур вторгнень. Послідовність дій, виконувана користувачем або програмою під час виконання, порівнюється з відомими сигнатурами. Ознакою спроби порушення безпеки може служити часткова відповідність послідовності подій сигнатурі. Типовими представниками, що реалізовують дану ідею, є антивірусні сканери, що працюють з базою даних сигнатур вірусів і системи виявлення мережевих атак. Необхідно зазначити, що безпосереднє порівняння сигнатури вторгнення з реєстрованої активністю, малоефективне, у зв'язку з тим, що реєстровані дані, що пов'язані з атакою, часто бувають зашумлені внаслідок варіацій дій порушника під час атаки. Зауважимо, що сигнатурний метод вторгнення припускає використання методів штучного інтелекту. Сигнатурні методи виявлення вторгнень використовують: експертні СВВ, СВВ на основі моделі, СВВ шляхом аналізу переходів системи з одного стану в інший, СВВ на основі зміни станів та мережі Петрі. Сигнатурний методи мають такі переваги: кількість і тип подій які необхідно контролювати обмежені даними, визначеними в сигнатурах, аналіз є достатньо швидкім, оскільки в ньому відсутні обчислення з плаваючою точкою над великими обсягами даних характерні для статистичного аналізу.

- Статистичні методи аналізу. До переваг статистичних методів відноситься: використання для виявлення атак класичних статистичних методів з добре розвиненою теорією, безліч контрольованих змінних не вимагає великого об'єму пам'яті при зберіганні, статистичні методи можуть використовувати час як параметр при аналізі, легко виявленню просте відхилення в поведінці користувачів. До недоліків статистичних методів відносять проблеми з формуванням статистики звичайної поведінки користувачів.
- Навчання в системах виявлення порушника. До них відносяться: навчання на класифікації прикладів, нейромережі та генетичні алгоритми. Використання традиційних методів навчання при побудові СВВ не позбавлене недоліків.

Література:

1. Корт С.С.Методы обнаружения нарушителя,
http://www.uran.donetsk.ua/~masters/2011/fknt/brich/library/article6.htm
2. Костров Дм. Системы обнаружения атак.
http://www.bytemag.ru/articles/detail.php?ID=6608

Дмитрук С.А.
Доцент каф. Соціології та гуманітарних дисциплін
Державний університет телекомунікацій
м. Київ, Україна

ТРАДИЦІЙНО-ПОБУТОВА КУЛЬТУРА ЧЕХІВ В УКРАЇНІ

Чехи селилися на території України з XIII ст. переважно у Галицькому князівстві. У XV–XVI ст. в українських землях, захоплених Польщею, чехи несли охоронну службу на польско-молдовському кордоні. Чехи були пов'язані з українським козацтвом і брали участь у його організації. Однак масове переселення чехів в Україну розпочалось у 1860-х – на початку 1870-х рр. Тривало переселення до початку XX ст. Чеські села з'являються у Волинській, Подільській, Таврійській, Херсонській губерніях.

Локальне проживання, особливо в сільській місцевості, сприяло збереженню традицій у сфері матеріальної культури. Основне заняття чехів – землеробство. Городництво і садівництво мали підсобний характер. Займалися чехи і тваринництвом. Тримали корів, коней, свиней, птицю. Худобу пасли на громадських пасовищах. Особливе місце у чехів займала реміснича діяльність. Практично кожен чех міг виготовити найпростіші сільськогосподарські знаряддя праці, кухонне начиння, прості й необхідні меблі. Серед чехів було багато професійних ремісників: шевців, кравців, столярів [1, с. 316–365].

Чеські поселення були вуличного типу, і тільки деякі мали риси однорядних будівель. У центрі села знаходився костьол, церковно-приходська школа, будинок сільської адміністрації. В якості будівельного матеріалу використовували дерево та глину. З глини робили сирцеву цеглу. Глина входила до складу розчину для скріплення цегли й «мазаної» підлоги. У деяких будинках підлога викладалася обпаленою цеглою. Фундамент робився з сирцевої цегли або каменю. Дах покривався соломою і будувався двосхилим. На фасаді прорубувалися два вікна для провітрювання і проникнення світла. Над вікнами робилося невелике заглиблення, де містилося скульптурне зображення святого, наприклад, Святого Йосифа. Стеля житла робилася дощатою, з двох рядів дощок. Зверху дошки обмащувалися глиною з соломою. Тримали цю конструкцію балки, виготовлені з дуба та оброблені спеціальним розчином. На горищі зберігали зерно, м'ясні вироби, картоплю та ін. Будинок огороджувався парканом. На території двору розташовувалися необхідні господарські будівлі (хлів, комора). До садиби також належали невеликий дворик, город і криниця. Будинки чехів – трьохроздільні: сіни, хата, комора. Пізніше сіни стали перегороджувати і з'являлося ще одне приміщення – кухня. Із сіней будинку сходи йшли на горище. Хата – кімната для гостей – простора і світла з вишивками й картинами релігійного змісту, скульптурними зображеннями святих. Комора була господарським приміщенням, де зберігалися продукти, одяг, дрібні господарські предмети. З 20-х рр. XX ст. стало змінюватися планування. З'являється простора веранда, передпокій, кухня-комора, парадна кімната – зала, спальня [2, с. 7–36].

У кухні чехів головне місце займали борошняні страви. Це, перш за все, кнедлики, з прісного і кислого тіста. Борошно використовувалося для приготування локшин – нудле і різного виду випічки. Вироби з тіста готувалися до кожного сімейного та календарного свята – бухти (булочки), калачі, струдлі. Чехи споживали переважно білий хліб, причому в невеликій кількості. Значну частину раціону становили молочні та м'ясні страви. З молока робили сметану, масло, сир. Серед м'ясних продуктів найбільш поширеним було м'ясо птиці та свинина. З м'яса готували ковбаси, копчені окости. Улюбленими напоями чехів були пиво і виноградне вино. Особливі блюда готували під час календарних свят. У день Святого Мартіна смажили гусака, пекли «мартінські рогалики». У день Святої Барбари і Святого Мікулаша – кренделі й інші фігурні вироби з борошна. Серед закусок були різноманітні салати. Багато закусок зі спаржі, кольорової капусти, грибів. Широко застосовувалися різноманітні спеції і пряні овочі – імбир, майоран, кмин, селера, мускатний горіх, цибуля, перець.

Для чеського жіночого національного одягу характерні довгі сорочки, із зібраними рукавами і коміром, корсет або ліф, зшиті в талію, зі шнурівкою спереду. Спідниці були дуже широкі, збористі, під них одягали декілька нижніх спідниць. Спереду пов'язували дуже широкий зі зборками фартух. На плечах носили хустку, схрещену на грудях. Головний убір заміжніх жінок – маленькі твердо накрохмалені очіпки, дівчата носили полотняну вишиту смужку. Взуттям були черевики, панчохи носили червоні, пізніше білі. З овчини шили кожушки. Чоловічий традиційний одяг – вовняні або шкіряні штани, довжиною до колін, сорочка з довгими рукавами й манжетами, хустка на шиї та святковий жилет. Верхній буденний одяг шили дуже коротким. Одружені чоловіки у свято одягали довгий каптан, темного кольору з фалдами і ґудзиками в кілька рядів. На ногах носили черевики або високі чоботи. Панчохи були вовняними, синіми або білими. Головними уборами були шапки з хутряною облямівкою або капелюхи. Більшість чеських переселенців їхало в Україні з промислово розвинених областей Чехії, де вже був поширений міський європейський костюм. В Україні одяг шився з фабричних тканин або купувалася в містах [3].

Етнічна специфіка чеського населення України збереглася, перш за все, у сфері духовної культури. Важливою подією в житті родини було весілля. Влаштовували весілля восени, після збирання врожаю, рідше навесні на Масницю. Весільний обряд складався з декількох етапів: вибір нареченої, сватання, змова (заручини), передвесільні приготування, вінчання, весільний бенкет, післявесільні обряди. На весілля запрошувалися всі жителі села. Святкування тривало три дні. У чеському весіллі дотримувалися традиційного складу весільних чинів – Дружба (сват), Стара Сварбія (родичка нареченої, обов'язково щаслива в шлюбі), дружки і дружечки (в чеській традиції вони називалися младенці і маршалки). Після вінчання відбувався обряд «очіплення» (процес знімання весільного вінка з нареченої). Після весілля наречена переїжджала до нареченого. Через 5–7 днів після весілля молоді, Дружба, Стара Сварбія, дружки та дружечки відвідували будинок батьків нареченої. Після нетривалого сімейного обряду молода забирала своє придане. Нова сім'я в результаті відокремлювалася від батьків і будувала свій будинок[4, с. 171–182].

Із народженням дитини пов'язані найдавніші обряди. Введення – матір вводили в костьол, де здійснювався відповідний обряд охорони та очищення породіллі (через 6 тижнів після народження дитини). Після відвідування костьолу, жінка брала участь у святковому обіді. Обряд хрещення новонародженого здійснювався в костьолі з хрещеними батьком і матір'ю, яких вибирали батьки з найближчих родичів. Авторитет батьків у сім'ї був незаперечний. З малих років дітей привчали до праці. Дівчатка допомагали вести домашнє господарство – готувати, вишивати. Хлопчиків брали в поле на посівну і збирання врожаю, вчили запрягати коня, лагодити інвентар.

За віросповіданням чехи України в основному були католиками. Серед календарних свят етнічну специфіку зберігали: день Святого Мікулаша (Миколи, 6 грудня), Різдво (25 грудня), Великдень (Веліконац), Хресні дні (Кшизові дні) і свято урожаю (обжинки, посвіцані). У літній період великих свят не було, що було пов'язано з польовими роботами. Різдвяні свята починалися Святвечором. Чехи називають різдвяний Святвечір Щедрим. З першого різдвяного вечора чи дня Святого Стефана починалося колядування. Після дня Святого Яна – 27 грудня – можна було починати працювати. Новий рік збігався з днем Святого Сильвестра. Зимові календарні торжества включали свято «трьох королів» чи Водохреща (6 січня). 2 лютого святкувалося Стрітення (Громиця). У березні починався 6-тижневий великодній піст, що вираховувався за церковним календарем. Під час посту відзначали два свята: 19 березня – день Святого Йосифа, і 25 березня – Благовіщеня. Напередодні Великодня, суботнім вечором уся родина йшла в костьол на вечірню, потім влаштовувалася святкова вечеря («розговіння»). Святковому столу приділялася особлива увага. Головними блюдами були «чеські паски», фарбовані яйця, що викладалися навколо пророслого ячменю. Після Великодня йшов провідний тиждень. П'ятий тиждень після Великодня – Хресні дні (Кшизові дні). На 40-й день після Великодня святкували Вознесіння, потім через один тиждень – Трійцю. У четвер після Трійці – свято Божого Тіла. 15 серпня (за ст. стилем) відзначали Успіння. Осінні свята починалися з 8 вересня (за ст. стилем) – Різдва Богородиці. Після збирання врожаю в чеських селах проходило свято врожаю (обжинки, посвіцані) Закінчувався рік за церковним календарем святом усіх святих – 1 листопада [5].

Література:

1. *Дмитрук С.А.* Чехи на Півдні України. В кн.: Історія чехів в Україні. – К., 2013. – С. 316–365.

2. *Волкова С.А.*Чешская эмиграция в Крым и основание колоний во второй половине XIX века. В кн.: Чехи в Крыму: Очерки истории и культуры. Симферополь, 2005. – С. 7–36.

3. Традиційно-побутова культура очима старожилів: За матеріалами етнографічних експедицій: Чехи. В кн.: Етнокультурний ландшафт Північного Приазов’я. – Запоріжжя–Мелітополь–Сімферополь,2004. – 276 с.

4. *Наулко В.* Чехи в Україні. В кн.: Під одним небом: Фольклор етносів України. – К., 1996. – С. 171–182.

5. *Волкова С.А.* Чехи на півдні України: друга половина XIX – перша третина XX століття. – Сімферополь, 2006. – 160 с.

Харечко І.З.

Асистент каф.Теорії та історії політичної науки

Львівський національний університет імені Івана Франка

м. Львів, Україна

НООПОЛІТИКА ЯК АЛЬТЕРНАТИВА СУЧАСНОЇ ПОЛІТИКИ УКРАЇНИ

У другій половині ХХ ст. сильна влада вимірювалася кількістю ядерних ракет і танків, обсягом промислового потенціалу, чисельністю чоловіківзі зброєю в руках. У 2000-х роках природавлади, що визначається як здатністьвпливати на інших, щоб отримати бажані результати, різко змінилася.Влада перестала бути статичною субстанцією; її історія – це історія зрушень іінновацій,технологійі відносин [7, с. 27].

При тенденціях розвитку сучасного світу, коли інформація стала інструментом влади, національна безпека України суттєвим чином залежить від забезпечення інформаційної безпеки, і в подальші роки із досягненнями технічного прогресу ця залежність зростатиме. Важко не погодитися із твердженням С. Ніконова, що «пряме використанняінформаціїяк засобуманіпулювання свідомістюміжнародної громадськостіможепризвести до крахувлади втих чи інших регіонахсвіту, що, у свою чергу,може змінитисучаснугеополітичну картусвіту» [3].

У 1999 році зявляється термін «ноополітика», котрий американські спеціалісти у сфері оборони Дж. Арквілла та Д. Ронфелдт вживають у прив’язці до концепту «м’якої сили». Вони розуміють це нове поняття як геополітика, що базується на системі знань та використанні інформаційних мереж [5].

Хоча термін спочатку з’явився у зв’язку з концепцією США «Революція у військовій справі», ноополітика також використовується в економіці знань як засіб досягнення політичних цілей та здобуття політичної ваги на міжнародній арені за рахунок знань, інновацій, результатів наукових досліджень. Ноополітика може бути визначена як використання інновацій і знань, щоб отримати максимальну користь від політичних зносин на міжнародному рівні. Такий «гонка знань» може бути засобом обстоювання політичної незалежності або генерування потенціалу для перерозподілу геополітичного балансу влади [7, с. 28]. Таким чином, ноополітика – це досконаліша модель формування та реалізації зовнішньої політики держави, що спирається на знання й загальнолюдські цінності.

Під даним поняття розуміють також форму політичного керівництва, яка необхідна для взаємодії з ноосферою – найширшим інформаційним простором свідомості, у якому об'єднані кіберпростір (або «мережа») та інфосфера (кіберпростір плюс засоби масової інформації).

Нооплітика – це метод реалізації зовнішньої політики в інформаціологічну епоху, яка підкреслює першість ідей, духовних цінностей, моральних норм, законів і етики, яку засновано на застосуванні м'якої сили, а не твердої сили [2]. За останні500років все світові державиздобували гегемонію саме через використання жорсткоїсили. На думку окремих дослідників, США є прикладом держави-гегемона, котра займає лідируючу позицію на міжнародній арені завдяки поєднанню підходів «жорсткої» та «м'якої сили».Стратегія глобального панування СШАпобудована на популяризації в інших країнах своїх цінностей, своєї політичної системи,свого визначеннядемократії, свободі прав людини, та пропагування їх як універсального світобачення [4].

На думку дослідника І. Аберкейна, ноополітика стала визначальноюпозицією для Китаю у проведенні економічної політики. Він відзначає трансформування політики КНР від «панацеї зростання» до «панацеї знань» [4], тобто успіх економічного розвитку пов'язують не із демографічними показниками країни, а із інтелектуальним розвитком, людськими ресурсами, науково-технічними досягненнями.

Російський дослідник С. Ніконов вказує на загрози для супільста, котрі не виключені при впровадженні концепції ноополітики у суспільно-політичні відносини держави. Він трактує дане поняття, як інформаційнустратегіюз маніпулюванняміжнароднимипроцесами за допомогою формуваннячерез засоби масової інформаціїу громадськостіпозитивногочи негативного ставленнядозовнішньої і внутрішньої політикидержави абоблокудержавз метою створенняпозитивного або негативногоіміджуідей іпропагованихморальних цінностей [6].

З точки зору ноополітики, найбільшу силу у сфері зовнішньої політики мають неурядові організації, що представляють громадянське суспільство. Роль держав у розв'язанні глобальних проблем відтак зменшується, а недержавні структури все більше набувають вирішального впливу. Реалізація концепції ноополітики передбачає можливості для суспільства стежити за подіями в усьому світі, володіючи достовірною інформацією. Це стає можливим завдяки діяльності ЗМІ, мережі неурядових організацій, окремих активістів, котрі проводять моніторинг і складають зразки того, що вони думають стосовно всіх глобальних проблем, організовують відкриті онлайн форуми тощо, виготовляючи і поширюючи таким чином вільну (громадську) інформацію [2]. Тобто, ноополітика виступає як засіб соціального контролю за міжнародною політикою.

Можливість вільно поширювати інформацію сприяє прийняттю саме консенсусних рішень за рахунок залучення до своєї позиції інших гравців світової політики. Держава, дотримуючись принципів ноополітики, намагається привернути увагу до проблеми та переконати у застосуванні невійськових методів для її розв'язання. Тому коли сторони визнають загальнолюдські цінності, а не тиск, військові методи, насилля, це зумовлює новий підхід до врегулювання конфліктних ситуації та формує нову парадигму міжнародних взаємодій.

Національні інтереси, сформовані в рамках державності, не можуть виступати засадничим принципом реалізації ноополітики. Інтереси держави повинні визначатися в загальнолюдському контексті, з врахуванням більш ширших, глобальних потреб.

Як і будь-яка теорія, практична реалізація концепту ноополітики обумовлюватиметься багатьма факторами, що призводитиме до модифікації ключових положень. Дослідник С. Гріняєв припускає, щоноополітіка має найбільше шансів прижитисятам, де домінують високорозвиненісуспільства:наприклад, частиниЗахідної Європи таПівнічна Америка.Але вона будеменш ефективнатам, деумови залишаютьсятрадиційноорієнтованимина державу,а нена громадянське суспільство, і таким чином заснованимина продовженнязастосування методівтрадиційної політики.Крім того,ноополітікабуденайбільш ефективнатам,де присутні всіспособи поширенняінформації, неурядові організаціїмають пріоритету залученні увагидо проблем іпри цьому саміпроблемикомплексні,ане однорідні(строгоекономічні, політичніабовійськові), а також там,де добреналагодженийпроцес взаємодіїдержавних і недержавнихструктур [1, с. 19].

Література:

1.Гриняев С. Н. Поле битвы-киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Мн.: Харвест, 2004. – 448 с.

2.Коломієць В.Ф. Формування ноополітичних технологій – атрибут інформаціологічного розвитку цивілізації / В. Ф. Коломієць // Проблеми міжнародних відносин. – 2010. – Випуск 1. – С. 120-131.

3.Никонов С.Б. Глобальное информационное пространство как среда формирования ноополитики / С.Б. Никонов // Мир и политика. – 2012. – № 09(72). – Режим доступу:http://mir-politika.ru/1608-globalnoe-info...oopolitiki.html (19.10.2015).

4.Aberkane I.J. An optimistic memo on the Chinese noopolitik: 2001-2011 / I.J. Aberkane // E-international relations. – 2011. – Jun. 14. – Mode of access: http://www.e-ir.info/2011/06/13/an-optimistic-memo-on-the-chinese-noopolitik-2001-2011/(19.10.2015).

5.Arquilla J. The emergence of noopolitik: toward an American information strategy / J. Arquilla, D. Ronfeldt. – Santa Monica: RAND, 1999. – 102 p. – 6.Mode of access: http://www.rand.org/pubs/monograph_reports/MR1033.html (19.10.2015).

7.Baichik A.V. Noopolitik as global information strategy / A.V. Baichik, S.B. Nikonov // Vestnik St.Petersburg University, Ser. 9. 2012. Issue. I. p. 207-213

Nye J. The Future of Power / J. Nye. – Public Affairs, 2011. – 300 p.

Odarenko O. V.
Senior teacher of department of journalism and new media,
The Kiev university of Boris Grinchenko
Kiev, Ukraine

ACTUAL TRENDS OF THE RISK MANAGEMENT OF TELECOMMUNICATIONS

The analysis of modern development of telecommunications testifies to a significant amount of the risks accompanying business in this sphere. Actual the risk trends for telecommunication sector of economy can be reconstructed on the basis of annual reports and researches of the main players in the market risk consulting – analytical and rating agencies, the consulting and auditor companies, insurance companies, experts of the market of telecommunications.

However, first of all, it is necessary to rely on researches of large players of the market risk consulting.

It is the Marsh company founded in 1845 and specializing on risk consulting; the companies big "the consulting four" - Bain & Company, BCG (The Boston Consulting Group), McKinsey & Company, Oliver Wyman and the company big "the auditor four" - Deloitte Touche Tohmatsu Limited, EY (till 2013 the company was called Ernst & Young), KPMG, PWC (PricewaterhouseCoopers).

On the basis of analytical reports of the specified companies we will allocate the main trends of a risk management of telecommunications in 2016:

-Strengthening of turbulent tendencies in the market of telecommunications.

-Need of new investments in infrastructure, in connection with the exponential growth of smartphones, falling of the income from "voice" and increase in the income from a mobile Internet traffic.

-The risks connected with profitability of investments, first of all, with introduction 4 G and 5 G.

-Decrease in volume of telecommunication services.

-Destruction of monopoly for the subscriber.

-Uncertainty of regulatory policy.

-Ensuring principle of "a network neutrality".

-Low level of business analytics in the telecommunication sphere.

-Lack of the productive business models focused on new types of communication and new scenarios of creation and rendering of services.

-The hardly predicted and controlled processes in the market of paid TV, first of all, mass transition of subscribers to new OTT-services.

-The risks connected with development of satellite technologies by criminal and terrorist community.

-The risks connected with introduction of new business models in the field of "cloudy decisions". This range of risks is in many respects connected with completion of decisions "under the specific client" and emphasis on self-service.

-The risks connected with development of a number of the directions of cloudy technologies - M2M (machine-to-machine) and IoT (Internet of Things). First of all, it is the risks connected with safety.

-Imperfection of a legal framework in respect of information security.

This range of actual risks forces the telecommunication companies to pay special attention to improvement of forecasting and management of both strategic and operational risks, and financial and risks connected with the legislation. In particular, the specified risks compel the companies to reconsider operational structure, to develop system of the reporting for the purpose of increase of effective management of client service, and also to develop the decisions connected with "new" consumer inquiries.

In our opinion, it is necessary to introduce the smart risk management based on short-term and long-term business and technological forecasts. Such risk management has to be incorporated in flexible structure of the company (now analysts note rigidity of organizational structures of the telecommunication companies). We offer the author's term "smart risk management" describing some sets of procedures for risk management which the company can apply to minimization / elimination of actual risks.

Essence of a smart risk management – in its efficiency. Speed of an assessment and elimination of risks is one of the main criteria of effective system of a risk management now.

Шевченко С.М.
К.п.н., доцент кафедри вищої математики,
Шаговий О.В.
Студент групи КСД-21
Державний університет телекомунікацій
м. Київ, Україна

МАТЕМАТИЧНІ КОМПЕТЕНЦІЇ СПЕЦІАЛІСТІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сучасні інтерактивні технології, що забезпечують отримання швидких адекватних відповідей на дії людини, можуть продуктивно використовуватись у навчально-виховному, а також освітньо-кваліфікаційному процесі з метою розвитку швидкої реакції, вмінь адекватно діяти в екстремальних умовах, швидко знаходити відповіді, формулювати запитання, висувати гіпотези та генерувати ідеї.

Інтерактивні графічні системи, імітатори експериментів, інформаційно-моделюючі системи при дидактично правильному застосуванні сприяють формуванню аналітичного мислення, розвитку конструктивної уяви, проектувальних навичок, вмінь чітко та правильно подавати результати виконання дій, вміння аналізувати, критикувати та оцінювати змістові та числові характеристики моделей об'єктів і явищ. За допомогою перелічених систем здобуття необхідної інформації вже не є проблемою, що значно впливає на наукові сфери, у тому числі у всі галузі математики. Використання електронних посібників, репетиторів через Інтернет, мережевих дидактичних засобів дозволяє інтенсифікувати пошук дослідження проблеми, знаходити загальний алгоритм розв'язання різного роду задач, формує нові навички орієнтації у просторовій, часовій, комунікативній сферах.

Сучасні інформаційні технології увібрали в себе лавиноподібні досягнення електроніки, а також математики, філософії, психології та економіки. Утворений в результаті життєздатний гібрид ознаменував революційний стрибок в історії інформаційних технологій. Виробництво і транспорт, банки та біржі, засоби масової інформації і видавництва, оборонні системи, соціальні та правоохоронні бази даних, сервіс і охорона здоров'я, навчальні процеси, офіси для переробки наукової та ділової інформації, нарешті, Інтернет – усюди інформаційні технології. Інформаційна насиченість не тільки змінила світ, а й створила нові проблеми, які не можна було передбачити. Сучасне суспільство просто переповнене потоками інформації, які безсумнівно потребують обробки. Через це без інформаційних технологій, так само як без енергетичних, транспортних і хімічних технологій, наше суспільство, а також сучасні науки нормально функціонувати не можуть і не будуть.

Успішна робота сучасного спеціаліста інформаційних технологій немислима без ґрунтовних знань математичних дисциплін: математичного аналізу, лінійної та аналітичної геометрії, дискретної математики, теорії ймовірностей та математичної статистики. Тому особливе місце серед фахових компетенцій спеціалістів інформаційних технологій посідають математичні компетенції. Математична компетентність – це здатність розвивати та використовувати математичне мислення для того, щоб вирішувати ряд проблем у повсякденних ситуаціях [1]. Математична компетентність – це вміння бачити та застосовувати математику в реальному житті, розуміти зміст і методи математичного моделювання, вміння будувати математичну модель, досліджувати її методами математики, інтерпретувати отримані результати, оцінювати похибку обчислень [2]. Математика – один з основних інструментів побудови абстрактних моделей програмних конструкцій і навіть цілих систем.

Кожний спеціаліст інформаційних технологій має володіти наступними уміннями: виконувати елементарні операції над числами (додавання, віднімання, множення, ділення); знаходити остачу від ділення; розуміти природу парних та непарних чисел; виконувати дії з відсотками; дії з комплексними числами; розуміти десяткову, двійкову та шістнадцяткову системи числення; будувати системи координат; виконувати дії з матрицями та векторами та інші.

Це короткий список, який потрібно застосовувати доволі часто, і його можна доповнювати або відкидати деякі пункти. Усі інші знання математики дуже сильно залежать від тієї задачі, над якою буде працювати майбутній ІТ спеціаліст. Тому, якщо ви вже володієте цим мінімумом, можна сміливо переходити до практики у тій сфері, в якій працюєте. А далі, добувати ті знання, які допоможуть покращити і полегшити роботу.

Є цілий ряд високотехнологічних задач, які вимагають знань вищої математики. Ось кілька напрямків, в яких без знань вищої математики буде важко працювати: 2d/3d графіка; криптографія; аналіз даних та прогнозування; розпізнавання моделей: зображень, аудіо, відео; штучний інтелект, нейронні мережі, машинне навчання.

У різних напрямках програмування використовуються зовсім різні області математики. Зазвичай приходиться надолужувати і довчатись безпосередньо для того чи іншого проекту.

Таким чином, інформаційні технології та математика є взаємопов'язаними, але незалежними між собою, оскільки вони впливають один на одного та тим чи іншим чином полегшують та систематизують інформацію, працю ІТ-спеціалістів та математиків-науковців.

Література:

1.Ключові компетентності для освіти впродовж життя усього – Європейські рекомендації [Електронний ресурс]. – Режим доступу: http//www.loippo.lviv.ua/fusion/uploads/Rec-EP

2.Раков С. Формування математичних компетентностей випускника школи як місія математичної освіти / С. Раков // Математика в школі. – 2005. - № 5. – С. 2 – 7.

Кірієнко О.Д.
Аспірантка каф. Теорії та історії політичної науки
Львівський національний університет імені Івана Франка
м.Львів, Україна

СУЧАСНІ МЕХАНІЗМИ КОНСТРУЮВАННЯ ПОЛІТИЧНОЇ ІДЕНТИЧНОСТІ В КОНТЕКСТІ ТЕОРІЇ СОЦІАЛЬНОГО КОНСТРУКТИВІЗМУ

Свідомість індивіда є інтенційною. Різні системи об'єктів викликають у свідомості відмінні враження із відповідним рівнем уваги, що дає можливість говорити про велику кількість реальностей, серед яких можемо виокремити і політичну. Політична реальність є цілісною і характеризуються нормативними, емоційними та когнітивними компонентами, має свою інституційну будову та передбачає апарат її легітимації, що супроводжується ритуальними та матеріальними символами. Головним елементом політичної реальності є її структура – сума типізацій і створених відповідно до них зразків взаємодій (котрі повторюються)[1, 91].

Політична реальність та політична ідентичність – діалектично пов'язані між собою та конструюється через процеси екстерналізації, об'єктивації та інтерналізації. Екстерналізація – процес накладання суб'єктивних значень на простір реальності, своєрідний процес іменування. Об'єктивація – процес, через який екстерналізовані продукти людської діяльності набувають характеру об'єктивності. Інтерналізація – процес через який об'єктивований політичний світ отримує відображення у свідомості індивіда в ході вторинної соціалізації. Отже, політична ідентичність постає як елемент суб'єктивної реальності індивіда, що виникає внаслідок інтерналізації структури політичної реальності, її інституційного та легітимаційного компонентів у свідомість індивіда, через процес вторинної соціалізації.

Знання визначається серцевиною фундаментальної діалектики суспільства і виконує різноманітні функцій: формує мотиваційну динаміку інституціоналізованої поведінки, визначає інституціоналізовану сферу поведінки і все, що потрапило у її рамки, визначає та контролює ролі. Знання здобувається в процесі соціалізації і опосередковує об'єктивовані структури соціального світу, в процесі інтерналізації в рамках індивідуальної свідомості [3, с.107].

Вторинна соціалізація представляє собою інтерналізацію структури реальності, вимагає «вивчення» певного специфічно-рольового словника, а також інтерналізації семантичних полів, що структурують інтерпретації і поведінку в рамках конкретної інституційної сфери. Актуальною сьогодні постає проблема успішності вторинної соціалізації крізь призму поширення феномену індивідуалізму. Явище «індивідуалізму», тобто індивідуального вибору між різноманітними реальностями та ідентичностями прямо пов'язане із можливістю неуспішної соціалізації. «Індивідуаліст» виникає як специфічний соціальний тип у якого є потенціал для міграції по великій кількості доступних реальностей. Він добровільно і свідомо конструює «Я» із «матеріалу» різноманітних доступних йому ідентичностей, проте подібний конгломерат досить часто не має підкріплення з боку конкретної структури, що і провокує його швидке розсипання.

На прикладі проблем успішності соціалізації ми можемо спостерігати динаміку відчуження. На рівні вторинної соціалізації в якості суб'єктивної можливості вибору з'являється велика кількість альтернативних реальностей та ідентичностей. Звичайно можливості вибору є обмеженими соціально-структурним контекстом індивіда. Коли диференційованість вторинної соціалізації досягає моменту де можливий суб'єктивний відрив ідентичності від власного місця у суспільстві, а соціальна структура в той же час не дозволяє реалізувати суб'єктивно обрану ідентичність формується певний тип відчуження. Суб'єктивно обрана ідентичність стає фантастичною – вона об'єктивується у свідомості індивіда як дійсне «Я» (основою для них виступають наприклад нереалізовані мрії). Проте, індивіди займають соціальні позиції згідно суб'єктивного досвіду і тільки – як наслідок вони можуть бути абсолютно соціально байдужими до різних соціально-політичних перетворень. Широке поширення подібного феномену привносить у соціальну структуру неспокій, загрожує інституційним програмам із побудованою ними реальністю.[1, с.258]

На рівні вторинної соціалізації можлива представленість індивіда одночасно у протилежних реальностях, адже у вторинній соціалізації інтерналізація необов'язково супроводжується емоційно навантаженою ідентифікацією із значимим іншими. Індивід може інтерналізувати різноманітні реальності без ідентифікації із ними. Тому при появі альтернативного світу у вторинній соціалізації індивід може здійснювати вибір на його користь маніпулятивним чином. Інтерналізуючи нову реальність, він використовує її для реалізації специфічних цілей. Оскільки це пов'язано із виконанням певних ролей – індивід зберігає по відношенню до них суб'єктивну дистанцію, направлено та довільно «одягаючи» їх. Інституційний порядок в цілому приймає характер мережі взаємних маніпуляцій, якщо подібний феномен досить поширений [2].

В умовах активного протікання процесів глобалізації ми стикаємось із суспільством в якому світи, що розходяться стають загальнодоступними як на ринку. Зростає загальне усвідомлення релятивності усіх світів (реальностей), включаючи і свій власний, що тепер усвідомлюється як один зі світів, а не як Світ. Внаслідок цього власне інституційна поведінка розуміється як «роль» від якої можна віддалятись у свідомості і яку можна програвати з допомогою маніпулятивного контролю (аристократ тепер не є аристократом – а грає роль аристократа, очевидно як і демократ грає роль демократа).

Література:

1. *Бергер П.* Социальное конструирование реальности. Трактат по социологии знания / П. Бергер, Т. Лукман. – М.: «Медиум», 1995. – 323 с.

2. *Миненков Г.* Концепт идентичности: перспективы определения / Г. Миненков [Електронний ресурс] – Режим доступу: http://www.belintellectuals.com/discussions/?id=74 – Назва з екрану

3. *Петруцийова Е.* По следам человеческой идентичности/ Е. Петруцийова// Мысль. Санкт-Петербургское философское общество – 2010. – Вып. 10. – С. 103–112 .

Храпова Т.К.
Студентка факультету ІТ
Державний університет телекомунікацій
м. Київ, Україна

ІННОВАЦІЙНІ ЗАСОБИ НАВЧАННЯ

Мета цієї статті описати роль іноваційних засобів навчання для освітнього середовища, яке створює особистісно-орієнтоване навчання та практику, пропонуючи нові, більш гнучкі методи навчання.

У еру цифрових технологій не можна досягти високих результатів у навчанні та навчальному процесі без інтеграції нових інформаційних і комунікаційних технологій в системі освіти.[1]

Інноваційні засоби навчання зосереджуються на проблемах, пов'язаних з інформаційними і комунікаційними системами у вищій освіті та на нових підходах до викладання, навчання і оцінки яких, засновані на використанні програмного забезпечення додатків, мультимедійної продукції та веб-інформації в основі.

Використання величезного інтегрованого набору комп'ютерних та інтернет-інструментів і ресурсів для здобуття нових знань, де середовище дозволяє домогтися більш потужної і ефективної підготовки в якому студенти більше не пасивні споживачі освітніх програм і послуг, а активні учасники.

Електронні засоби навчального призначення – це засоби, що зберігаються на цифрових або аналогових носіях даних і відтворюються на електронному обладнанні. Для підвищення ефективності використання засобів навчання при викладанні з множини усіх засобів навчання слід утворювати їх відповідні сукупності, в яких забезпечується техніко-технологічна і функціонально-цільова інтеграція.

Сьогодні на заміну традиційним навчальним підручникам з паперу приходять електронні підручники. Декілька електронних підручників утворюють електронну бібліотеку. Електронна бібліотека створюється у вигляді централізованого сховища, побудованого на поєднанні машинної пам'яті, мікроносіїв і засобів передавання інформації. Інформація відшуковується в системі 4 запам'ятовуючих пристроїв за допомогою відповідних методів пошуку. До інформаційних ресурсів належать інформаційно-навчальні матеріали лекції, словники, посилання на літературні джерела, посилання на віддалені мережеві ресурси (бази даних WWW-сервери, програмне забезпечення та ін.) Ці інформаційні ресурси є основною складовою електронних курсів – навчальних курсів, поданих мовою HTML [2, с. 155]. На мою думку, як ефективний інформаційний засіб слід використовувати доступ до глобальної комп'ютерної мережі Інтернет. Internet (Inet, I-net, Net) – (Інтернет, мережа, «мережа мереж») глобальна комп'ютерна мережа, що використовує стандартизовані протоколи й об'єднує понад 50 тисяч мереж. Її попередницею була мережа ARPAnet [3]. У сучасному Інтернеті будь-який учень або вчитель зможе потрапити на необхідний освітній ресурс у будь-який час із будь-якого місця земної кулі. Технології освіти майбутнього, за прогнозами сьогоднішнього дня, будуть будуватися на основі ділових ігор у мережі й досягнень мультимедіа, а освітні ресурси будуть доступні й відкриті для користувачів. Навчання стане мобільним і буде проходити як індивідуально, так і у команді. Велику роль буде грати зв'язок через Інтернет. Аудіо та відео матеріали стануть однією з основ модернізації освіти. Наприклад, навіть зараз все частіше в навчальні матеріали входять аудіокниги, які можна прослухати на iPod або mp3-плеєрі. Мобільність і велика кількість контенту, який можна розмістити на сучасні носії, сприятиме підвищенню інформованості та ерудиції [4].

Дидактичні засоби навчання - це засоби навчання, які базуються на використанні персональних комп'ютерів, охоплюють широке коло програмного забезпечення навчального призначення. Серед програмного забезпечення навчального призначення слід виділити: електронні навчальні курси, програмно-педагогічні засоби, електронний навчально-методичний комплекс, мережеві програми та контрольно-діагностичні системи. Електронні навчальні курси присвячені вивченню якої-небудь окремої дисципліни. Крім інформаційних матеріалів містяться ще й матеріали для організації контролю та самоконтролю завдання для самостійного виконання, питання для самоконтролю, тести тощо. Матеріал із електронного навчального курсу викладач може доповнити, виправити, відправити учневі електронною поштою, записати на компакт- диску або розмістити на освітньому веб-сайті для одночасного доступу до нього всіх учнів. Електронний навчальний курс забезпечує режим самонавчання та можливість самоконтролю. Включення в електронний курс елементів анімації та комп'ютерних ігор посилює його ефективність і привабливість. Гіпертекстова структура курсу дозволяє здійснювати індивідуальну траєкторію навчання. Програмно-педагогічні засоби – сукупність комп’ютерних програм навчального призначення. На думку В. С. Круглика, сучасний програмно-педагогічний засіб повинен містити такі модулі: електронний підручник, електронний довідник, тренажерний комплекс (комп'ютерні моделі, конструктори й тренажери), задачник, електронний лабораторний практикум, комп'ютерна тестуюча система, система планування процесу навчання [4].

Звичайно, представлені компоненти ППЗ самі не вирішують педагогічних завдань. Навчальна функція реалізується через педагогічний сценарій, за допомогою якого вчитель вибудовує освітні траєкторії. Індивідуалізація навчання, диференційований підхід до кожного окремого учня чи студента, особистісно-орієнтована методика викладання предмету, інтерактивність реалізації процесу роботи під час виконання ними практичного фрагменту уроку є дуже важливим як методичним, так і психологічним аспектом застосування програм у навчальному процесі. Використання мультимедійних технологій та можливості Інтернету дозволяє підняти на новий рівень якість та ефективність систем тестування знань. Тому можна беззаперечно сказати, що мультимедійна складова даних систем буде постійно зростати, і використання мультимедія буде відігравати провідну роль в розвитку і в ефективному застосуванні систем тестування знань, як в галузі освіти, так і на підприємствах [5, с. 13]. Розвиток засобів навчання зумовлює і розвиток нових методів навчання, відродження тих методів, які не могли бути реалізовані без застосування комп'ютеризованих засобів навчання.

Отже, розвиток нових інформаційних технологій в 21-ому столітті розширює спектр інформаційних ресурсів; це також створює умови для формування глобального інформаційного, освітнього та культурного простору, а значить ці зміни відбуваються в системі освіти. Ця стаття підкреслює, що високі результати не можуть бути досягнуті в навчальному процесі без інтеграції нових інформаційних та комунікаційних технологій. Використання величезних інтегрованих наборів комп'ютерних та інтернет-інструментів і ресурсів дозволяє досягти більш ефективного і дієвого навчання. Студенти більше не будуть пасивними споживачами освітніх програм і послуг, вони станують активними співучасниками освітнього процесу. Їх навички та вміння ефективно працювати з цифровими технологіями станують передумовою для успішного і відповідального рішення для представлення наукових проблем і справ.

Розробка нових технологій і використання електронного обладнання у викладанні та навчанні має велике значення. Інтеграція цифрових технологій в освітнє середовище може підвищити ефективність і якість системи освіти.

Література:

1.Рада Європейського Союзу (2011): Висновки Ради про роль освіти в Реалізація стратегії "Європа 2020". 2011 / C 70 / 01.Official Журнал uropean Союзу,4.3.2011, отримані від http://eur-lex.europa.eu

2.Дементієвська Н.П., Морзе Н.В. Як можна комп'ютерні технології використати для розвитку учнів та вчителів // Актуальні проблеми психології: Психологічна теорія і технологія навчання / За ред. С.Д.Максименка, М.Л.Смульсон. – К.: Міленіум, 2005. -Т. 8, вип. 1. – 238 с. – с. 152-158.

3.Англо-український тлумачний словник з обчислюваної техніки, Інтернету і програмування. – Вид.1 – К.: Видавничий дім "Софт Прес", 2005. – 756 с.

4.Круглик В. С. Концепція сучасного педагогічного програмного засобу/ В. С. Круглик. – [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/ejournals/ITZN/em3/content/07kvsspm.htm.

[5] .Бирка М.Ф. Комп'ютер – помічник під час тематичної атестації.// Крайова освіта № 3 (195) від 22 січня 2003 р. – с. 13.

Параняк П.Р.

Асистент кафедри теорії та історії політичної науки

Львівський національний університет імені Івана Франка

м.Львів, Україна

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ СТАНОВЛЕННЯ МУЛЬТИКУЛЬТУРАЛІЗМУ В УКРАЇНІ

Глобалізаційні процеси які відбуваються у світі, створюють швидкий процес культурної трансформації. Відбувається культурне взаємопізнання на різних рівнях. Змішуються традиційні національні культури та масова культура, і все це представляє собою новий тип відносин, який вимагає відповідного регулювання з боку держав. Уряди багатьох країн Європи зіштовхуються з таким питанням і відповідають на нього різними рішеннями та організаційними заходами. Україна сьогодні не є виключенням, оскільки країна поступово розвивається і все більше старається інтегруватись в європейський культурний простір.

В європейському суспільстві сьогодні увага зосереджена навколо полікультурності складу населення у державах. Через дану ситуацію відбувається поділ між людьми на прихильників та опонентів такого культурного розмаїття, і все це супроводжується протестами, які часто переростають у масові заворушення. Таку ситуацію пояснюють провалом політики мультикультуралізму, яка активно впроваджувалась на кінці двадцятого століття, в розвинутих країнах Європи. Постає питання чи готова Україна до вирішення таких питань в разі повної інтеграції в європейський простір, та чи політика мультикультуралізму буде для України новим кроком, на шляху до розвитку демократичних цінностей?.

Мультикультуралізм являється принципом організації суспільства, який передбачає соціокультурну та етнічну різноманітність[1]. Позиція Української держави в політиці мультикультуралізму розглядається як нейтральна, тобто вона не долучається до розвитку певної культури, і її діяльність спрямована на створення умов для гармонійного розвитку всіх культур, які розташовані в зоні її юрисдикції.

Україна є поліетнічною країною, і на території держави проживає близько ста тридцяти національностей і народностей[2]. У національному складі населення переважають українці і становлять 78% від загальної кількості населення. До національних меншин на території відносяться росіяни, білоруси, молдавани, кримські татари, євреї, румуни та інші національності. Розглядаючи Україну, можна зазначити, що політику спрямовану на побудову раціональних відносин між етносами було ще започатковано на початку дев’яностих років двадцятого століття. Метою була реконструкція політики Радянського Союзу з введенням ліберальних ідей, аби забезпечити найбільш гармонійний розвиток кожної культури на території держави. Основною метою було створити толерантний зв'язок корінної нації з національними меншинами[3]. Впроваджувались різні законопроекти, які передбачали умови розвитку кожної культури, виробилась ціла етнокультурна політика мета, якої була задоволення духовних та культурно-освітніх потреб. Політика реалізовувалась через створення різних об’єднань національних меншин, запроваджувались освітні заклади в яких велось навчання мовою спільноти, яка проживала в тому регіоні. Випускається низка газет, яка відображає життя кожного етносу, який проживає на території України.

Умови, які створила Україна для побудови демократичних в етнополітичному контексті, можна вважати цілком раціональними та відповідними до стандартів Європи.

В Європі акцент робиться на побудові суспільства з приїжджого населення, яке потрапило в країну по різних причинах, а в Україні проблема мультикультуралізму розгортається через історичне минуле. Оскільки території держави часто перебували під впливом інших держав, як Польща, Румунія,Австро-Угорська імперія, Російська імперія, та ін., і українське населення, яке проживало на захоплених територіях, потрапляло під асиміляційні заходи, відповідно це призвело до того, що змінився склад населення, а особливо в прикордонних областях[3]. Виходячи з такої історичної ситуації метою політики мультикультуралізму в Україні є врегулювання відносин між етносами, які історично осіли на території сучасної Української держави.

Розглядаючи політику мультикультуралізму України та її особливості слід зазначити, що дана форма політичного курсу є зовсім не новою для України, і вона насправді являється значним кроком на шляху формування демократичного суспільства. Прагнення України інтегруватись в європейську спільноту змушує активно розвивати політику мультикультуралізму на державному рівні саме це дозволить покращити, як політичну культуру так і економіку держави.

Література:

1.Вихров М. «Мультикультурализм в Украине: спасибо, не нужно» [електронний ресурс]. Режим доступу: http://polemika.com.ua/news-121768.html}

2.Державний комітет статистики України[електронний ресурс]. Режим доступу: http://2001.ukrcensus.gov.ua/

3.Калакура О. Я. «Мультикультуралізм: сутність і перспективи для України» [електронний ресурс].
Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Chl/2010_2/2-2.pdf