ISSN 2412-9070

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Є ЧЛЕНОМ МІЖНАРОДНОГО СОЮЗУ ЕЛЕКТРОЗВ'ЯЗКУ

З В' Я З О К

Випуск № 5 (129), 2017

Заснований 1995 року

Наукове періодичне видання, в якому відображено результати наукових досліджень з розробки та вдосконалення інформаційних систем, мереж та технологій у різних проблемних галузях

З А С Н О В Н И К
Державний університет телекомунікацій

Періодичність виходу — 6 разів на рік
Передплатний індекс 74224

Адреса редакційної колегії:
Україна, 03110, м. Київ, вул. Солом'янська, 7.
Прийом статей:
E-mail: kpstorchak@ukr.net
Телефон: (044) 249 25 42, +38 (095) 878 93 81

Телефон: (044) 249 25 75 (довідки, консультації)
E-mail: zviaz-ok@ukr.net
Інформаційний сайт: www.dut.edu.ua

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор

Затверджено до друку вченою радою Державного університету телекомунікацій (протокол № 24 від 12.06.2017 р.).

Занесено до Переліку наукових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук, затвердженого Постановою Президії ВАК України від 10.05.2017 р. № 693 за напрямком «Технічні науки»

Свідоцтво про державну реєстрацію КВ № 20996-10796 ПР від 25.09. 2014 р.

ЧИТАЙТЕ У НОМЕРІ

ЕКСКЛЮЗИВ

У ФОКУСІ УВАГИ

СЛОВО НАУКОВЦЯ

ПРОБЛЕМИ РОЗВИТКУ ТА ВДОСКОНАЛЕННЯ ЄДИНОЇ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗВ'ЯЗКУ

ПРОБЛЕМИ ПОШТОВОГО ЗВ'ЯЗКУ. ПОШТОВІ ТЕХНОЛОГІЇ

НАУКА, ЕКСПЛУАТАЦІЯ, ВИРОБНИЦТВО

ДО ВІДОМА АВТОРІВ ТА ПАРТНЕРІВ ЖУРНАЛУ

У часопису на платній основі вміщуються праці, які відповідають профілю видання, раніше не опубліковані й такі, що водночас не публікуватимуться в інших виданнях.

Думка редакції може не збігатися з позицією, викладеною авторами. Листування з читачами провадиться виключно на сторінках журналу. При передруку посилання на «ЗВ'ЯЗОК» обов'язкове.

РУКОПИСИ НЕ ПОВЕРТАЮТЬСЯ

Матеріали, які подаються до редакції, мають бути роздруковані на одному боці сторінки, при цьому бажано додати текстовий файл у форматі Word. Шрифт — Times New Roman (12 кегль), міжрядковий інтервал — не менш ніж 2, з полями: згори — 20 мм, ліворуч — 30 мм, праворуч —10 мм, знизу — 25 мм. Усі сторінки мають бути послідовно пронумерованими. За наявності рисунків (графіків) потрібно подати їх в окремих файлах (CorelDraw чи у форматах TIF та EPS), причому текст не конвертується в криві.

Матеріали мають бути підписані автором із зазначенням прізвища, імені, по батькові, місця роботи, посади, домашньої та електронної адреси, паспортних реквізитів, контактних телефонів.

УДК 502/504 (15)+621.739
С. В. КОЗЕЛКОВ, доктор техн. наук, професор;
В. Ф. ФРОЛОВ, доктор техн. наук, професор;
Л. А. КИРПАЧ, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

АНАЛІЗ ВПЛИВУ КОСМІЧНОЇ ПОГОДИ ТА КОСМІЧНОГО СМІТТЯ НА ЯКІСТЬ РОБОТИ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Запропоновано визначати якість роботи телекомунікаційних систем з урахуванням космічної погоди та космічного сміття, рознесеного на всіх робочих орбітах, де виконують свою місію космічні апарати різного призначення.

Ключові слова: космічна погода; геомагнітна та сонячна активність; електронна концентрація; телекомунікаційні системи; космічне сміття.

Вступ

Якість роботи телекомунікаційних систем стає дедалі важливішим показником при їх оцінюванні. Умови, в яких виконують свої функції телекомунікаційні системи, що перебувають на різних космічних орбітах, безперервно змінюються. Це відбувається з двох основних причин: по-перше, через вплив космічної погоди, не залежної від людського фактора (сонячна активність, геомагнітні зміни, галактичне випромінювання, метеоритні та астероїдні потоки), а по-друге, через вплив людини на стан навколоземного космічного простору. Ідеться про космічне сміття, утворене за понад 60 років космічної діяльності людства на всіх орбітах. Ураховуючи ці причини, маємо змогу здійснювати пуск ракет-носіїв із певним корисним навантаженням у конкретний рік, місяць та час, забезпечуючи надійність телекомунікаційних систем, високу якість та вірогідність їхніх сигналів.

Основна частина

Як відомо, кількісні значення похибок у технічно справній телекомунікаційній системі визначаються не тільки умовами поширення сигналу супутникової навігації (GPS, ГЛОНАСС, EUROSAT, COMPASS), а й станом космічної погоди та наявністю космічного сміття на робочих орбітах. Космічна погода, у свою чергу, визначається параметрами геомагнітної і сонячної активності, залежачи від сезону, часу доби, метеоумов. Так, щільність атмосфери при 11- та 22-річних циклах сонячної активності підвищується в багато (від 20 до 50) разів: улітку щільність атмосфери в 2-3 рази вища, ніж узимку. Це стосується й часу доби — удень щільність вища, ніж уночі. Вочевидь, усіх таких природних факторів впливу космічної погоди на якість телекомунікаційних систем уникнути неможливо. Проте якість навігаційних сигналів істотно залежить і від зміни електронної концентрації на шляху проходження сигналу: сонячні бурі, космічне та галактичне випромінювання.

Зрештою негативний вплив явищ космічної погоди на якість телекомунікаційних сигналів призводить до таких наслідків [1]:

- зростання кількості помилок позиціонування під дією іоносферних збурень на шляху поширення сигналу від передавача до приймача;
- втрати сигналу через мерехтіння, до якого призводять сильні сонячні бурі;
- виникнення в періоди сонячної активності радіосплесків на частотах, які збігаються з частотами, що їх використовує система супутникової навігації.

Що ж до помилок позиціонування супутникових систем, то їх залежно від джерел появи можна поділити на два типи:

1) помилки апаратної природи, що виникають у передавально-приймальних трактах і залежать від засобів та методів обробки сигналів;

2) помилки, зумовлені впливом на якість радіосигналів із боку космічного середовища, що призводить до змін швидкості поширення радіохвиль.

Найбільша кількість помилок другого типу спричинюється трансформаціями іоносфери та обробкою даних навігаційних сигналів за допомогою емпіричної моделі іоносфери Клобучара [1]. Відповідний алгоритм базується на сталості іоносферної затримки в нічні години і косинусному поданні (додатний півперіод) у денні години.

Оцінка зенітної іоносферної затримки в перерахунку на місцевий час t подається формулою

$$\frac{I_z}{C}=\left\{A_1+A_2\cos\left(\frac{2\pi(t-A_3)}{A_4}\right)\right\},\ \text{якщо}\ |t-A_3|<A_4/4, \quad (1)$$

де A_1 — зенітна затримка в нічний час (зафіксоване значення становить 5 нс);

A_2 — амплітуда функції косинус у денний час;

A_3 — фаза, яка відповідає піку функції косинус, зафіксованому при t = 50 400 с, що відповідає 14-й годині за місцевим часом;

A_4 — період функції косинус (> 72.000 с).

Варто наголосити, що іоносферна похибка є головною причиною недостатньої точності супут-

никових навігаційних систем (СНС). Установлено пряму залежність між іоносферною похибкою СНС і повним електронним вмістом (ПЕВ), що визначається як кількість електронів у стовпі одиничного перерізу, котрий з'єднує навігаційний супутник і приймач.

За виміряними затримками з робочими частотами f_1 і f_2 можна визначити іоносферне запізнювання сигналів. Ураховуючи геометричний фактор, можна дістати формулу для визначення ПЕВ в іоносфері:

$$\text{ПЕВ} = \frac{f_1^2 \cdot f_2^2 \left(L_{\text{вим}_2} - L_{\text{вим}_1}\right)\left[1 - \left(\frac{R\cos\beta}{R + z_{\max}}\right)\right]^{0,5}}{40A\left(f_2^2 - f_1^2\right)}. \quad (2)$$

Утім ця модель не враховує нерегулярних флуктуацій іоносферних параметрів під впливом космічної погоди, а через це знижується точність позиціонування та якість самих параметрів, що пройшли іоносферу.

У результаті потужних та середніх за інтенсивністю сонячних хромосферних спалахів спостерігаються такі явища:

- раптове припинення радіозв'язку на частотах 5…20 МГц (15…60 м) через денну половину земної кулі (ефект Мегеля – Делліндже ра);
- повне припинення відбиття від іоносферних шарів та поглинання радіовипромінювання на хвилях 10…15 м;
- раптове посилення атмосферних завад або сигналів від дуже віддалених станцій на довгих (> 10 км) хвилях.

Після сонячних спалахів іоносфера, поглинаючи сонячне рентгенівське випромінювання, нагрівається та роздувається, що призводить до значного аеродинамічного гальмування супутників і пілотованих станцій. Суттєво порушується (або частково зникає) радіозв'язок, виходять із ладу системи керування станцією, спричинюючи катастрофи. Так, унаслідок надпотужних сонячних спалахів в 1972 році американська станція «Скайлеб» впала в океан. Японська рентгенівська обсерваторія ASCA, увійшовши 15.07.2000 року в розігріту атмосферу ($H_{\text{пер}} = 440$ км), втратила орієнтацію і перейшла у «сплячий» режим, з якого вивести її було неможливо. Частота аварій та катастроф у дні геомагнітних збурень та бур суттєво зростає. Під час сонячних спалахів та магнітних бур кількість заряджених частинок у іоносфері збільшується нерівномірно, через що утворюються плазмові кулі та згустки.

Не менш значним фактором впливу на якість роботи телекомунікаційних систем виступає космічне сміття [2], рознесене на всіх орбітах, де перебувають космічні апарати. Воно створює численні завади проходженню радіохвиль різного діапазону. Уже сьогодні загальна маса космічного сміття сягає майже 10 000 т [3]. Щорічно країни — члени космічного клубу запускають у космос понад 100 ракет-носіїв. Станом на 1.05.2017 року кількість об'єктів, які спостерігаються засобами моніторингу космічного простору, сягає 17 900 одиниць. До складу об'єктів, за якими ведеться спостереження, входять 4 280 космічних апаратів (ті, що функціонують, а також «мертві»), 13 650 ступенів ракет-носіїв, паливних баків, інших уламків космічного сміття, утвореного внаслідок вибухів супутників або через їх зіткнення з великими уламками. Як було повідомлено в доповіді NASA Orbital Debris Program Office, за 2016 рік було зафіксовано кілька випадків дефрагментації супутників, а саме: 18 липня розпався американський супутник ДЗЗ World View-2; 27 липня — блок ДМ-2; 8 вересня — японський астрономічний супутник Hitomi; 30 вересня зруйнувався індійський супутник ДЗЗ RISAT, але фрагментів його руйнування на орбіті не знайдено.

Щорічно маса космічного сміття збільшується на 150–200 т, а його щільність (згідно з ефектом Кесслера) підвищується на 4% [4]. Таким чином, навколоземний космічний простір не тільки створює небезпеку для виконання космічних місій, (що призводить до аварійних і катастрофічних зіткнень), а й являє собою джерело завад для проходження сигналів із космічних апаратів, а також призводить до поширення помилок при позиціонуванні космічних апаратів.

Зауважимо, що точні математичні моделі, які описують процеси в сонячно-земній фізиці, відсутні. У цій сфері використовують феноменологічні математичні моделі, тобто такі, що описують послідовність фізичних явищ, кожний крок яких виконується з імовірністю менш як 100%. При цьому ймовірність реалізації повного ланцюжка може бути нижча за той рівень, коли її можна враховувати на практиці. Ідеться про прогноз на 27-45 та 7 діб; 2 доби та 1 годину.

Найбільш цікавим є 1-годинний прогноз, який спирається на прямі вимірювання параметрів плазми та магнітного поля на космічному апараті, розташованому в передній лібраційній точці L1 на відстані 1,5 млн км від Землі поблизу напряму Сонце–Земля.

При цьому надійність 1-годинного прогнозу не менша за 95%.

Таким чином, фактори космічної погоди, а також наявність космічного сміття на різних орбітах впливають і на якість телекомунікаційних радіосигналів, а це, у свою чергу, знижує точність управління та позиціонування космічних апаратів на орбітах. Із космічною погодою боротися неможливо, і цей фактор доводиться лише враховувати при виведенні космічних апаратів у космічний простір. Ураховуючи 11- та 22-річні цикли сонячної активності, необхідно так планувати космічні

місії та їх перебування на робочих орбітах, щоб уникнути впливу різних видів космічної погоди, а також скупчення космічного сміття на конкретних робочих орбітах, на роботу телекомунікаційних систем [2]. Дані про такі скупчення реєструються в каталогах з космічного сміття (NASA, ЄКА, Україна), де визначаються їхні балістичні характеристики: висота апогею та перигею, нахил орбіт, маса, балістичний коефіцієнт, швидкість [4]. Ці дані дають змогу визначати безпечні зони роботи телекомунікаційних систем на орбітах та забезпечувати стабільне поширення сигналу супутникових навігаційних систем.

Висновки

Проведений аналіз впливу космічної погоди та космічного сміття на якість роботи телекомунікаційних систем підтверджує необхідність враховувати ці фактори при визначенні похибок у технічно справній телекомунікаційній системі та умов поширення сигналу супутникової навігації.

Список використаної літератури

1. **Калашник, Г. А.** *Забезпечення стійкого функціонування засобів навігації літальних апаратів під впливом зовнішніх дестабілізуючих факторів / Г. А. Калашник, Д. М. Обідін, М. А. Калашник // Системи обробки інформації.— 2016.— Вип. 3 (140).— С. 52–56.*

2. **Фролов, В. Ф.** *Екологічна безпека біосфери Землі і Космосу: монографія / В. Ф. Фролов.— ТОВ «НВП Інтерсервіс», 2015.— 220 с.*

3. **Власов, М. Н.** *Экологическая опасность космической деятельности / М. Н. Власов, С. В. Кричевский.— М.: Наука, 1999.— 238 с.*

4. **Техногенное** *засорение околоземного космического пространства / [А. П. Алпатов, В. П. Басс, С. А. Баулин и др.].— Днепропетровск, 2012.— 378 с.*

Рецензент: доктор техн. наук, професор **К. С. Козелкова**, Державний університет телекомунікацій, Київ.

С. В. Козелков, В. Ф. Фролов, Л. А. Кирпач

АНАЛИЗ ВОЗДЕЙСТВИЯ КОСМИЧЕСКОЙ ПОГОДЫ И КОСМИЧЕСКОГО МУСОРА НА КАЧЕСТВО РАБОТЫ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Проведенный анализ воздействия космической погоды и факторов космического мусора на качество работы телекоммуникационных систем подтверждает гипотезу, что оба фактора необходимо учитывать при обеспечении надежности и достоверности работы этих систем.

Ключевые слова: космическая погода; геомагнитная и солнечная активность; электронная концентрация; телекоммуникационные системы; космический мусор.

S. V. Kozelkov, V. F. Frolov, L. A.Kyrpach

ANALYSIS OF SPACE WEATHER IMPACT AND THE SPACE DEBRIS ON QUALITY OF TELECOMMUNICATION SYSTEMS OPERATION

Performed analysis of the impact of space weather and factors of space debris on the quality of telecommunication systems operation proves the hypothesis that both factors should be considered in providing reliability and authenticity of these systems' operation.

Keywords: space weather; geomagnetic and solar activity; electronic concentration; telecommunication systems; space debris.

УДК 621.396

С. В. КОЗЕЛКОВ, доктор техн. наук, професор,
Державний університет телекомунікацій, Київ;
О. В. ШЕФЕР, канд. техн. наук, доцент;
О. В. ШУЛЬГА, доктор техн. наук, доцент,
Полтавський національний технічний університет імені Юрія Кондратюка

Удосконалення показників якості бортових радіолокаційних систем у реальних умовах їх застосування

Досліджено вплив нелінійності амплітудних характеристик радіоприймальних пристроїв (РПП) на якість функціонування бортових радіолокаційних систем (БРЛС). Визначено реальні причини зниження дальності дії БРЛС за наявності нелінійних шумів і завад. Установлено, що розширення динамічного діапазону РПП дозволяє забезпечити необхідні значення показників якості БРЛС. Розроблено теоретичне підґрунтя для вдосконалення сучасних та розроблення нових ефективних схемних способів розширення динамічного діапазону РПП, які можуть бути практично реалізовані на основі існуючої радіоелементної бази.

Ключові слова: бортова радіолокаційна система; радіоприймальний пристрій; показники якості; нелінійні процеси; динамічний діапазон; амплітудні характеристики.

Вступ

Аналіз питань побудови перспективних систем дистанційного зондування Землі (ДЗЗ) та шляхи вдосконалення їх характеристик свідчить, що одним із найбільш ефективних напрямків є підвищення завадостійкості [1]. Аналітичний огляд вимог, що висуваються до систем ДЗЗ показав, що на даний час

підвищити якість функціонування космічних бортових радіолокаційних систем (БРЛС) можна, передусім, на основі застосування сучасних радіотехнічних методів [2].

Основна частина

Порівняльний аналіз можливих шляхів та напрямків підвищення показників якості БРЛС, із урахуванням їх основних особливостей і реальних умов застосування систем ДЗЗ, довів, що в загальному випадку якість функціонування БРЛС найбільш повно характеризується деякою множиною показників якості, вектор яких перебуває в певній функціональній залежності від внутрішніх властивостей цієї БРЛС і характеристик зовнішнього середовища [3; 4]:

$$\vec{K} = A\left[\{\vec{\varepsilon}\}, \{\vec{z}\}\right], \tag{1}$$

де $\vec{K}$ — показник якості БРЛС у векторному вигляді, $\vec{K} = [K_1, K_2 \ldots]$;

K_i — скалярний показник якості БРЛС (K_1 — роздільна здатність; K_2 — точність вимірювань);

$\{\vec{\varepsilon}\}$ — сукупність параметрів, котрі характеризують БРЛС, $\{\vec{\varepsilon}\} = [\varepsilon_1, \varepsilon_2 \ldots]$;

ε_1 — апаратурна надійність БРЛС; ε_2 — динамічний діапазон РПП БРЛС;

$\{\vec{z}\}$ — сукупність характеристик зовнішнього середовища, $\{\vec{z}\} = [z_1, z_2, z_3, z_4 \ldots]$;

z_1 — характеристики радіолокаційних сигналів; z_2 — характеристики завад; z_3 — коефіцієнт загасання під час поширення радіохвиль; z_4 — ступінь відхилення параметрів руху носія БРЛС (КА) від рівномірного прямолінійного руху.

Характерною особливістю БРЛС ДЗЗ є оцінка якості їх функціонування, в основному за одним зі скалярних показників якості, наведених у табл. 1 [1; 2; 5].

Таблиця 1

Показники якості БРЛС, що характеризують якість функціонування різних типів комплексів ДЗЗ

Тип (призначення) систем та комплексів ДЗЗ	Основний показник якості функціонування БРЛС
Системи автономної навігації КА	Точність (роздільна здатність)
Системи космічного виявлення об'єктів	Імовірність правильного виявлення
Космічні системи картографування земної поверхні	Роздільна здатність

У зв'язку з цим вважаємо за доцільне ввести поняття узагальненого показника якості БРЛС ДЗЗ, під яким розуміється той скалярний показник якості K_i, який найбільш повно відображає ступінь пристосованості даної системи ДЗЗ до виконання покладених на неї завдань у заданих умовах застосування [1]. Для узагальненого показника якості БРЛС ДЗЗ векторне рівняння (1) вироджується у скалярну функціональну залежність [1; 6]

$$K_i = A_i\left[\{\vec{\varepsilon}\}, \{\vec{z}\}\right], \tag{2}$$

де $A_i[\cdot]$ — проекція векторного функціоналу $A[\cdot]$ на вісь K_i.

З огляду на статистичну незалежність або дуже слабку корельованість між апаратурною надійністю БРЛС, умовами поширення радіохвиль і відхиленнями носія БРЛС від прямолінійного рівномірного руху, з одного боку, і сигналами на вході РПП і його динамічним діапазоном, із другого боку, можна показати, що функціонал $A_i[\cdot]$ є таким, котрий факторизується [2]. Отже,

$$K_i = A_i'\left[\{\vec{\varepsilon}_j\}, \{\vec{z}_k\}\right] A_i''\left[\vec{\varepsilon}_2, \{\vec{z}_1, \vec{z}_2\}\right]. \tag{3}$$

Тут $A_i'[\cdot]$ — функціонал залежності узагальненого показника якості БРЛС від сукупностей $\{\vec{\varepsilon}_j\}, \{\vec{z}_k\}$, де $j \neq 2$, $k \neq 1, 2 \ldots$;

$A_i''[\cdot]$ — функціонал залежності узагальненого показника якості БРЛС від ширини динамічного діапазону РПП (ε_2) та характеристик радіосигналів (z_1) і завад (z_2).

Слід наголосити, що функціональну залежність $A_i'[\cdot]$ на даний час достатньо докладно вивчено і на основі проведених досліджень розроблено практичні рекомендації щодо зниження впливу факторів $\{\vec{\varepsilon}_j\}$ і $\{\vec{z}_k\}$ на якість функціонування БРЛС [2]. У ряді практично важливих випадків використання даних рекомендацій є достатнім для зменшення ступеня впливу зазначених чинників до деякого прийнятного рівня [2]. Разом із тим досі недостатньо повно досліджено вплив обмеженості динамічного діапазону реальних РПП на якість функціонування БРЛС в умовах РЕП [7]. Це зумовлено значними ускладненнями теоретичного і обчислювального характеру, котрі виникають під час дослідження складних нелінійних РПП, і відсутністю достатньо розроблених і точних та зручних методів аналізу нелінійних динамічних РТС високого порядку [8]. Окрім того, актуальність даної проблеми стає очевидною, як правило, на більш пізніх етапах реальної оптимізації і максимально повної практичної реалізації потенційних можливостей БРЛС [8]. У зв'язку з цим основну увагу необхідно приділити аналізу впливу обмеженості динамічного діапазону РПП унаслідок нелінійності його амплітудної характеристики (АХ) на показники якості БРЛС, тобто дослідженням функціоналу $A_i''[\cdot]$.

Серед відомих праць [9], присвячених дослідженню впливу нелінійності АХ РПП на якість функціонування БРЛС, слід відзначити ті, де розкрито фізичну сутність впливу нелінійних процесів, що відбуваються у РПП, на якість функціонування БРЛС. Нелінійність АХ РПП призводить до суттєвих амплітудних спотворень сигналу на його виході, які можна описати виразом [8]

$$\Delta I_{н} = \Phi_1[U_{вх}, G(U_{вх})], \quad (4)$$

де $\Delta I_{н}$ — амплітудні нелінійні спотворення; $U_{вх}$ — амплітуда вхідного сигналу; $G(U_{вх})$ — нелінійна АХ РПП; $\Phi_1[\cdot]$ — функціональна залежність, що описує амплітудні нелінійні спотворення.

Вплив амплітудних нелінійних спотворень проявляється в зменшенні коефіцієнта передачі РПП, а також у появі додаткового нелінійного шуму [3].

Зі сказаного випливає, що нелінійний шум окремих радіолокаційних цілей додається, утворюючи сумарний фон, котрий зберігає досить великий рівень на суттєвій відстані вздовж лінії шляху носія БРЛС і може маскувати слабкі сигнали на значній відстані. Загалом амплітудні нелінійні спотворення призводять до істотного зниження контрастності та деталізації радіолокаційного зображення (РЛЗ) унаслідок значного погіршення відношення сигнал/шум. Зокрема, у [8] отримано наближену залежність контрастності РП від відношення сигнал/шум. Окрім того, під час проходження сигналів досить великого рівня через РПП із нелінійною АХ унаслідок амплітудно-фазової конверсії (АФК) [8] з'являється фазовий шум, який можна подати формулою вигляду [6]

$$\Delta\varphi_{н} = \Phi_2[U_{вх}, G(U_{вх})], \quad (5)$$

де $\Delta\varphi_{н}$ — фазові (амплітудно-фазові) нелінійні спотворення;

$\Phi_2[\cdot]$ — функціональна залежність, яка описує АФК.

Фазовий шум зберігає значний рівень на досить великій відстані вздовж лінії шляху носія БРЛС [2; 3], а також спричинює суттєве розфазування когерентних БРЛС. Це призводить до незворотної втрати деякої частини інформації про вимірювані координати цілей, котрі перебувають у фазі прийнятого радіолокаційного сигналу. При цьому вплив фазових шумів може бути зведено до зменшення максимуму, розширення і зміщення відносно центральної осі головної пелюстки діаграми спрямованості антени (табл. 2), а також до появи додаткових бічних пелюсток [5; 8; 10].

Таблиця 2

Вплив фазових шумів на характеристики синтезованої діаграми спрямованості РЗА

Швидкість фазових шумів, рад	Розширення основної пелюстки, частка $\Theta_з$	Відхилення осі основної пелюстки, частка $\Theta_з$	Зменшення коефіцієнта передачі основної пелюстки, дБ
0,5	0,001–0,002	0,01–0,11	0,1–0,2
1,0	0,006–0,007	0,3–0,4	0,4–0,97
1,5	0,01–0,05	0,4–0,6	0,75–1,3
2,0	0,05–0,08	0,6–0,85	1,0–1,4

Тут $\Theta_з$ — потенційна ширина основної пелюстки синтезованої діаграми спрямованості (роздільна здатність апертури (РЗА)).

Отже, фазові шуми внаслідок АФК у РПП призводять до появи істотних координатних спотворень РЛЗ, а також до значного зниження його детальності і контрастності. Проте на основі результатів праць [2; 3] не завжди є змога точно і досить просто інтегрально оцінити вплив нелінійних процесів у реальних інерційних РПП безпосередньо на показники якості БРЛС [1; 8]. Аналіз впливу нелінійних властивостей РПП на якість функціонування РЛС проведено щодо простих РП із уведенням цілої низки пропозицій і припущень для спрощення [1; 6; 8].

Усе це призводить зрештою до того, що здобуті результати не мають достатньо загального і конструктивного характеру, оскільки не завжди дозволяють однозначно і точно ставити науково обґрунтовані вимоги до параметрів реальних складних РПП [6; 8].

Тому зазначені результати не повною мірою прийнятні для створення єдиної методологічної основи проектування БРЛС для використання їх за заданих зовнішніх умов функціонування комплексів ДЗЗ [2]. Слід зауважити, що отримані результати в прямому поданні не можуть бути використані під час впливу завад на вхід РПП [3].

У відомих працях, присвячених дослідженню завадостійкості БРЛС [2; 6; 8], здобуто чимало дуже важливих результатів, котрі свідчать про те, що потрапляння завад на вхід РПП може призвести до істотного зниження показників якості БРЛС. Зокрема, за наявності завад зменшується дальність дії БРЛС, причому [2]

$$L_{н} = L_0 10^{\frac{1}{40}(\nu_0 - \nu_{зав})};\ \nu_{зав} \geq \nu_0, \quad (6)$$

де $L_{н}$, L_0 — дальність дії БРЛС відповідно за наявності та відсутності завад;

$\nu_{зав}$ — відношення потужності зовнішньої завади до потужності внутрішніх шумів РПП (відношення завада/шум), дБ;

ν_0 — порогове відношення завада/шум, починаючи з котрого завада впливає на БРЛС, дБ.

Ефект зниження дальності дії БРЛС за наявності завад можна трактувати як зростання дальності пригнічення БРЛС деяким джерелом завад [7]. Із основного рівняння радіолокації отримуємо вираз для максимальної дальності радіолокаційного спостереження або, що те саме, мінімальної дальності пригнічення БРЛС станцією завад, поєднаної з радіолокаційною ціллю

$$L_{\min_{\text{лін}}} = k_{0\text{с}}\sqrt{q}, \tag{7}$$

а також для випадку, коли джерело завади не збігається з радіолокаційною ціллю

$$L_{\min_{\text{лін}}} = k_0\sqrt[4]{q}, \tag{8}$$

де $k_{0\text{с}}$, k_0 — коефіцієнт пропорційності у разі відповідно суміщеної і несуміщеної завади;

q — відношення сигнал/шум за потужністю на вході РПП.

У тому разі, коли завади впливають також на бічні пелюстки діаграми спрямованості, завадостійкість БРЛС зручніше оцінювати секторами і зонами пригнічення.

Площу зони пригнічення БРЛС із лінійним РПП $\delta_{\text{пр}}$, побудованим на основі РЛС, за умови знаходження станції завади в центрі смуги огляду можна знайти з формули

$$\delta_{\text{пр}} = k_{\text{п}}q^{-1}, \tag{9}$$

де $k_{\text{п}}$ — коефіцієнт пропорційності, який залежить, як k_0 і $k_{0\text{с}}$, від характеристик БРЛС, а також станції завад.

Вплив завад призводить також до помітного зниження ймовірності правильного виявлення D точкових радіолокаційних цілей за умови заданої ймовірності хибної тривоги Q, що може бути описано таким виразом [2]:

$$D = \exp\left[\frac{\ln Q}{1+Q}\right]. \tag{10}$$

Потрапляння завад на вхід РПП викликає зменшення роздільної здатності і зниження точності вимірювань БРЛС порівняно з її потенційними значеннями [8; 10]. Але безпосереднє використання загальних виразів, заснованих на виділенні просторово-часових кореляційних функцій у процесі оцінювання завадостійкості БРЛС, як правило, вельми ускладнене [8; 10]. Тому іноді зручніше застосовувати наближені вирази [8], що дозволяють порівняно просто оцінити збільшення інтервалу розрізнення БРЛС унаслідок погіршення реальної чутливості («сприйнятливості») РПП під час впливу завади на його вхід [7]

$$\Delta\alpha_{\text{лін}} \cong \Delta\alpha_{\text{пот}}\left|\frac{N_0(f)+M(f)}{N_0(f)}\right|, \tag{11}$$

де $\Delta\alpha_{\text{лін}}$ — реальна ширина інтервалу розрізнення БРЛС із лінійним РПП за параметром α;

$\Delta\alpha_{\text{пот}}$ — потенційна ширина інтервалу розрізнення за параметром α;

$N_0(\cdot)$ — миттєвий рівень внутрішніх шумів РПП, перерахованих на його вхід;

$M(\cdot)$ — миттєвий рівень завад на вході РПП.

Під час оцінювання реальної точності вимірювань БРЛС в інженерній практиці широко використовують формулу для потенційної точності вимірювань [1; 6; 8]

$$\sigma_{\alpha\text{пот}} = \frac{\Theta_\alpha}{\sqrt{2}\left|\frac{S(f)}{N_0(f)}\right|}, \tag{12}$$

де $\sigma_{\alpha\text{пот}}$ — потенційне значення СКП вимірювання параметра α;

Θ_α — величина, що характеризує потенційну роздільну здатність БРЛС за параметром α (зазвичай вважають, що $\Theta_\alpha = \Delta\alpha_{\text{пот}}$);

$S(\cdot)$ — миттєвий рівень радіолокаційного сигналу на вході РПП.

Згідно зі сказаним уводяться коефіцієнти втрат, які враховують погіршення значення Θ_α і зменшення відношення сигнал/шум [2]. З урахуванням формули (11) можна дістати вираз для реальної СКП вимірювання БРЛС із лінійним РПП $\sigma_{\alpha\text{лін}}$ [2]

$$\sigma_{\alpha\text{лін}} \cong \sigma_{\alpha\text{пот}}\left|\frac{N_0(f)+M(f)}{N_0(f)}\right|^2. \tag{13}$$

Вплив завад призводить також до погіршення інформаційних властивостей БРЛС [2]. Зокрема, якщо БРЛС побудовано на основі РЛС, то максимальна кількість інформації $V_{\max}$, отриманої за сеанс вимірювань, може бути оцінена за формулою вигляду

$$V_{\max} = \frac{L_{\alpha1}L_{\alpha2}}{\Delta\alpha_1\Delta\alpha_2}\log_2 K, \tag{14}$$

де $L_{\alpha1}$, $L_{\alpha2}$ — площа смуги радіолокаційного огляду;

$\Delta\alpha_1, \Delta\alpha_2$ — площа роздільного елемента;

K — розрізнювана кількість градацій сигнальної функції.

Із урахуванням формули (11) вираз (14) для БРЛС із лінійним РПП можна подати у вигляді

$$V_{\text{лін}} \cong V_{\max}\left|\frac{N_0(f)+M(f)}{N_0(f)}\right|^2. \qquad (15)$$

При цьому вважалося, що ступінь впливу завад на роздільну здатність за параметрами $\Delta\alpha_1$ та $\Delta\alpha_2$ однакова [7].

Аналіз співвідношень (6), (10) і (14) показує, що потрапляння завад на вхід РПП нерідко призводить до помітного зниження показників якості БРЛС. Однак ці результати здобуто за припущення про лінійність РПП, що загалом знижує їх точність і вірогідність [9]. Дійсно, як випливає з формул (4) і (5), характер впливу завад на БРЛС із реальним РПП має значною мірою залежати від їх амплітуди і виду нелінійності АХ РПП. У [8] показано, зокрема, що під час зростання амплітуди завади збільшується смуга частот її впливу на реальний РПП із неминучою нелінійністю його АХ. Це зумовлено позасмуговим нелінійним впливом завад на РПП-блокування, а також перехресні та інтермодуляційні спотворення. Відповідно зростає й імовірність впливу завад на реальний РПП порівняно з ідеальним лінійним РПП, причому [9]

$$p(\Delta f_{\text{р}}) = 1 - [1 - p(\Delta f_{\text{і}})]^{\Delta f_{\text{р}}/\Delta f_{\text{і}}}, \qquad (16)$$

де $\Delta f_{\text{р}}$, $\Delta f_{\text{і}}$ — смуга частот впливу завад заданого рівня відповідно на реальний і ідеальний РПП;

$p(\Delta f_{\text{і}})$, $p(\Delta f_{\text{р}})$ — імовірність того, що в смузі частот $\Delta f_{\text{і}}$ та $\Delta f_{\text{р}}$ виявиться відповідно хоч одна завада заданого рівня.

Нелінійний вплив завад на якість функціонування БРЛС, як правило, значно складніше враховувати й усувати, аніж лінійний вплив таких самих завад [9].

Необхідно зазначити, що відомі результати досліджень впливу завад на РПП із нелінійними АХ зазвичай мають наближений і, в основному, якісний характер [10]. Недостатньо враховується той факт, що нелінійність АХ реальних РПП є частотно-залежною, що особливо важливо під час дослідження позасмугового нелінійного впливу завад [7]. Тому дані результати умовно прийнятні для аналізу і синтезу сучасних БРЛС, РПП котрих, як правило, являють собою складне багатокаскадне з'єднання різнорідних РП із різними значеннями їх частотно-залежних параметрів [1; 5; 10]. Це зумовлює актуальність проведення більш чітких і точних досліджень нелінійних процесів у реальних багатокаскадних РПП у заданому електромагнітному оточенні (ЕМО) [7].

Аналітичний огляд відомих наукових праць, присвячених дослідженню нелінійних РПП, показує, що здобуті результати носять частинний характер [2]. Іноді такі результати недостатньо поєднуються між собою та з критеріями оцінки нелінійних властивостей РПП, що застосовуються на практиці, а також із висновками, отриманими в лінійному наближенні.

Окремі результати теоретичного аналізу важко піддаються ідентифікації, що істотно ускладнює їх експериментальну перевірку та подальше використання. Багато з методів розв'язання зазначених нелінійних задач дуже специфічні і можуть бути використані для аналізу лише окремих властивостей порівняно вузького класу нелінійних РТС [8]. Однак такий стан речей суттєво ускладнює аналіз і обмежує реальні можливості синтезу і проектування РПП деякою шириною динамічного діапазону, яка дозволяє забезпечити необхідні значення показників якості БРЛС ДЗЗ у заданому зовнішньому ЕМО [2; 3; 7]. У зв'язку з цим вельми актуальним є проведення загальних аналітичних досліджень впливу нелінійних властивостей широкого класу РПП на якість функціонування БРЛС в умовах РЕП. При цьому проведення даних досліджень на основі єдиної розробленої методології дозволило б узагальнити результати наукових розробок цього напряму. Досить важливою є також вимога ідентифікованості результатів і порівнянності їх між собою та з даними аналізу в лінійному наближенні, а також з практичними інженерними критеріями оцінки нелінійних властивостей РПП.

З урахуванням випадкового характеру вхідних впливів, а також особливостей функціонування БРЛС в умовах РЕП [7] можна записати вираз для узагальненого показника якості у вигляді імовірнісного співвідношення [2]

$$p = p_0\left[(1-p_1)p_{\text{БРЛС}_1} + p_1 p_{\text{БРЛС}_2}\right], \qquad (17)$$

де p — імовірність практичної реалізації значення узагальненого показника якості БРЛС не гірше від заданого рівня;

p_0 — складова ймовірності p, що визначається функціоналом $A'_i[\cdot]$;

p_1 — імовірність впливу завад на вхід РПП БРЛС;

$p_{\text{БРЛС}_1}$, $p_{\text{БРЛС}_2}$ — складові ймовірності p, котрі визначаються функціоналом $A''_i[\cdot]$ відповідно за відсутності та наявності завад.

Із формули (17) випливає, що розрізнюване значення ширини динамічного діапазону РПП суттєво зростає зі збільшенням імовірності впливу завад p_1 [2].

З огляду на те, що смуга пропускання за входом РПП БРЛС ДЗЗ зазвичай у десятки або сотні разів перевершує його вихідну смугу пропускання [2], імовірність позасмугового нелінійного впливу завад іноді навіть істотно перевищує ймовірність прямого проходження завад на вихід РПП (особливо за умови використання режиму зміни носійної частоти БРЛС від імпульсу до імпульсу за випадковим законом). У зв'язку з цим доцільно поділити позасмуговий та прицільний за частотою вплив завад на РПП. Тоді вираз (17) перетвориться до виду [2]

$$p = p_0\{(1-p_1)p_2 + p_1[(1-p_3)p_4 + p_3p_5]\}. \tag{18}$$

Тут

$p_2 \equiv p_{\text{БРЛС}_1} = \int\limits_{x_{\min}}^{x'_{\max}+\Delta x'} B_1(S)dS;$

$p_3 = \int\limits_{f_1}^{f_2} C(f)df$ — імовірність прямого проходження завад на вихід РПП $(\Delta f_{\text{вих}} = f_2 - f_1)$;

$p_4 = \int\limits_{x_{\min}}^{x''_{\max}+\Delta x''} B_2(X)dX$ — складова ймовірності $p_{\text{БРЛС}_2}$, зумовлена позасмуговим впливом завад;

$C(\cdot)$ — щільність розподілу завад за частотою;

$X_{\min}$ — нижня межа динамічного діапазону (чутливість) РПП;

$X'_{\max}, X''_{\max}$ — верхня межа динамічного діапазону РПП відповідно за основним і сусіднім каналом прийому;

$B_1(\cdot)$, $B_2(\cdot)$ — щільність розподілу амплітуд відповідно радіолокаційних сигналів (S) та їх суміші із завадами ($S + M$);

X', X'', X''' — величини, котрі визначають гранично допустимі співвідношення відповідно між амплітудою сигналу, позасмугової завади та завади, прицільної за частотою, а також верхньою межею динамічного діапазону РПП (зазвичай $X' = X''$; $X''' = \dfrac{x_{\text{вхmax}}}{x'_{\max}}\dfrac{1}{100}$, причому $x_{\text{вхmax}} = x'_{\max} + \Delta x'$ [5; 8]).

У процесі дослідження БРЛС, як правило, вводиться припущення щодо нормальності законів розподілу радіолокаційних сигналів, а також їх суміші із завадами [2]. Тоді амплітуда нормальних вхідних впливів із конкретною СКП σ підпорядковується розподілу Релея [2]

$$B(x,\sigma) = \frac{x}{\sigma^2}\exp\left[-\frac{x^2}{2\sigma^2}\right]. \tag{19}$$

Однак конкретні значення параметрів законів розподілу вхідних впливів зазвичай апріорно невідомі, можуть змінюватися в часі вздовж лінії шляху та за зоною огляду [8; 10]. Окрім того, сигнали, котрі заважають, можуть надходити як за головною, так і за бічною пелюсткою діаграми спрямованості антени БРЛС, а також за основним або неосновним каналом прийому РПП [5–7]. Враховуючи ці фактори, доходимо висновку, що загалом апріорний розподіл амплітуд як радіолокаційних сигналів, так і їх суміші із завадами досить коректно описуються гіперболічним (рівномірно-логарифмічним) законом [2], причому

$$B_1(S) = \frac{1}{S}\ln\frac{S_{\max}}{x_{\min}}, \tag{20}$$

$$B_2(x) = \frac{1}{x}\ln\frac{x_{\max}}{x_{\min}}. \tag{21}$$

Це відповідає загальному апріорному закону розподілу випадкової величини з великим динамічним діапазоном її зміни (закон Шеннона) [8; 10].

Якщо вважати, що порушення нормальної роботи БРЛС можливе у разі перевищення амплітуди X вхідного впливу деякого рівня X_0, то ймовірність даної події можна оцінити за допомогою такого співвідношення [10]:

$$p(x > x_0) = 1 - \int\limits_0^{x_0} B(x)dx \cong 1 - \int\limits_{x_{\min}}^{x_0} B(x)dx. \tag{22}$$

Слід зазначити, що лінійний динамічний діапазон відомих РПП БРЛС, як правило, не перевищує 40-50 дБ [8; 10].

Висновки

За результатами досліджень, проведених у рамках статті, можна обґрунтовано стверджувати, що ймовірність порушення нормальної роботи БРЛС досить висока і становить 0,16-0,33 за відсутності завад і 0,58-0,66 в умовах РЕП. Це зумовлює необхідність істотного розширення динамічного діапазону РПП. Водночас створення НВЧ широкосмугових РПП із лінійним динамічним діапазоном є досить складним науково-технічним завданням, далеким від свого повного вирішення. Передусім це зумовлено реальними можливостями відомої радіоелементної бази.

З огляду на це особливого значення набуває застосування і вдосконалення сучасних та розроблення нових ефективних схемних способів розширення динамічного діапазону РПП, котрі можуть бути практично реалізовані на основі існуючої радіоелементної бази.

Список використаної літератури

*1. **Петров, А. В.** Анализ и синтез радиотехнических комплексов / А. В. Петров; под ред. В. Е. Дуневича.— М.: Радио и связь, 1984.— 248 с.*

*2. **Ширман, Я. Д.** Теория и техника обработки радиолокационной информации на фоне помех / Я. Д. Ширман, В. Н. Манжос.— М.: Радио и связь, 1981.— 248 с.*

*3. **Букингем, М.** Шумы в электронных приборах и системах / М. Букингем; пер. с англ.— М.: Мир, 1986.— 399 с.*

*4. **Goodman, John M.** Space Weather & Telecommunications / John M. Goodman // Springer-Verlag, New York, USA.— 2005.— P. 382.*

*5. **Ванькевич, В. В.** Теоретические и экспериментальные исследования специфики тропосферного распространения СВЧ и КВЧ радиосигналов / В. В. Ванькевич, М. А. Иванов, С. В. Козелков // Радиотехника.— 1990.— Вып. 92.— С. 106–114.*

*6. **Помехоустойчивость** и эффективность систем передачи информации / [А. Г. Зюко, А. И. Фалько, И. П. Панфилов, Л. В. Банкет].— М.: Радио и связь, 1985.— 272 с.*

*7. **Егоров, Е. И.** Использование радиочастотного спектра и радиопомехи / Е. И. Егоров, Н. И. Калашников, А. С. Михайлов.— М.: Радио и связь, 1986.— 304 с.*

*8. **Тихонов, В. И.** Статистический анализ и синтез радиотехнических устройств и систем / В. И. Тихонов, В. Н. Харисов.— [3 изд.].— М.: Горячая линия-Телеком, 2015.— 608 с.*

*9. **Dunn, Mark R.** The Volterra Series and its Application / Mark R. Dunn // Calif., Davis., USA.— 2013.— P. 268.*

*10. **Madisetti Vijay K.** Digital Signal Processing Fundamentals / Vijay K. Madisetti // Second Edition. CRC Press.— 2017.— P. 904.*

Рецензент: доктор техн. наук, професор **Л. Н. Беркман**, Державний університет телекомунікацій, Київ.

С. В. Козелков, А. В. Шефер, А. В. Шульга

СОВЕРШЕНСТВОВАНИЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА БОРТОВЫХ РАДИОЛОКАЦИОННЫХ СИСТЕМ В РЕАЛЬНЫХ УСЛОВИЯХ ИХ ПРИМЕНЕНИЯ

Исследовано влияние нелинейности амплитудных характеристик радиоприемных устройств на качество функционирования бортовых радиолокационных систем.

Ключевые слова: бортовая радиолокационная система; радиоприемное устройство; показатели качества; нелинейные процессы; динамичный диапазон; амплитудные характеристики.

S. V. Kozelkov, O. V. Shefer, O. V. Shulga

IMPROVEMENT OF QUALITY INDICATORS OF ONBOARD RADIO LOCAL SYSTEMS IN REAL CONDITIONS OF THEIR APPLICATION

In the article the influence of nonlinearities of the amplitude characteristics of radio receivers (RR) on the quality of the operation of on board radar systems (OBRS) is investigated. Real reasons for reducing the range of the radio local system in the presence of nonlinear noise and interference are established, which in general also reduces the accuracy and reliability of radar images. It is established that the expansion of the dynamic range of RR allows providing the necessary values of the quality indicators of the OBRS. Frequent dependence of nonlinear amplitude characteristics of real RRs is taken into account, which significantly influences on the study of off-band nonlinear influence of interference on radio signals. It is proved in the article that both priori distribution of amplitudes as radar signals and their mixture with obstacles are fairly well described by the hyperbolic (uniformly logarithmic) law. The theoretical basis for the improvement of modern and development of new effective circuit methods for expanding the dynamic range of RRs, which can be practically implemented on the basis of the existing radio element base, has been developed.

Keywords: onboard radio local system, radio receiver, the indicators of quality, nonlinear processes, dynamic diapason, amplitude characteristics.

УДК 004.891.3
Г. І. ГАЙДУР, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

Побудова інтелектуальної інформаційної мережі на основі самоорганізуючих мереж

Розглянуто принципи створення адаптивних самоорганізуючих мереж, здатних підвищувати свою функціональну стійкість до зовнішніх впливів. Запропоновано модель, яка дозволить підтримувати роботу мережі в разі її функціонування під дією зовнішніх збурень. Згідно з такою моделлю подано математичний опис процесів навчання та перевірки об'єктів самоорганізуючої мережі.

Ключові слова: інтелектуальна інформаційна мережа; адаптація; самоорганізація; навчання; модель.

Вступ

Самоорганізація будь-якої складної системи передбачає неухильне скорочення обсягу апріорної інформації, що її вносить автор моделі при моделюванні системи на ЕОМ, маючи на меті більш чи менш обмежити участь людини в процесі моделювання, зробити його необтяжливим і таким, що не викликає жодних проблем, а отже, не вимагає залучення експертів. Цього вдається досягти, наприклад, в інформаційних ергатичних системах за допомогою переходу на метамову діалогу людина–машина, таку як мова постановки критеріїв найзагальнішого вигляду, мінімум яких знаходить ЕОМ. Від людини вимагається лише повідомити дані спостережень і вказати критерії, що їх має задовольняти модель, а іноді — здійснити довизначення моделі, тобто процедуру остаточного її вибору.

Постановка проблеми

Розробка математичного апарату для забезпечення функціональної надійності із заданим коефіцієнтом $K_г$ готовності інтелектуальної інформаційної мережі (ІІМ), здатної до самоадаптації та самоорганізації, набуває особливої актуальності в разі багаторівневих інформаційних мереж. При цьому мережа, про яку йдеться, повинна мати властивості адаптації та самоорганізації, а отже, знадобляться дослідження адаптивної моделі ІІМ, здатної до самоорганізації, спрямовані на побудову математичного опису такої мережі для отримання математичної моделі її поводження.

Основна частина

Адаптивною, або *відновлюваною*, будемо називати таку ІІМ S, в якій під час роботи відбувається цілеспрямована зміна її параметрів, що має на меті стабілізувати роботу мережі [1].

Подамо адаптивну ІІМ функцією $F(x)$ структури мережі, яка зазнає впливу внутрішніх і зовнішніх дестабілізуючих факторів (відмови мережі, обрив зв'язків між її елементами тощо). Функціонування такої ІІМ описується системою диференціальних рівнянь, розв'язок якої в аналітичному або чисельному вигляді дозволяє розраховувати ймовірність значення коефіцієнта $K_г$ для заданого часу, середній час життя ІІМ та ймовірність перебування її у стані адаптації.

При заданому співвідношенні між інтенсивностями відмов ($\lambda 0$, $\lambda 1$) і збоїв ($\lambda^* 0$, $\lambda^* 1$) постає завдання визначити тип адаптивної ІІМ і алгоритм адаптації, який забезпечує інформаційній системі на інтервалі $[0, t]$ імовірність отримання $K_г$, не нижчого від заданого, при мінімальному впливі завад на мережу.

Інакше кажучи, для заданих співвідношень між інтенсивностями відмов і збоїв необхідно визначити такий тип адаптивної ІІМ і такий алгоритм адаптації, за яких ІІМ матиме максимальний середній час життя.

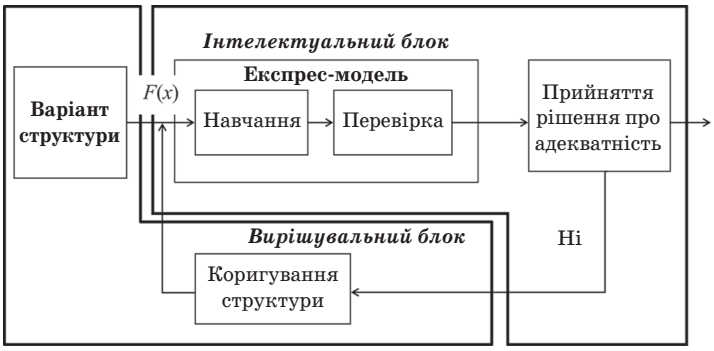
Для швидкої ідентифікації стану ІІМ побудуємо новий алгоритм експрес-проектування (див. рисунок) на основі запропонованої експрес-моделі. Спроектована мережа відрізняється від традиційної мережі тим, що вона автоматично «сама себе навчає» і «сама себе організує», залучаючи при цьому відповідно налаштоване обладнання або користувача [2].

Така модель має низку характерних властивостей:

1) на вхід блока подається інформація лише про ***початкову структуру*** об'єкта проектування (одного з варіантів цього об'єкта);

2) у разі автоматичної побудови та роботи з експрес-моделлю оптимізація параметрів елементів не виконується, оскільки вважається, що значення цих параметрів при ***навчанні експрес-моделі*** автоматично налаштовуються на деякий прихований багатоцільовий квазіоптимум;

3) робота з експрес-моделлю передбачає автоматичне виконання набору непрямих стандартних комп'ютерних процедур за допомогою швидкодійного інваріантного щодо зовнішніх збурень ***програмного модуля***, пов'язаного зі структурою проектованого об'єкта;



Самоорганізуюча інтелектуальна інформаційна мережа

4) ***блок експрес-моделі*** видає результат своєї роботи у вигляді деякого числового значення, придатного для безпосереднього порівняння і ранжування проектованих варіантів об'єкта;

5) експрес-модель дозволяє легко моделювати численні стратегії технічного обслуговування мережі.

Отже, ***інтелектуальний блок*** дозволяє впорядковувати багаторазові відмови мережних елементів і відповідно до якості експрес-моделі формувати адаптивну математичну модель у вигляді інтелектуальних блоків, пов'язаних між собою за допомогою мережних елементів.

Одна з головних особливостей самоорганізуючих мереж — це здатність чинити опір зовнішнім збуренням, а також адаптуватися до змінюваних умов, перетворюючи при потребі свою структуру.

Можна виокремити два підходи до самоорганізації: *кібернетичний підхід*, згідно з яким система організується під дією управляючого органу, та *синергетичний підхід*, коли система власними зусиллями, за допомогою сукупності певних управляючих параметрів «запускає» процес самоорганізації, вибираючи власний шлях подальшого розвитку.

Зауважимо, що сучасні ІІМ відзначаються різнорідністю обладнання та ієрархічністю структури. Окремі їхні компоненти розосереджуються по певній території. За цих умов актуалізується завдання щодо створення адекватних моделей, які дозволяють оцінити параметри окремих об'єктів ІІМ і визначити властивості, характерні для функціонування мережі в цілому. Особливий інтерес при розрахунку параметрів мережі та прогнозуванні змін їхніх значень викликають моделі складних об'єктів, здатних до самоорганізації.

Як відомо, для розв'язування комплексу задач, які стосуються функціонування ІІМ, створено ***метод групового врахування аргументів*** (***МГУА***), що його запропонував **А. І. Івахненко**. Цей метод реалізує вибір моделі оптимальної складності. Пропонується застосування ітераційного МГУА, на основі якого дістаємо оптимальні альтернативні моделі, що дозволяють здійснити вибір найкращих за певними показниками [2].

Принципова відмінність від звичайного регресійного аналізу полягає в тому, що перший має на меті знайти мінімум критерію вибору певної множини, а другий — мінімізувати середньоквадратичну помилку (СКП) в усіх експериментальних точках при наперед заданому вигляді рівняння регресії (яке, утім, має суб'єктивний характер).

Згідно з МГУА пропонується розбивати послідовність даних на дві частини: перевірну і навчальну. Навчальну послідовність використовують для оптимізації коефіцієнтів рівняння регресії, як і в разі звичайного регресійного аналізу, а перевірну — для оцінювання ступеня регулярності за відносним значенням СКП.

Нагадаємо, що регресія — імовірнісна залежність середнього значення деякої величини від іншої величини.

Відповідно до теорії функціонально стійких систем підвищення рівня завад призводить до зменшення коефіцієнта $K_г$ готовності системи в цілому, а також до зменшення кількості рівнянь і спрощення структури прогнозуючої моделі, отримуваної в результаті самоорганізації.

Варто наголосити, що алгоритми самоорганізації при певному виборі їх структури і вигляду критеріїв забезпечують високу завадостійкість: завади можуть у кілька разів перевищувати корисний сигнал, але майже не спотворювати його. Адже розміри області моделювання (кількість рівнянь моделі) та складність моделі (кількість доданків у кожному рівнянні), коли йдеться про моделювання процесів самоорганізації, визначаються в результаті перебору варіантів: за допомогою спеціальних програм вибираємо лише таку фізичну модель, яка дає змогу мінімізувати ансамбль чи ієрархію заданих критеріїв.

Слід зазначити, що для моделювання процесів самоорганізації, особливо в інформаційних мережах, часто бракує обсягу вихідної інформації, проте є змога отримати інформацію стосовно процесів по інших об'єктах, схожих на досліджуваний. Тоді створюються однорідні групи досліджуваних об'єктів, а далі в межах кожної групи здійснюється побудова адекватних моделей.

Існують різні прийоми визначення однорідних класів об'єктів. Наприклад, вважають, що два об'єкти належать до одного й того самого класу, якщо обидва вони можуть бути описані анало-

гічними моделями. При цьому припускають, що структура вихідної інформації для об'єктів, які належать одному класу, однакова.

Отже, для кожного i-го об'єкта існує m реалізацій $\left(y_t^i, u_t^i\right)$, де u_t^i — вектор.

Для i-го та j-го об'єктів отримано моделі

$$y_t^i = f_i\left(u_t^i\right);\ y_t^j = f_i\left(u_t^j\right).$$

Як міру відповідності взято критерій

$$E_{ij} = \sum_{t=1}^{m}\left(y_t^i - f_j\left(u_t^i\right)\right)^2 \Big/ m + \sum_{t=1}^{m}\left(y_t^j - f_i\left(u_t^j\right)\right)^2 \Big/ m$$

— середню суму відхилень однієї з моделей, обчислену за вихідною інформацією іншої моделі. Цей критерій можна розглядати як різновид критерію мінімуму зсуву, причому реалізації одного об'єкта утворюють навчальну послідовність A, а реалізації іншого — перевірну послідовність B.

Для n об'єктів бажаний поділ на класи досягається в такий спосіб. Обчисливши значення E_{ij} для всіх можливих комбінацій пар об'єктів, знаходимо для кожного i-го об'єкта елемент, що належить йому з найменшим розузгодженням. Якщо справджується нерівність $\min E_{ij} \le E_0$ (E_0 — деяке задане значення), то обидва елементи належать одному класу, інакше — різним класам. Ця процедура багато разів повторюється доти, доки для заданого E_0 не буде утворено класи однорідних об'єктів.

При обчисленні E_{ij} припускаємо, що для кожного об'єкта існує m реалізацій, достатніх для моделей $y = f_j\left(u_t^i\right),\ j = 1, 2, \ldots, n$.

Для малих значень m такий підхід неприйнятний. Тоді можна побудувати загальну модель $y_m = f_m(u_m)$, яка відповідає деякому усередненому об'єкту. Якщо у виразі для t функції достатньо «рівні» між собою, то тоді виразом

$$\Delta_i = \sum_{t=1}^{m}\left(y_{it} - f_m\left(u_{it}\right)\right),\ i = 1, 2, \ldots, m,$$

подаються середні відхилення окремих i-х об'єктів від значень усередненої моделі.

Якщо, наприклад, y — значення коефіцієнта $K_г$ готовності, то $\Delta_i < 0$ означає, що відповідний об'єкт міститься нижче середнього рівня коефіцієнта $K_г$. Згідно зі сказаним розглядувані об'єкти можна поділити на три класи:

1) $\Delta_i \le -B$;
2) $|\Delta_i| < B$;
3) $\Delta_i > B$.

Одна з основних пропозицій полягає в тому, аби як дані по кожному контрольованому об'єкту застосовувати навчальну послідовність [3]. При цьому для утворення перевірної послідовності використовуються дані по іншому контрольованому об'єкту, найближчому за своїми характеристиками до першого. Звідси постає завдання щодо виокремлення об'єктів, схожих між собою за своїми характеристиками.

Згідно з такою постановкою задачі поводження контрольованих об'єктів, що підлягає прогнозуванню, можна розглянути як вихідну величину деякої динамічної керованої системи, котра зазнає впливу випадкових збурень. У результаті самоорганізації такої системи математична модель, що описує її поводження, зводиться до перетворення вхідного вектора $F(t)$ на вихідний вектор $y(t)$. Залежно від апріорної інформації про досліджувану систему можуть бути отримані моделі статичних систем, динамічних систем, а також систем із зосередженими чи розподіленими параметрами.

Висновок

Досліджено характеристики адаптивних інтелектуальних інформаційних мереж і доведено доцільність побудови самоорганізуючих мереж для підтримання заданого рівня коефіцієнта готовності.

Список використаної літератури

1. **Беркман, Л. Н.** *Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ «КПІ».— 2007.— № 2.*

2. **Гороховський, О. І.** *Інтелектуальні системи / О. І. Гороховський // Вінниц. нац. техн. ун-т.— Вінниця, 2010.— 193 с.*

3. **Інтелектуальні** *системи підтримки прийняття рішень: навч. посібник / [Б. М. Герасимов, В. М. Локазюк, О. Г. Оксіюк, О. В. Поморова]— Європ. ун-т.— К., 2007.— 335 с.*

Рецензент: доктор техн. наук, професор **Л. Н. Беркман**, Державний університет телекомунікацій, Київ.

Г. И. Гайдур

ПОСТРОЕНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ НА ОСНОВЕ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ

Рассмотрены принципы создания адаптивных самоорганизующихся сетей, способных повышать свою функциональную устойчивость к внешним воздействиям. Предложена модель, которая позволит поддерживать работу сети в процессе ее функционирования под влиянием внешних дестабилизирующих факторов. Для такой модели представлено математическое описание процессов обучения и проверки объектов сети.

Ключевые слова: интеллектуальная информационная сеть; адаптация; самоорганизация; обучение; модель.

H. I. Haidur

CONSTRUCTION OF THE INTELLECTUAL INFORMATION NETWORK ON THE BASIS OF SELF-ORGANIZING NETWORKS

The creation of adaptive self-organizing networks is considered, which will reduce the functional stability to the external influences of such networks. In the paper a model is proposed that will support the operation of the network, in the process of its functioning, under the influence of external factors. For such a model, the learning process for verifying network objects is mathematically described.

Keywords: intellectual information network; adaptation; self-organization; training; model.

УДК 621.391.82
Д. В. БАРИШЕВ,
Державний університет телекомунікацій, Київ

ПЕРЕДАВАННЯ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО СИГНАЛУ ЗА ДОПОМОГОЮ СИСТЕМИ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Розглянуто структуру передавання супутникового сигналу на Землю та відстежено шлях сигналу від космічної станції до споживача.

Ключові слова: передавання сигналу; споживач; супутниковий сигнал; ретранслятор; частота; антена.

Вступ

Сьогодні набуває подальшого поширення використання телевізійних супутників для передавання високоякісного телевізійного сигналу абонентам у будь-якій точці Землі. Супутникове телебачення в усьому світі розвивається настільки стрімко, що навіть фахівці далеко не завжди встигають вчасно відстежувати зміни, що відбуваються. Адже постійно здійснюється запуск нових супутників, «відкриваються» і «закриваються» ті чи інші канали.

Основна частина

Супутниковий зв'язок — це вид зв'язку, що використовує ретрансляцію сигналів за допомогою спеціального апарата — космічного ретранслятора, розміщеного на борту штучного супутника Землі, котрий перебуває на стаціонарній орбіті. За допомогою одного чи кількох таких супутників, використовуваних як космічні ретранслятори, забезпечується зв'язок між багатьма наземними станціями.

Уявімо, що на Землі встановлено передавач, який у космос передає високочастотний (телебачення, інтернет) сигнал у напрямі супутника, розташованого на геостаціонарній орбіті, котра перебуває над екватором на висоті 35 786 км. Особливість цієї орбіти полягає в тому, що супутники, які містяться на ній, рухаються зі швидкістю, котра дорівнює швидкості самої Землі, тобто вони роблять один оберт за 24 години, і для людини, що перебуває на Землі, вони здаються нерухомими відносно її поверхні. Тому як нерухомі антени сприймаються й антени, націлені на ці супутники.

Сфера застосування супутникових систем — супутникове телебачення. Згадайте супутникові тарілки (антени), що облямовують будинки кожного міста, органічно вписуючись у загальний його пейзаж. При цьому кількість супутників, що працюють на різних космічних орбітах, дедалі зростає. Освоюються нові діапазони частот.

Прийнятий супутником сигнал посилюється і за допомогою його передавачів (транспондерів) передається на певну територію Землі — так звану зону покриття. Оскільки супутник перебуває на великій висоті над поверхнею планети, його сигнал приймається на території, що досягає кількох тисяч квадратних кілометрів. Проте сила сигналу, його потужність однакова не скрізь. Вочевидь, у центрі вона максимальна, а з наближенням до краю поступово слабшає, оскільки за своєю формою і властивостями сигнал нагадує промінь світла.

Зазвичай транспондери, спрямовані на певну частину суші, дають змогу передавати величезний обсяг інформації. При цьому за допомогою тільки одного ретранслятора, установленого на супутнику, можна забезпечити передавання інформації на відстань до 15 000 км, а за допомогою лише трьох супутників можлива організація майже глобальної системи зв'язку.

Частоти, на яких передаються супутникові програми, набагато вищі за частоти наземного телебачення, саме тому для їх прийому використовуються згадані вже спеціальні антени, що за формою нагадують тарілку. На ній встановлено приймальну головку (конвертер), яка за допомогою кабелю з'єднується з ресивером, а той, у свою чергу, із телевізором. Отже, сигнал із супутника, потрапляючи на поверхню тарілки, відбивається і фокусується на опромінювачі конвертера, який додатково опромінює поверхню антени (дзеркало) для більш повного зняття і посилення прийнятого сигналу. На виході конвертера посилений і перетворений до нижчої частоти сигнал по кабелю подається на вхід ресивера, а з його виходу вже перетворений у звичайний телевізійний формат подається на вхід телевізора.

Комплект апаратури для прийому програм з будь-якого супутника складається з трьох основних елементів: антени, конвертера та ресивера.

Загалом зазначений принцип роботи аналогічний принципу роботи звичайної телевізійної антени. Різниця полягає в тому, що роль телевежі

тут відіграє супутник і сигнал від нього йде не аналоговий, а цифровий. Тому й доводиться крім антени використовувати конвертер із ресивером, завдяки чому досягається висока якість і уможливлюється велика кількість каналів. Відмітна особливість супутникового ТБ — можливість прийому «закритих» або комерційних каналів.

Варто наголосити, що сьогодні все більшого поширення набуває обладнання, яке дозволяє приймати ТБ сигнал і під'єднуватись до мережі Інтернет, працюючи лише з одним супутниковим комплектом.

Розвиток технологій супутникових систем зв'язку дозволяє зрештою знижувати вартість абонентських терміналів, зменшувати розміри антен і потужність передавачів, досягаючи поліпшення характеристик каналів зв'язку.

Якісним стрибком у розвитку супутникових технологій може стати технологія перенесення функцій управління мережею з центральної земної станції на сам супутник («HUB на борту»). При цьому істотно скоротиться затримка, пов'язана з часом проходження сигналу до супутника і у протилежному напрямі, що, вочевидь, істотно поліпшить якість зв'язку.

Як приймаюче устаткування мають використовуватися дві супутникові антени, що різняться напрямом відбиваного від їх рефлектора сигналу, тобто від самого дзеркала антени.

При цьому електромагнітний сигнал високої (до кількох десятків гігагерц) частоти із супутника, зустрічаючи супутникову антену і відбиваючись від її дзеркала, падає на опромінювач конвертера. У конвертері відбувається перетворення носійної частоти до проміжної (від кількох сот мегагерц до 1,5 гігагерц). Через коаксіальний кабель сигнал потрапляє в супутниковий ресивер, в якому з проміжної частоти, що містить велику кількість ущільнених телевізійних каналів, відбувається виділення певного телевізійного каналу за вибором користувача.

Висновок

Переваги цифрового супутникового телебачення очевидні: це і висока якість зображення, і стереозвук, і величезна кількість каналів.

Список використаної літератури

1. ***Карякин, В. Л.*** *Цифровое телевидение: учеб. пособие для вузов.— 2-е изд. перераб. и доп. / В. Л. Карякин.— М.: СОЛОН-ПРЕСС, 2012.— 448 с.*

2. ***Жуковский, А. Г.*** *Спутниковые и радиорелейные системы передачи: учеб. пособие / А. Г. Жуковский.— Ростов-на-Дону: Северно-Кавказский филиал МТУСИ, 2012.— 270 с.*

3. ***Основы*** *информационно-коммуникационных технологий / В. В. Величко, Г. П. Катунин, В. П. Шувалов; под ред. проф. В. П. Шувалова.— М.: Горячая линия-Телеком, 2009.— 712 с.*

4. ***Спутниковое*** *телевидение: справочник / Сост. В. И. Назаров, В. И. Рыженко.— М.: Оникс.— 2006.— 32 с.*

Рецензент: доктор техн. наук, професор **К. С. Козелкова**, Державний університет телекомунікацій, Київ.

Д. В. Барышев

ПЕРЕДАЧА ТЕЛЕВИЗИОННОГО СИГНАЛА ПРИ ПОМОЩИ СПУТНИКОВОЙ СИСТЕМЫ СВЯЗИ

Рассмотрена структура передачи спутникового сигнала на Землю и отслежен путь сигнала от космической станции до потребителя.

Ключевые слова: передача сигнала; потребитель; спутниковый сигнал; ретранслятор; частота; антенна.

D. V. Baryshev

TRANSMISSION OF TELEVISION SIGNAL VIA SATELLITE COMMUNICATION SYSTEM

The article describes the structure of transmitting the satellite signal to earth considered the signal path from the space station to the consume.

Keywords: signal transmission; consumer; satellite signal repeater; frequency; antenna.

УДК 004.58
Д. С. ОЛЕНИЧ, О. Ю. ПОГЛУБКО, М. О. КЛИНОВСЬКИЙ,
Державний університет телекомунікацій, Київ

ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ ІНТЕРНЕТ-МОВЛЕННЯ ТА РОЛЬ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ У МЕДІАПРОСТОРІ

Розглянуто основні компоненти потокової трансляції, а також обладнання для передавання даних за допомогою стримінгу.

Ключові слова: потокове мовлення; відеокамери; стрим-сервер; сервіси; штучний інтелект; кодер; відеокодек; аудіокодек; комп'ютер; мобільний пристрій; інтернет.

ВСТУП

Швидкість передавання інформації життєво важлива в нашому повсякденні. Такі галузі діяльності людини, як журналістика, військова справа, бізнес тощо, не можна уявити без швидкого передавання даних. Досягнення технологій оперативного передавання інформації дедалі більше використовуються в нетрадиційний спосіб, скажімо у сфері розваги чи мистецтва.

Поява та розвиток мережі Інтернет спонукали до переосмислення практичної цінності безперервної трансляції відео- та аудіоконтенту для масового споживача. З'явилося поняття інтернет-мовлення — безперервного надання та демонстрування користувачеві мережі Інтернет мультимедійних даних у реальному часі. Термін «стримінг» характеризує саме **процес** такого передавання мультимедійних даних, а не самі дані, тобто виступає як альтернатива скачуванню файлів.

Інтернет-мовлення — найбільш близька до споживача функція сучасної мережі: кожний має змогу опублікувати глобально доступну інформацію, мовником може стати будь-хто — пересічна людина, теле- або кінокомпанія, а згодом і штучний інтелект!

В інтернеті існують і набувають розвитку різні види ресурсів, які надають відеоматеріали. Це і відеохостинги, і незалежні інтернет-телеканали, і традиційні (ефірні) телеканали, що здійснюють дублювання мовлення в мережу. Усі ці види ресурсів часто відносять до інтернет-телебачення, хоча в кожному є свої особливості та можливості.

Поняття Інтернет-мовлення (internet-broadcasting) включає в себе передавання по мережі Інтернет відео- та аудіоінформації. Мовлення може здійснюватися в реальному потоці, коли йдеться про так званий *стримінг* (streaming), подібний до прямого ефіру в ефірному телебаченні. Окрім того, мовлення може здійснюватися за запитом (on demand), що можна умовно порівняти з переглядом записаної раніше програми.

До речі, найчастіше в інтернеті використовується поєднання двох видів мовлення — стримінгу та за запитом. Чимало сайтів використовують телевізійне та радійне інтернет-мовлення з опублікуванням текстових і фотоматеріалів, що є продуктом конвергенції. Такі сайти пропонується розглядати як інтернет-канали.

ОСНОВНА ЧАСТИНА

При створенні інтернет-студії слід передусім визначитись із її розміром, що, у свою чергу, залежить від завдань, поставлених перед студією. Якщо ми плануємо зняти хор, танцювальну програму, розважальне шоу або відеокліп, то розміри студії будуть великі. Якщо постає завдання знімати публіцистику, новини, рекламу — площа студії знадобиться значно менша. Тоді є сенс скористатись уже наявним приміщенням, яке нескладно пристосувати під студію.

Що ж до устаткування інтернет-студії, скажімо для зйомки відеоматеріалів, необхідні комп'ютери, відеокамери, пристрої відеозахвату від виробника — BlackMagic, монітори, аудіомікшери, радіосистеми, підсилювач та аудіомонітори.

Варто наголосити, що важлива перевага стримінгу — його демократичність, тобто невисока вартість і мобільність. Адже стримеру достатньо мати мережну картку, проводовий чи безпроводовий доступ до інтернету та будь-якого пристрою для зйомки (окрема камера або смартфон/планшет).

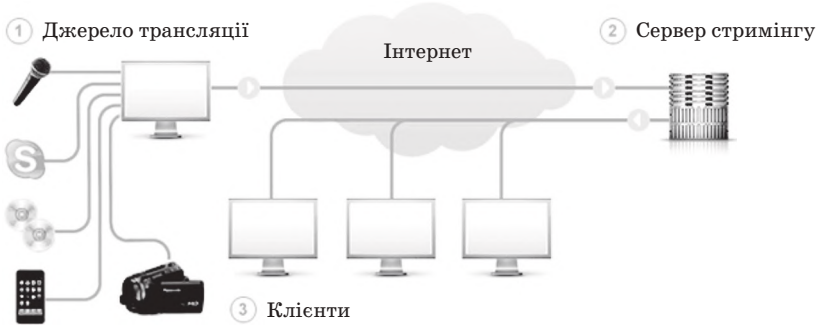
Для формування повноцінної студії потрібні синхронізовані між собою два потужні комп'ютери (головний і резервний). Трансляція відео- та аудіоматеріалу відбувається через головний комп'ютер.

Основні компоненти інтернет-стримінгу

Загальну схему розподілу основних компонентів потокової трансляції наведено на рисунку.

Компоненти з боку джерела трансляції

Комп'ютерне обладнання застосовується для об'єднання та контролю всієї апаратури. При цьому маємо змогу спостерігати, що знімає камера, та здійснювати перемикання на іншу камеру для зміни ракурсу.



Загальна схема розподілу основних компонентів потокової трансляції

Технічні характеристики (орієнтовні) головного комп'ютера:

- процесор Intel I 7 із частотою 3,6 ГГц, кількість ядер — 4, кількість потоків — 8;
- оперативна пам'ять — 16 Гбайт;
- відеокарта — 2 Гбайт;
- блок живлення — 1 кВт.

Технічні характеристики (орієнтовні) резервного комп'ютера:

- процесор Intel I 3 із частотою 1,8 ГГц, кількість ядер — 2, кількість потоків — 4;
- оперативна пам'ять — 8 Гбайт;
- відеокарта — 1 Гбайт;
- блок живлення — 0,65 кВт.

На комп'ютерах має бути інстальоване спеціалізоване програмне забезпечення:

- програма Wirecast або vMix для онлайн трансляції;
- професійний відео- та аудіоредактор.

Проміжна ланка

Стрим-сервер, який обслуговує потокову трансляцію на її шляху від джерела до кінцевого споживача, складається з апаратної частини (комп'ютера) та встановленого на ній програмного додатка, який опрацьовує передавання потокового відео.

Wirecast — програмне забезпечення для онлайн відеотрансляцій, що виступає як альтернатива дорогим апаратним вирішенням з організації відеотрансляцій в мережі Інтернет.

Wirecast має версію Pro з інтегрованою підтримкою карт захвату Blackmagic. Окрім того, підтримуються високоякісні відеоформати Main Concept H.264 і On2 VP6 Flash.

Отже, аби виробляти й транслювати шоу, зовсім не обов'язково бути телевізійником і мати відповідний бюджет. Використовуючи Wirecast, завдяки підтримці карт захоплення Blackmagic і формату Main Concept H.264, можна за секунди створювати професійне шоу і розсилати його в будь-які точки світу.

Інструмент живого відеомовлення Wirecast 6 дозволяє Mac і PC користувачам створювати в реальному часі відеотрансляції в інтернеті. Нові функції включають у себе вдосконалені шаблони lower-thirds (тексту в нижній частині екрана) і підтримку плат Blackmagic Intensity Pro, Decklink SDI і Decklink Duo. На додаток до віртуальних 3D шаблонів у Wirecast Pro надається підтримка HDV і IP камер, плюс стандартні функції регулятора звуку із синхронізатором затримки.

Програма vMix — це сучасний багатофункціональний відеомікшер, який дозволяє легко компонувати відео високого розрізнення. У програмі є безліч функцій та інструментів, що уможливлюють створення високоякісного ролика з просунутими графічними ефектами переходів від кадру до кадру. Працює програма з великою кількістю форматів (AVI, WMV, MPEG, QuickTime). Вона дозволяє здійснити захват екрана віддаленого комп'ютера, із накладанням зображень, записати готовий ролик на диск, скористатися готовими шаблонами і створити «картинку в картинці». До того ж, vMix підтримує багато різноманітних графічних ефектів. Набір стандартних інструментів для обробки відеофайлів допоможе змінити колірний баланс, контраст, насиченість, масштаб, різкість та інші параметри запису. Користувальницький інтерфейс справляє приємне враження завдяки простоті та естетичності. До швидкодії vMix претензій також не виникає.

Використання штучного інтелекту

Будь-яку систему, що містить процесор, вже можна вважати системою інтелектуальною. Штучний інтелект (ШІ) — це доволі розпливчасте поняття, але коли йдеться про ШІ, мають на увазі сукупність платформ, від взаємодії яких отримується очікуваний результат.

Здебільшого ШІ (робот) використовується в сервісах відео за запитом, де сукупність багатьох алгоритмів здійснює аналіз багатьох критеріїв, за якими в робота формується розуміння, що́ саме схильний переглядати той чи інший користувач сервісу, і пропонує йому музику або відео за його інтересами. Такі системи швидко прогресують і все більше приваблюють користувачів.

Один із характерних алгоритмів передбачає такі дії: якщо користувач слухає музику за запитом, то система встановлює, які саме групи, який стиль музики подобається користувачеві, а також аналізує власні плейлісти інших користувачів, інтереси яких близькі до інтересів даного користувача. Далі система виокремлює треки, що найчастіше

трапляються в інших користувачів. Зрештою алгоритм здійснює найбільш прийнятний вибір і пропонує його користувачеві, який надає перевагу схожій музиці.

Кінцеві пристрої для перегляду стримінгу

Комп'ютер або мобільний пристрій для перегляду потокової трансляції має бути оснащений спеціальним програмним забезпеченням, програмою-плеєром. Це можуть бути такі програми:

- Flash медіаплеєр (безкоштовний популярний програвач мультимедіа для перегляду у форматі Flash);
- HTML5 відеоплеєр (HTML5 video — елемент, що входить у проект специфікації HTML5 /HyperText Markup Language ver. 5/, який використовується для відтворення відеозаписів; існує багато безкоштовних плеєрів, які підтримують цей формат);
- VLC плеєр (безкоштовний багатоплатформовий медіаплеєр).

Популярні відеокодеки (програми/алгоритми стиснення даних відеопотоку і відновлення стиснених даних):

- H.264, H.263, VP6.

Популярні аудіокодеки (програми/алгоритми стиснення та відновлення аудіопотоку):

- MP3, AAC.

Необхідна швидкість для стриму після ділення максимального показника зі Speedtest на 2,5:

- 480 p — від 5 Мбіт/с;
- 720 p — від 10 Мбіт/с;
- 1080 p — від 20 Мбіт/с

Варто наголосити, що коли виходять граничні показники, то проводити стрим такої високої якості завжди ризиковано. Навіть невелике відхилення і просідання швидкості може сильно вплинути на якість передавання стриму [3].

ВИСНОВКИ

♦ Інтернет-студія — це альтернатива щодо професійних студій, які працюють у телецентрах. Адже вона дешевша, мобільніша, простіша і здатна транслювати матеріал в інтернет.

♦ У сучасному соціумі інтернет-ТБ все активніше становить конкуренцію традиційним медіаресурсам, а його масштаби набувають колосального розмаху, оскільки глядач може використовувати масу можливостей, про які й не йшлося в разі аналогового сигналу.

♦ Аналіз сучасного стану систем інтернет-телебачення показав, що сьогодні інтернет-технології вельми перспективні стосовно передавання відеоінформації. В інтернет-мережах база єдиної транспортної інфраструктури може інтегрувати всі види додатків в єдину сервіс-орієнтовану технологічну платформу, яка дозволить не тільки забезпечувати традиційний перегляд телевізійних каналів та аудіоконтент високого рівня якості, а й упроваджувати абсолютно нові послуги, які перетворюють інтернет-ТБ на революційну технологію в цифровому телебаченні.

♦ Ще одне революційне досягнення полягає в тому, що для керування контентом телебачення люди майже зовсім будуть не потрібні. Нейромережа (ШІ) самостійно буде обирати найцікавіший матеріал для глядачів (якщо це стримінг у реальному часі), або якщо це буде сервіс відео за запитом (youtube тощо), то ШІ буде налаштовуватись на вимоги кожного користувача і пропонувати контент саме за його інтересами. При цьому ШІ розумітиме, що саме зображено на відео, які емоції та події відтворюються, і пропонувати контент, знаючи настрій користувача.

Список використаної літератури

1. ***Забровский, А.*** *Потоковое вещание (Live streaming). Общая информация [Електронний ресурс] / Анатолий Забровский // IT и Мультимедиа. Опубліковано 04.12.2012.— URL: http://itmultimedia.ru/potokovoe-veshhanie-live-streaming-obshhaya-informaciya/*

2. ***H.264*** *// Wikipedia. Редакція від 15.05.2016 [Електронний ресурс].— URL: https://ru.wikipedia.org/wiki/H.264*

3. ***Какой*** *комп и интернет нужен для стрима? [Електронний ресурс].— URL: http://veestream.ru/twitch/kakoy-komp-i-internet-nuzhen-dlya-strima/*

Рецензент: доктор техн. наук, ст. наук. співробітник **М. М. Степанов**, Державний університет телекомунікацій, Київ.

Д. С. Оленич, А. Ю. Поглубко, Н. А. Клиновский

ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ИНТЕРНЕТ-ВЕЩАНИЯ И РОЛЬ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В МЕДИАПРОСТРАНСТВЕ

В статье рассмотрены основные компоненты потоковой трансляции, а также оборудование для передачи данных при помощи стриминга.

Ключевые слова: потоковое вещание; видеокамеры; стрим-сервер; сервисы; искусственный интеллект; кодер; видеокодек; аудиокодек; компьютер; мобильное устройство; интернет.

D. S. Olenich, A. Y. Poglubko, M. O. Klynovskyi

PERSPECTIVE TECHNOLOGIES INTERNET BROADCASTING AND THE ROLE OF INTELLIGENT SYSTEMS IN MEDIA SPACE

The article considers the main components of streaming and equipment for data transmission using streaming.

Keywords: streaming; video cameras; a stream server; services; artificial intelligence; an encoder; a video codec; an audio codec; a computer; a mobile device; the internet.

УДК 321.396
О. С. ІВАНИЧЕНКО;
Є. В. ГАВРИЛКО, доктор техн. наук, ст. наук. співробітник,
Державний університет телекомунікацій, Київ

Технологія Wi-Fi та її основні характеристики

Розглянуто головні характеристики безпроводової технології Wi-Fi та її компоненти.
Ключові слова: Wi-Fi; адаптер; точка доступу; Wi-Fi мережа; WEP-ключ; IEEE; інтернет.

ВСТУП

Безпроводові мережі Wi-Fi відіграють важливу роль у сучасному технологічному світі: до цих мереж під'єднано мільярди мобільних пристроїв. При цьому більшість підімкнень до інтернету здійснюється з використанням безпроводових мереж. За даними Juniper Research, до 2019 року через них проходитиме понад 60% мобільного трафіку. Глобальний ринок Wi-Fi, що 2015 року становив $14,8 млрд, зросте до $33,6 млрд уже на початку 2020 року. Із поширенням інтернету речей і автомобільних хот-спотів мережі Wi-Fi стануть основною сполучною ланкою інформаційного простору. Більшість користувачів слово Wi-Fi тлумачать як засіб підімкнення до інтернету. Але насправді Wi-Fi є стандартом безпроводового під'єднання до локальної мережі. Простіше кажучи, Wi-Fi — це система, здатна об'єднувати безліч пристроїв і оснащена маршрутизатором (роутером), який може бути підімкнений до інтернету. При цьому немає потреби використовувати проводи, завдяки чому підімкнення можливе «на льоту», скажімо під час пішохідної прогулянки або їзди на велосипеді.

Мережі Wi-Fi здобули визнання індустрії, демонструючи переваги щодо кабельних мереж за багатьма параметрами.

По-перше, вони зручніші в модифікації: зробити перестановку в кабінеті, додати або прибрати робоче місце — усе це не вимагає додаткових витрат на зміну топології мережі.

По-друге, мережі Wi-Fi, усупереч усталеній думці, гарантують достатньо високий рівень безпеки. Адже зняти інформацію набагато легше з кабелю, ніж із зашифрованого радіоканалу, який до того ж змінює частоту передавання даних. Єдине, що призводить до уразливості мереж Wi-Fi, — хибне налаштування. Отже, головне — правильно настроювати механізми шифрування та інші захисні засоби. Інакше ви полегшуєте зловмисникам життя, надаючи їм дуже простий спосіб проникнення у вашу мережу.

ОСНОВНА ЧАСТИНА

Wi-Fi — це сучасна безпроводова технологія, що найшвидше розвивається і уможливлює доступ до інтернету за допомогою спеціальних радіоточок доступу.

Ядром безпроводової мережі Wi-Fi слугує ***точка доступу*** (AP), що підмикається до деякої наземної мережної інфраструктури (каналів інтернет-провайдера), забезпечуючи передавання радіосигналу. Точка доступу — це «прозорий» міст, що сполучає станції, які обладнано безпроводовими мережними картами, із комп'ютерами, об'єднаними в мережу за допомогою проводів. Завдяки точкам доступу безпроводові робочі станції можуть, у свою чергу, бути швидко об'єднані в мережу.

Точка доступу складається із приймача, передавача, інтерфейсу для підімкнення до проводової мережі та програмного забезпечення з обробки даних. Навколо точки доступу формується територія радіусом 50…100 м, котру називають ***хот-спотом***, або ***зоною Wi-Fi***, у межах якої можна користуватися зазначеною мережею.

У разі кількох підімкнень до однієї і тієї самої точки смуга пропускання (наприклад, 11 Мбіт/с — стандарт 802.11b) поділяється на частини, кількість яких дорівнює кількості під'єднаних користувачів. Так, троє користувачів, підімкнених до DWL-1000AP, отримають по 3,67 Мбіт/с (11/3 = 3,67). Теоретично обмежень щодо кількості підімкнень немає, але на практиці є сенс під'єднувати не більш як 10–15 користувачів.

Аби під'єднатися до точки доступу, власникові ноутбука або мобільного пристрою із Wi-Fi адаптером достатньо просто опинитися в радіусі її дії. Усі функції з визначення пристрою та налаштування мережі більшість операційних систем комп'ютерів і мобільних пристроїв виконують автоматично. Якщо користувач одночасно потрапляє в кілька Wi-Fi зон, то підімкнення здійснюється до точки доступу, що забезпечує найсильніший сигнал.

Під'єднатися до мережі Wi-Fi можна за допомогою ноутбуків і кишенькових комп'ютерів, бо практично всі новітні пристрої такого типу є Wi-Fi сумісні. Утім і власники далеко не нових мобільних ПК також можуть легко використати цю зручну технологію, уставивши в PCMCIA слоти своїх комп'ютерів спеціальні Wi-Fi картки або здійснивши під'єднання зовнішнього Wi-Fi пристрою через USB-порт.

Основні елементи мережі Wi-Fi

Для побудови безпроводової мережі використовуються ***Wi-Fi адаптери***, а також згадувані вже ***точки доступу***.

Адаптер — це пристрій, який підмикається через слот розширення PCI, PCMCIA, CompactFlash. Існують також адаптери з підімкненням через порт USB 2.0. При цьому Wi-Fi адаптер виконує ту саму функцію, що й мережна карта в проводовій мережі, уможливлюючи під'єднання комп'ютера користувача до безпроводової мережі. Завдяки платформі Centrino всі сучасні ноутбуки мають вбудовані адаптери Wi-Fi, сумісні з багатьма сучасними стандартами. Wi-Fi адаптерами, як правило, забезпечені й кишенькові персональні комп'ютери — КПК, що дозволяє під'єднувати їх до безпроводових мереж.

Для доступу до безпроводової мережі адаптер може встановлювати зв'язок безпосередньо з іншими адаптерами. Така мережа називається одноранговою мережею, або Ad-Hoc («до випадку»). Адаптер може встановлювати зв'язок і через точку доступу. Тоді йдеться про інфраструктурний режим.

При виборі способу підімкнення адаптер має бути налаштований на використання або Ad-Hoc, або інфраструктурного режиму.

Точка доступу — це, по суті, автономний модуль із вбудованим мікрокомп'ютером і приймально-передавальним пристроєм.

Через точку доступу здійснюється взаємодія і обмін інформацією між безпроводовими адаптерами, а також забезпечується зв'язок із проводовим сегментом мережі. Таким чином, точка доступу відіграє роль комутатора.

Точка доступу має мережний інтерфейс (uplink port), за допомогою якого вона може бути під'єднана до звичайної проводової мережі. Через цей самий інтерфейс може здійснюватися і налаштування точки.

Точка доступу може використовуватися як для підімкнення до неї клієнтів (базовий режим точки доступу), так і для взаємодії з іншими точками доступу з метою побудови розподіленої мережі (*Wireless Distributed System* — **WDS**). Це режими безпроводового моста «точка–точка» і «точка–багато точок», безпроводового клієнта і повторювача.

Доступ до мережі забезпечується передаванням широкосмугових сигналів через ефір. Приймальна станція може отримувати сигнали в діапазоні роботи кількох передавальних станцій. Станція-приймач використовує ідентифікатор зони обслуговування (*Service Set IDentifier* — **SSID**) для фільтрації отримуваних сигналів і виділення того, який їй потрібний.

Захищеність Wi-Fi мережі

Безпроводову мережу вважають захищеною, якщо в ній функціонують три основні складові системи безпеки: *автентифікація* користувача, *конфіденційність* і *цілісність* передавання даних. Для досягнення достатнього рівня безпеки необхідно скористатися низкою правил при організації і настроюванні приватної Wi-Fi мережі:

1) шифрувати дані з використанням різних систем. Максимальний рівень безпеки забезпечить застосування VPN;

2) використовувати протокол 802.1X;

3) заборонити проникнення в налаштування точки доступу за допомогою безпроводового підімкнення;

4) управляти доступом клієнтів за MAC-адресами;

5) заборонити трансляцію в ефір ідентифікатора SSID;

6) розташовувати антени якомога далі від вікон і зовнішніх стін будівлі, а також обмежувати потужність радіовипромінювання;

7) використовувати максимально довгі ключі;

8) змінювати статичні ключі та паролі;

9) використовувати метод WEP автентифікації Shared Key оскільки клієнтові для входу в мережу необхідно буде знати WEP ключ;

10) користуватися складним паролем для проникнення в налаштування точки доступу.

Який стандарт Wi-Fi для смартфона найкращий

Усі сучасні смартфони обладнано модулем Wi-Fi, розрахованим на роботу з кількома версіями 802.11. Як правило, підтримуються всі взаємно сумісні стандарти: b, g і n. Утім робота з останнім нерідко може відбуватись тільки на частоті 2,4 ГГц. Пристрої, здатні працювати в мережах 802.11n 5 ГГц, також забезпечують підтримку 802.11a.

Зростання частоти сприяє збільшенню швидкості обміну даними, хоча при цьому зменшується довжина хвилі та ускладнюється проходження через перешкоди. Саме тому теоретична дальність зв'язку 2,4 ГГц буде вища, ніж у разі 5 ГГц. Проте на практиці ситуація дещо інша. Діапазон 5 ГГц ширший (від 5170 до 5905 МГц) і менш завантажений. Тому хвилі гірше долають перешкоди (стіни, меблі, тіло людини), зате в умовах прямої видимості забезпечують більш стійкий зв'язок.

З огляду на це смартфони з підтримкою IEEE 802.11ac у діапазоні 5 ГГц забезпечують високу швидкість передавання та якість сигналу, достатню для покриття квартири, а мережа менш потерпає від впливу перешкод. А оскільки всі смартфони з підтримкою 802.11ac працюють і з більш ранніми версіями стандарту, то за наявності перешкод пристрій автоматично підмикатиметься до будь-якої точки доступу.

Огляд стандартів технології Wi-Fi

Інститут інженерів з електротехніки та електроніки (*Institute of Electrical and Electronics Engineers*, **IEEE**) — міжнародна організація інженерів у галузі електротехніки, радіоелектроніки та радіоелектронної промисловості, світовий лідер у сфері розроблення стандартів з електроніки та електротехніки. Штаб-квартиру організації розташовано в США, штат Нью-Джерсі.

Існує низка стандартів сімейства IEEE 802.11, зокрема 802.11, 802.11a, 802.11b, 802.11c, 802.11d, 802.11e і багато інших. Але на практиці здебільшого використовуються всього три, що їх визначив IEEE: 802.11b, 802.11g і 802.11a.

IEEE802.11 — початковий стандарт безпроводових локальних мереж на базі передавання даних у діапазоні 2,4 ГГц. Підтримує обмін даними зі швидкістю до 1-2 Мбіт/с. Прийнятий 1997 року.

IEEE802.11a — стандарт безпроводових локальних мереж на базі безпроводового передавання даних у діапазоні 5 ГГц. Діапазон поділено на три неперетинні піддіапазони. Максимальна швидкість обміну даними становить 54 Мбіт/с, при цьому доступні також швидкості 48, 36, 24, 18, 12, 9 і 6 Мбіт/с.

IEEE802.11b — стандарт безпроводових локальних мереж на базі передавання даних у діапазоні 2,4 ГГц. Він був прийнятий 1999 року в розвиток прийнятого раніше стандарту IEEE 802.11. У всьому діапазоні існують три неперетинні канали, тобто на одній території, не впливаючи одна на одну, можуть працювати три різні безпроводові мережі. Передбачено два типи модуляції — DSSS і FHSS. Максимальна швидкість роботи становить 11 Мбіт/с; доступні також швидкості 5,5; 2 і 1 Мбіт/с; автоматичне зниження швидкості при погіршенні якості сигналу [3]. Продукти стандарту IEEE 802.11b, що їх поставляють різні виробники, тестуються на сумісність і сертифікуються організацією *Wireless Ethernet Compatibility Alliance* (**WECA**), відомою під назвою Wi-Fi Alliance.

IEEE802.11b+ — поліпшена версія стандарту 802.11b у виконанні окремих виробників, що забезпечує підвищення швидкості обміну даними. В інтерпретації компанії Texas Instruments відрізняється від оригінального варіанта модуляцією **PBCC** (*Packet Binary Convolutional Coding*), подвоєною (до 22 Мбіт/с) максимальною швидкістю. Також анонсувалися рішення з продуктивністю, збільшеною до 44 Мбіт/с.

IEEE802.11e — стандарт, головне призначення якого пов'язане з використанням засобів мультимедіа. Він обумовлює механізм призначення пріоритетів різним видам трафіку, таким як аудіо- і відеододатки. Вимога щодо якості запиту така сама, як для всіх радіоінтерфейсів IEEE WLAN.

IEEE802.11g — стандарт безпроводових локальних мереж на основі передавання даних у діапазоні 2,4 ГГц. Він новіший за стандарт 802.11b. Максимальна швидкість передавання даних становить 54 Мбіт/с. Діапазон поділено на три неперетинні канали, тобто на одній території без взаємовпливу можуть працювати три різні мережі. Для збільшення швидкості обміну даними при ширині каналу, як у стандарті 802.11b, розроблено метод модуляції з ортогональним частотним мультиплексуванням (**OFDM** — *Ortogonal Frequency Division Multiplexing*), а також метод двійкового пакетного згорткового кодування **PBCC** (*Packet Binary Convolutional Coding*). Серед переваг 802.11g слід відзначити низьку споживану потужність, велику дальність дії та високу проникаючу здатність сигналу. Можна сподіватися й на розумну вартість обладнання, оскільки низькочастотні пристрої простіші у виготовленні.

IEEE802.11i — стандарт, що усуває недоліки у сфері безпеки попередніх стандартів. Він розв'язує проблеми захисту даних канального рівня, дозволяючи створювати безпечні безпроводові мережі практично будь-якого масштабу.

IEEE802.11e — додатковий стандарт, що дозволяє забезпечити гарантовану якість обміну даними (**QoS** — *Quality of service*) завдяки переставленню пріоритетів різних пакетів; необхідний для роботи таких потокових сервісів, як VoIP або IP-TV.

IEEE802.11n — стандарт останнього покоління на базі передавання даних у діапазоні 2,4 ГГц. Цей стандарт значно перевищує за швидкістю обміну даними попередні стандарти 802.11b і 802.11g, забезпечуючи швидкість на рівні Fast Ethernet; зворотно сумісний із 802.11b і 802.11g. Основна відмінність від попередніх версій Wi-Fi — додавання до фізичного рівня (PHY) підтримки протоколу **MIMO** — *Multiple-Input Multiple-Output*.

ВИСНОВКИ

Конвергенція обчислювальної, комунікаційної та мобільної технологій стимулює в усьому світі попит на безпроводові вирішення, що дозволяють незмінно залишатися на зв'язку — в будь-який час і в будь-якому місці. Із поширенням безпроводових технологій кінцеві користувачі прагнуть отримати для роботи та розваг такі вирішення, які мають відповідати їх мобільному стилю життя. Зручність використання та висока захищеність дозволяють застосовувати зазначені технології і в домашніх умовах.

Таким чином, Wi-Fi розв'язує три важливі завдання:

1) спростити спілкування з мобільним комп'ютером;

2) забезпечити комфортні умови для роботи діловим партнерам, які завітали в офіс зі своїм ноутбуком;

3) створити локальну мережу в приміщеннях, де прокладання кабелю неможливе або надто витратне.

Завдяки технології Wi-Fi є змога встановлювати бюджетні варіанти безпроводових мостів, виконання та налаштування яких не вимагає жодних специфічних знань і навичок з програмування, (у web-інтерфейсі точок доступу можуть розібратися практично всі). Безпроводові мости Wi-Fi можуть працювати на відстанях до 15–20 км за умови прямої видимості.

Список використаної літератури

1. ***Безпровідна*** *мережа Wi-Fi [Електронний ресурс].— URL: http://www.bestreferat.ru/referat-184480.html*

2. ***Wi-Fi*** *[Електронний ресурс].— URL: http://ua.gecid.com/netlan/wi-fi_-_razvitie_i_osnovnyee_prinjipye_samogo_rasprostranennogo_standarta_besprovodnyeh_seteyi/?s=all*

Рецензент: доктор техн. наук, професор **Л. Н. Беркман**, Державний університет телекомунікацій, Київ.

А. С. Иваниченко, Е. В. Гаврилко

ТЕХНОЛОГИЯ Wi-Fi И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Рассмотрены главные характеристики беспроводной технологии Wi-Fi и ее компоненты.

Ключевые слова: Wi-Fi; адаптер; точка доступа; Wi-Fi сеть; WEP ключ; IEEE; интернет.

O. S. Ivanichenko, E. V. Havrylko

Wi-Fi TECHNOLOGY AND ITS MAIN FEATURES

The article describes the main features wireless technology Wi-Fi and its components.

Keywords: Wi-Fi adapter; access point; Wi-Fi network; WEP key; IEEE; Internet.

УДК 681.883

М. П. ТРЕМБОВЕЦЬКИЙ, доктор техн. наук, ст. наук. співробітник;
Є. В. ІВАНІЧЕНКО, аспірант;
А. П. БОНДАРЧУК, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

Розв'язання задач цифрової обробки даних за допомогою операторів з унітарною нелінійністю

Стрімкий розвиток техніки й технологій у сфері цифрової обробки сигналів (ЦОС) дає поштовх до поліпшення відомих і розробки нових алгоритмів, що мають високу прикладну цінність. Скажімо, для аналогової фільтрації сигналів хоча й існувала математична модель, вона, утім, через недосконалість технічної бази не піддавалась реалізації. Натомість завдяки використанню ЦОС є змога формувати спектр сигналу в будь-якому базисі, виконуючи всілякі перетворення — як лінійні, так і нелінійні. Саме ці переваги ЦОС і становлять головний предмет пропонованої статті.

Ключові слова: цифрова обробка сигналів (ЦОС); нелінійні ортогональні перетворення; завадозахищеність каналу зв'язку; нелінійне рівняння Шредінгера.

Вступ. Постановка проблеми

Один із методів, широко застосовуваних у ЦОС, — це метод подавлення зосереджених завад (ЗЗ) у каналах зв'язку. Базується він на вибірковому стисненні спектра завади без спотворення спектра сигналу. Досягти такого результату вдається лише з використанням нелінійних ортогональних перетворень (НОП).

Цю ідею вперше висловили та втілили в життя такі вчені, як С. М. Широков і А. В. Петров. Загалом результати їхніх досліджень стосуються оптимального вибору параметрів нелінійних перетворень сигналів. Далі наведено приклади ефективного використання цього методу на практиці.

Основна частина

Виконуючи теоретичний аналіз сигналів і спектрів, їх інтерпретують як функції неперервних аргументів. При цьому нелінійне перетворення спектра здійснюється, здебільшого, за допомогою операторів з унітарною нелінійністю, які подаються нелінійним рівнянням Шредінгера (НРШ)

$$i\frac{\partial\psi}{\partial\eta}+\alpha\frac{\partial^2\psi}{\partial\omega^2}+f\left(\psi\right)\psi=0, \qquad (1)$$

де $\psi(\eta, \omega)$ — нормована спектральна функція, залежна від частоти ω та допоміжної змінної η.

Зауважимо, що математична модель (1) дозволяє розглядати спектр як функцію частоти з певними значеннями в гільбертовому просторі.

Рівняння (1) добре відоме. Використовується воно в багатьох розділах фізики і докладного розгляду не потребує. Нелінійне ортогональне перетворення, що його описує цей вираз, після відповідної дискретизації за змінними η і ω здійснюється методами ЦОС за допомогою ланцюжка дискретних перетворень — як лінійних, так і нелінійних.

Варто наголосити, що будь-яке НОП має таку важливу властивість: зі збільшенням кількості ланок у зазначеному ланцюжку результат НОП дедалі менше залежить від початкових умов і форми спектра ЗЗ. Завдяки цій властивості уможливлюється подавлення широкого класу ЗЗ без змін алгоритмів обробки сигналу.

Теоретично стаціонарну форму перетвореного спектра можна розрахувати за допомогою відомого методу [5]. Для цього необхідно подати $\psi(\eta, \omega)$ у вигляді

$$\psi(\eta, \omega) = \rho_c(\omega)\exp(-i\gamma\eta). \quad (2)$$

Підставивши (2) в (1) і виконавши певні перетворення, дістанемо рівняння вигляду

$$\gamma\rho_c^2 + \alpha(\rho_c)^2 + k\rho_c^4 = 0, \quad (3)$$

яке при певних значеннях γ, α і k матиме такий розв'язок:

$$\rho_c(\omega) = \rho_{c0}\,\mathrm{sech}(\omega/\omega_{сп}), \quad (4)$$

де ρ_{c0} — значення амплітуди перетвореного спектра ЗЗ; $\omega_{сп}$ — ширина цього спектра.

Звідси випливає, що в разі достатньо великої кількості ланок НОП забезпечується перетворення спектра ЗЗ до вигляду, що задовольняє умови солітонного розв'язку НРШ у формі гіперболічного секанса [4]. Результати комп'ютерного моделювання перетворень ЗЗ із різною шириною спектра унаочнюють графіки, подані на рис. 1 і 2, де зображено ЗЗ та їхні обвідні.

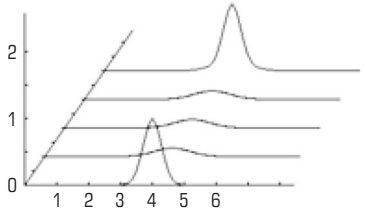


Рис. 1

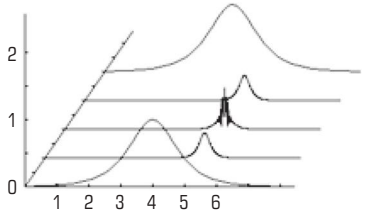


Рис. 2

У плані нашого дослідження значний інтерес становить стійкість виконуваного перетворення до змін форми обвідної ЗЗ. Адже інтенсивність виникнення завад у каналах зв'язку досить хаотична.

Застосувавши метод [5], подамо обвідну вихідного спектра ЗЗ у вигляді

$$\psi(\omega) = \rho_0(\omega) + \delta\psi(\omega), \quad (5)$$

де $\rho_0(\omega)$ — детермінована складова, а $\delta\psi(\omega)$ — випадкова складова спектра ЗЗ, яка характеризує флуктуації в каналі. Виконавши перетворення виразу (1) з урахуванням (5), дістанемо систему рівнянь

$$\begin{cases} \dfrac{\partial}{\partial\eta}\mathrm{Re}\,\delta\psi(\eta,\omega) = -j\alpha\dfrac{\partial^2}{\partial\omega^2}\mathrm{Im}\,\delta\psi(\eta,\omega), \\ \dfrac{\partial}{\partial\eta}\mathrm{Im}\,\delta\psi(\eta,\omega) = j\alpha\,\mathrm{Re}\,\psi(\eta,\omega) - \gamma\,\mathrm{Re}\,\psi(\eta,\psi). \end{cases} \quad (6)$$

Розв'язуючи цю систему рівнянь, знаходимо дисперсійне співвідношення, яке вказує на можливу нестійкість перетворення, оскільки дисперсійний параметр є уявний.

Незважаючи на те, що як теоретично, так і практично було доведено такий факт: за певного вибору параметрів можна досягти достатньо стійкого процесу формування солітоноподібного імпульсу [1], усе ж у даному випадку оптимізація вибору параметрів за заданим критерієм стикається зі значними труднощами, коли доводиться використовувати чисельні методи аналізу.

Утім потрібні оцінки можна дістати для частинного випадку, коли нелінійна функція у виразі (1) набирає вигляду $f(\psi) = k|\psi|^2$.

Розв'язок такого рівняння можна подати в континуально-інтегральній формі, скориставшись методом Фейнмана:

$$\psi(\eta, \omega) = \int_{-\infty}^{\infty}\psi_0(\theta)G. \quad (7)$$

Тут $\psi(\theta) = \psi(\theta, \eta = 0)$; $G(\cdot)$ — функція Гріна, яка подається за допомогою континуального інтеграла такого виду:

$$G(\theta, \omega, \eta) = \int\exp\left[-\int_0^{\eta}L\left(\omega(x), \dot{\omega}(x)\right)dx,\right]D\omega(x), \quad (8)$$

де $L\left(\omega(x), \dot{\omega}(x)\right) = \omega^2(x) + k|\psi(\omega(x), x)|^2$;

$D\omega(x)$ — оператор диференціювання.

За допомогою цього виразу можна виконувати інтегрування по нескінченній кількості траєкторій, які пов'язують точки обвідної з координатами θ, 0, ω.

У загальному вигляді аналітичний розв'язок розглядуваного рівняння не існує. Задачі, які тут постають, можна розв'язати за допомогою методу оптимізації, відомого як *наближення заданого каналу* [3]. Тут ідеться про НОП, яке включає в себе тільки дві ланки — лінійну і нелінійну.

Як приклад можна розглянути ЗЗ із флуктуаційною складовою спектра виду

$$\delta\psi(\eta,\omega)=\xi(\omega)\operatorname{sech}(\omega/\omega_{33}), \quad (9)$$

де $\xi(\omega)$ — випадкова функція частоти з гауссівським розподілом.

Стійкість такого перетворення залежить від інтервалу кореляції випадкового процесу

$$q(t)=\int_{-\infty}^{\infty}\xi(\omega)\exp(j\omega t)d\omega. \quad (10)$$

У разі, коли інтервал співрозмірний із тривалістю ЗЗ, то перетворення стійке. Якщо це не так, то ЗЗ та її спектр розкладаються на послідовність випадково розподілених складових, кількість яких залежить від інтервалу кореляції. Результат комп'ютерного моделювання, який підтверджує цей висновок, наведено на рис. 3.

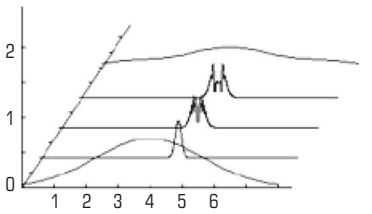


Рис. 3

Висновок

Наведені результати засвідчують ефективність методик підвищення завадозахищеності каналів зв'язку зі складними видами завад на основі нелінійних методів цифрової обробки сигналів.

Список використаної літератури

1. ***Теория*** *электрической связи / [А. Г. Зюко, Д. Д. Кловский, В. И. Коржик, М. В. Назаров; под ред. Д. Д. Кловского].— М.: Радио и связь, 1998.— 432 с.*

2. ***Кловский, Д. Д.*** *Передача дискретных сообщений по радиоканалам / Д. Д. Кловский.— М.: Радио и связь, 1982.— 304 с.*

3. ***Агаян, С. С.*** *Оптимальные методы зонного кодирования посредством дискретных ортогональных преобразований / С. С. Агаян, А. А. Петросян.— М., 1989.*

4. ***Лайонс, Р.*** *Цифровая обработка сигналов / Ричард Лайонс.— М., 2006.— 656 с.*

5. ***Агаян, С. С.*** *Оптимальные алгоритмы ортогональных преобразований и их реализация на ЭВМ / С. С. Агаян // Кибернетика и вычислительная техника.— 1986.— Вып. 2.— С. 231–319.*

Рецензент: доктор техн. наук, ст. наук. співробітник **М. М. Степанов,** Державний університет телекомунікацій, Київ.

М. П. Трембовецкий, Е. В. Иваниченко, А. П. Бондарчук

РЕШЕНИЕ ЗАДАЧ ЦИФРОВОЙ ОБРАБОТКИ ДАННЫХ ПРИ ПОМОЩИ ОПЕРАТОРОВ С УНИТАРНОЙ НЕЛИНЕЙНОСТЬЮ

Ускоренное развитие техники и технологий в области цифровой обработки сигналов (ЦОС) стимулирует совершенствование существующих и разработку новых алгоритмов, имеющих высокую прикладную ценность. Например, для аналоговой фильтрации сигналов существовала математическая модель, которая, однако, из-за несовершенства технической базы не подлежала реализации. И только использование ЦОС позволяет формировать спектр сигнала в любом базисе, осуществляя различные преобразования — как линейные, так и нелинейные. Именно указанные преимущества ЦОС являются предметом данной статьи.

Ключевые слова: цифровая обработка сигналов (*ЦОС)*; нелинейные ортогональные преобразования; помехозащищенность канала связи; нелинейное уравнение Шредингера.

M. P. Trembovetskiy, E. V. Ivanichenko, A. P. Bondarchuk

SOLUTION OF DIGITAL DATA PROCESSING PROBLEMS WITH THE USE OF OPERATORS WITH UNITARY NONLINEARITY

Rapid development of technologies in the field of digital signal processing (DSP) technology provides an impetus for improving existing and developing new algorithms. In particular, when using analog filtering of signals, there was only a mathematical model, because of the imperfection of the technical base there was no implementation. In contrast, when using DSP, it becomes possible to generate a signal spectrum in any basis and perform various transformations, both linear and non-linear, which is the main direction of this article.

Keywords: digital signal processing; nonlinear orthogonal transformation; interference protection of communication channel; nonlinea Schrödinger equation.

УДК 621.391.3

В. В. ДУБРОВСЬКИЙ[1], канд. фіз.-мат. наук, доцент;
С. І. ОТРОХ[2], канд. техн. наук, доцент;
В. І. КРАВЧЕНКО[2], аспірант;
В. О. КУЗЬМІНИХ[3], канд. техн. наук, доцент;
О. І. ГОЛУБЕНКО[2],
[1] Білоруська державна академія зв'язку, Мінськ
[2] Державний університет телекомунікацій, Київ
[3] Національний технічний університет України «КПІ», Київ

Методологія розрахунку завадостійкості багатопозиційних сигнальних сузір'їв

Виконано розрахунок завадостійкості багатопозиційних сигнальних сузір'їв. Доведено ефективність маніпуляційного кодування багатопозиційних сигналів. На основі розрахунків побудовано графіки, що характеризують середню ймовірність помилки при розрізненні пари сигналів кожного розглядуваного сузір'я для заданих значень відношення сигнал/шум. Здійснено порівняльний аналіз квазікогерентного методу демодуляції та неоптимальних методів прийому.

Ключові слова: сигнальні сузір'я; завадостійкість; OFDM сигнали; багатопозиційні сигнали.

Вступ

Нагадаємо, що статистичний метод багаторазової імітації сумарного вектора сигналу і шуму з подальшим прийняттям рішення за правилом Котельникова потребує для достатньої точності не менш ніж $20/P^*$ спроб імітації кожного сигналу, де P^* — середнє значення ймовірності помилки розрізнення сигналів при заданому відношенні сигнал/шум. Через це статистичний розрахунок в області великих відношень сигнал/шум (властивості маніпуляційних кодів проявляються найбільш повно) потребує дуже великої кількості вимірювань. Тому розрахунок виконувався аналітично, методом інтегрування двовимірної функції розподілу щільності ймовірності значень суміші сигналу з білим шумом в областях сигналів. Такий розрахунок дозволяє визначити не лише ймовірності помилок розрізнення кожної пари сигналів сузір'я, а й імовірності помилок у кожному двійковому розряді кодів сигналів.

Основна частина

Як відомо, функції розподілу ймовірностей миттєвих значень сигналу, що включає в себе інформаційний компонент з координатами (x, y) і заваду, котра відповідає моделі білого шуму, подаються такими виразами:

$$\omega(x)=\frac{1}{\sqrt{2x\sigma_x}}e^{-\left[\frac{(\bar{x}-x)^2}{2(\sigma_x)^2}\right]};$$
$$\omega(y)=\frac{1}{\sqrt{2x\sigma_y}}e^{-\left[\frac{(\bar{y}-y)^2}{2(\sigma_y)^2}\right]}. \quad (1)$$

При цьому параметри розподілу ймовірностей значень шуму не залежать від координатної системи приймача:

$$\sigma_x = \sigma_y = \sigma. \quad (2)$$

Тоді інтегральні функції розподілу подаються в такому вигляді:

$$F(X)=\int_{-\infty}^{X}\omega(x)dx=\frac{1}{2x}\int_{-\infty}^{\frac{(\bar{x}-x)}{\sigma}}e^{\frac{z^2}{2}}dz=\Phi(Z)=\Phi\left[\frac{(\bar{x}-x)}{\sigma}\right];$$
$$F(Y)=\int_{-\infty}^{Y}\omega(y)dy=\frac{1}{2x}\int_{-\infty}^{\frac{(\bar{y}-y)}{\sigma}}e^{\frac{z^2}{2}}dz=\Phi(Z)=\Phi\left[\frac{(\bar{y}-y)}{\sigma}\right], \quad (3)$$

де $\Phi(Z)$ — інтеграл Лапласа.

Для сигнальних сузір'їв QAM області сигналів (окрім периферійних сигналів сузір'я) являють собою квадрати, центри яких збігаються із сигнальними точками, а сторони перпендикулярні до відрізків, що сполучають сигнальні точки. У такому разі, згідно з основними положеннями теорії ймовірностей,

інтегральне значення ймовірності прийняття рішення за правилом Котельникова на користь сигнальної точки J при передаванні через канал із білим шумом того сигналу, що відповідає точці I, визначається як імовірність одночасного настання відповідних подій (рис. 1):

$$P_{ij} = Px_{ij}Py_{ij} = (\Phi((x_a - x_i)/\sigma) - \Phi((x_b - x_i)/\sigma))(\Phi((y_c - y_i)/\sigma) - \Phi((y_b - y_i)/\sigma)). \quad (4)$$

Тут Px_{ij} — імовірність потрапляння проекції сигнальної точки на виході каналу з білим шумом у діапазон значень координат x, який належить околу точки J, якщо на вході каналу маємо сигнал I;

Py_{ij} — імовірність потрапляння в діапазон значень координат y, який належить околу точки J, проекції сигнальної точки на виході каналу з білим шумом, якщо на вході каналу маємо сигнал I;

$\Phi((x_a - x_i)/\sigma)$ — значення функції Лапласа, коли аргументом є відношення різниці абсцис точок A та I до дисперсії σ миттєвих значень білого шуму ($\sigma = \sqrt{P_з}$, де $P_з$ — середня потужність завади).

Позначивши $\Delta x = x_j - x_i$, $\Delta y = y_j - y_i$ та врахувавши, що

$$x_a - x_i = 0{,}5d0e, \quad x_b - x_i = 0{,}5d0e, \quad y_c - y_i = 0{,}5d0e, \quad y_b - y_i = 0{,}5d0e,$$

дістанемо:

$$P_{ij} = (\Phi((\Delta x + 0{,}5d0e)/\sigma) - \Phi((\Delta x - 0{,}5d0e)/\sigma))(\Phi((\Delta y + 0{,}5d0e)/\sigma) - \Phi((\Delta y - 0{,}5d0e)/\sigma)). \quad (5)$$

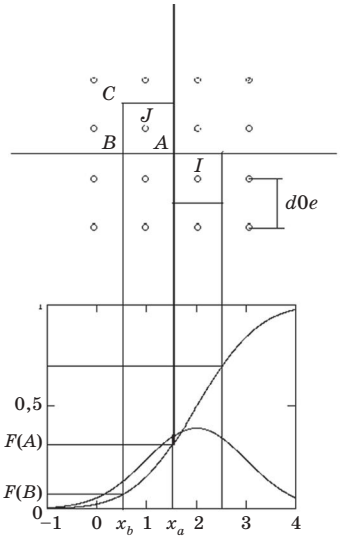


Рис. 1. Функції розподілу ймовірностей амплітуд суміші сигналу з гауссівським шумом в області сигналу сузір'я QAM16

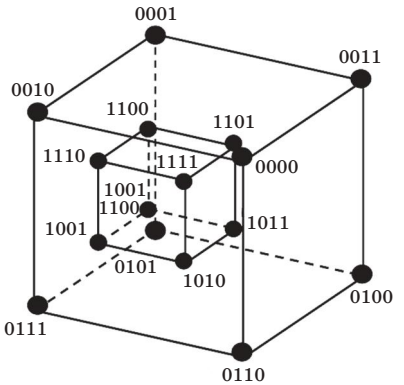


Рис. 2. Оптимальне укладання областей сигналів у тривимірному просторі для 16-позиційного сигналу кубічної амплітудно-фазової модуляції

Формула (5) описує залежність імовірності прийняття рішення про прийом не периферійної точки сузір'я QAM із координатами ($x_i + \Delta x$, $y_i + \Delta y$) при передаванні сигналу (x_i, y_i) через канал із білим шумом.

Для периферійних точок розрахункова формула дещо спрощується. Справді, якщо в (5) одна зі змінних x_a, x_b, y_b або y_c відповідно до положення точки набуває значення ±∞, то один з інтегралів Лапласа набуває значення 0 або 1. Незалежно від того, чому (нулю або одиниці) дорівнює один з інтегралів Лапласа, імовірність Px_{ij} або Py_{ij} набуває того самого значення:

$$\begin{gathered} Px_{ij} = \Phi((\Delta x + 0{,}5d0e)/\sigma) = 1 - \Phi((\Delta x - 0{,}5d0e)/\sigma); \\ Py_{ij} = \Phi((\Delta y + 0{,}5d0e)/\sigma) = 1 - \Phi((\Delta y - 0{,}5d0e)/\sigma); \\ P_{ij} = Px_{ij}Py_{ij}. \end{gathered} \quad (6)$$

Отже, в обох випадках геометричній симетрії сигнального сузір'я відповідає симетрія ймовірностей помилок.

Для кутових периферійних точок розрахункова формула спрощується ще більше. Адже тоді в (5) значення ± ∞ набуває не одна зі змінних x_a, x_b, y_b або y_c, а дві з них. При цьому нулю або одиниці дорівнюють два інтеграли Лапласа.

Аналогічні співвідношення маємо і для сузір'їв НАР. Відмінність полягає у змінних межах інтегралів функції розподілу ймовірностей, що є наслідком шестигранної форми областей сигналів.

Для сигнальних сузір'їв САМ областями сигналів (окрім периферійних сигналів сузір'я) є куби, вершини яких збігаються із сигнальними точками, а ребра перпендикулярні до відрізків, що сполучають сигнальні точки (рис. 2).

Зрештою інтегральне значення ймовірності прийняття рішення визначається ймовірністю:

$$P_{ij} = Px_{ij}Py_{ij} = (\Phi((x_a - x_i)/\sigma) - \Phi((x_b - x_i)/\sigma))(\Phi((y_c - y_i)/\sigma) - \Phi((y_b - y_i)/\sigma))(\Phi((z_c - z_i)/\sigma) - \Phi((z_b - z_i)/\sigma)). \quad (7)$$

Позначивши $\Delta x = x_j - x_i$, $\Delta y = y_j - y_i$, $\Delta z = z_j - z_i$ і врахувавши, що $x_a - x_i = 0{,}5d0e$, $x_b - x_i = 0{,}5d0e$, $y_c - y_i = 0{,}5d0e$, $y_b - y_i = 0{,}5d0e$, $z_c - z_i = 0{,}5d0e$, $z_b - z_i = 0{,}5d0e$, дістанемо:

$$P_{ij} = (\Phi((\Delta x + 0{,}5d0e)/\sigma) - \Phi((\Delta x - 0{,}5d0e)/\sigma))(\Phi((\Delta y + 0{,}5d0e)/\sigma) - \Phi((\Delta y - 0{,}5d0e)/\sigma)) \times$$
$$\times (\Phi((\Delta z + 0{,}5d0e)/\sigma) - \Phi((\Delta z - 0{,}5d0e)/\sigma)). \quad (8)$$

Формула (8) описує залежність імовірності прийняття рішення про прийом не периферійної точки сузір'я CAM із координатами $(x_i + \Delta x, y_i + \Delta y, z_i + \Delta z)$ при передаванні сигналу (x_i, y_i, z_i) через канал із білим шумом.

Для периферійних точок у даному разі розрахункова формула також спрощується. Справді, якщо у (5) одна зі змінних відповідно до положення точки набуває значення $\pm\infty$, то один з інтегралів Лапласа дорівнює нулю або одиниці. Незалежно від того, якого саме значення набуває один із цих інтегралів Лапласа, одна з імовірностей Px_{ij}, Py_{ij} або Pz_{ij} має те саме значення:

$$Px_{ij} = \Phi((\Delta x + 0{,}5d0e)/\sigma) = 1 - \Phi((\Delta x - 0{,}5d0e)/\sigma);$$

$$Py_{ij} = \Phi((\Delta y + 0{,}5d0e)/\sigma) = 1 - \Phi((\Delta y - 0{,}5d0e)/\sigma);$$

$$Pz_{ij} = \Phi((\Delta z + 0{,}5d0e)/\sigma) = 1 - \Phi((\Delta z - 0{,}5d0e)/\sigma);$$

$$P_{ij} = (1 - \Phi((\Delta x - 0{,}5d0e)/\sigma))(1 - \Phi((\Delta y - 0{,}5d0e)/\sigma))(1 - \Phi((\Delta z - 0{,}5d0e)/\sigma)). \quad (9)$$

Отже, в усіх розглянутих випадках геометричній симетрії сигнального сузір'я відповідає симетрія ймовірностей помилок.

Розрахунки було виконано для кожного сигнального сузір'я на базі системи «MathCAD ® v.14 Professional Edition».

Результати розрахунків подано у вигляді графіків (рис. 3 і 4).

Зокрема, наведені на рис. 3 залежності відношень імовірностей $P_{\text{сигн}}$ помилок розрізнення сигналів (усереднених по всіх значеннях у сузір'ї) до ймовірностей P_2 помилок у двійкових розрядах (також усереднених по всіх значеннях у сузір'ї) від значень відношення сигнал/шум у каналі доводять ефективність маніпуляційного кодування.

Справді, маніпуляційні коди сузір'їв QAM (суцільні лінії) забезпечують значно більший виграш у завадостійкості, аніж коди сузір'їв HAP (пунктирні лінії). Це пояснюється тим, що відношення кількості інверсій до кількості мінімальних евклідових відстаней у сузір'ях HAP (6/5) більше, ніж у сузір'ях QAM (4/4). Згідно з графіками найкращий показник демонструє CAM, оскільки евклідова відстань сузір'їв менша, ніж у HAP і QAM. Графіки мають дві ділянки: на першій зі зростанням відношення сигнал/шум зростає частка помилок розрізнення сусідніх сигналів сузір'я, хеммінгова відстань між якими мінімальна. Отже, перша ділянка характеризує виграш, що його забезпечує розроблений маніпуляційний код порівняно з результатом випадкового кодування. Друга ділянка характеризує потенційні можливості коду. При даних значеннях відношення сигнал/шум усі помилки розрізнення сигналів стосуються розрізнення сусідніх сигналів. При відношенні сигнал/шум, близькому до 25 дБ, імовірності помилок у сузір'ях HAP8 і QAM8 (нижні криві на рис. 3) спадають до нуля.

Графіки, що характеризують поводження середньої по сузір'ю ймовірності помилки у двійковому розряді на виході напівнеперервного каналу, зображено на рис. 4.

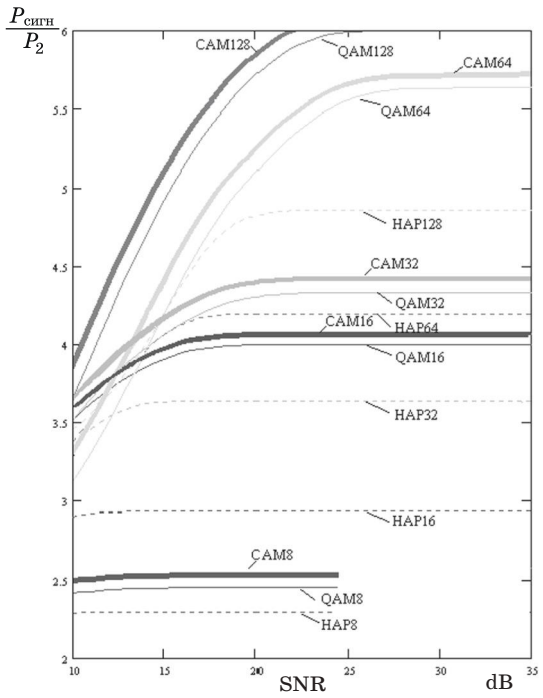


Рис. 3. Ефективність маніпуляційного кодування

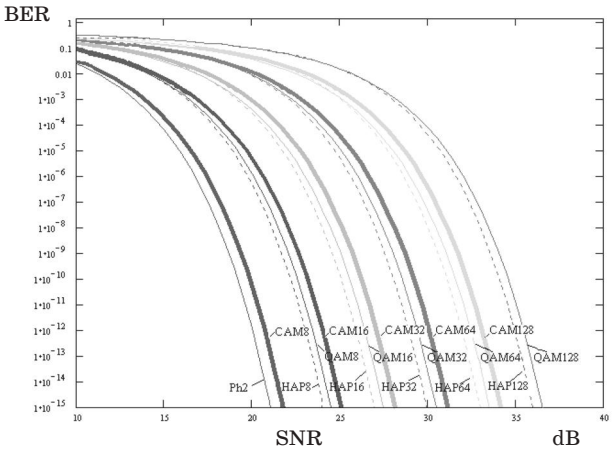


Рис. 4. Абсолютний виграш щодо ймовірності помилки у двійковому розряді

Висновки

Запропоновано метод побудови ефективного цифрового каналу для передавання управляючої інформації. Щоб увести в дію високошвидкісний і завадостійкий цифровий канал, було розв'язано низку завдань.

1. Створено універсальний квазікогерентний алгоритм обробки багатопозиційних OFDM сигналів.

2. Завдяки максимально правдоподібній оцінці сигналу забезпечено для каналу зв'язку відношення сигнал/шум понад 10 дБ. Це, у свою чергу, уможливило визначення фази сигналу на вході демодулятора з точністю, достатньою для реалізації квазікогерентного методу демодуляції для багатопозиційних сигналів. Зрештою дістали додатковий виграш до 11 дБ.

3. Реалізація квазікогерентного демодулятора дозволяє застосувати модуляцію OFDM сигналами, отримавши в умовах обмеженої смуги пропускання низку переваг.

4. Показано, що застосовуваний для демодуляції групового сигналу OFDM метод швидкого перетворення Фур'є (ШПФ) забезпечує лінійність перетворень сигналу та скорочує кількість операцій з його обробки. Утім, метод ШПФ не виключає необхідності підстроювання фаз сигналів підканалів, а операції множення-додавання відліків сигналу знижують точність обробки. Окрім того, модульне нарощування демодулятора додаванням нових частотних підканалів у разі використання ШПФ ускладнюється. Натомість універсальний квазікогерентний алгоритм демодуляції OFDM сигналів демонструє високу ефективність.

Список використаної літератури

1. ***Гостев, В. И.*** *Системы автоматического управления с цифровыми регуляторами / В. И. Гостев, В. К. Стеклов.— К.: Радіоаматор, 1998.— 704 с.*

2. ***Емельянов, Г. А.*** *Передача дискретной информации / Г. А. Емельянов, В. О. Шварцман.— М.: Радио и связь, 1982.— 240 с.*

3. ***Порівняльна*** *характеристика завадостійкості систем при використанні n-вимірних багатопозиційних сигналів / [В. Б. Толубко, Л. Б. Беркман, С. І. Отрох, Є. П. Гороховський, В. О. Ярош] // Наук. записки УНДІЗ.— 2017.— №2(46).— С. 5–11.*

Рецензент: доктор техн. наук, професор **А. І. Семенко**, Державний університет телекомунікацій, Київ.

В. В. Дубровский, С. И. Отрох, В. И. Кравченко, В. А. Кузьминых, А. И. Голубенко

МЕТОДОЛОГИЯ РАСЧЕТА ПОМЕХОУСТОЙЧИВОСТИ МНОГОПОЗИЦИОННЫХ СИГНАЛЬНЫХ СОЗВЕЗДИЙ

Проведен расчет помехоустойчивости многопозиционных сигнальных конструкций и доказана эффективность их манипуляционного кодирования. На основе расчетов построены графики, характеризующие среднюю вероятность ошибки, возникающей при различении пары сигналов каждого из рассматриваемых созвездий для заданных значений отношения сигнал/шум.

Проведен сравнительный анализ квазикогерентного метода демодуляции и неоптимальных методов приема.

Ключевые слова: сигнальные созвездия; помехоустойчивость; OFDM сигналы; многопозиционные сигналы.

V. V. Dubrovskiy, S. I. Otrokh, V. I. Kravchenko, V. O. Kuzminykh, O. I. Holubenko

METHODOLOGY OF CALCULATING OF THE NOISE IMMUNITY OF MULTIPOSITION SIGNAL CONSTELLATIONS

The calculation of noise immunity of multiposition signal constellations is carried out. The efficiency of manipulation coding of multiposition signals is proved. Based on the calculations, graphs of the ratio of the mean error probability are given. A comparative analysis of the quasicoherent demodulation method is made in comparison with non-optimal methods of reception.

Keywords: signal constellations; noise immunity; OFDM signal; multiposition signal.

УДК 621.398.96

Н. В. РУДЕНКО, здобувач,
Державний університет телекомунікацій, Київ

Розробка методу масштабування систем ФАП

Запропоновано ефективні підходи до масштабування систем ФАП — статичних і астатичних, а також розглянуто можливість використання диференціальних зв'язків за фазою вхідного сигналу для підвищення точності в усталених режимах. Наведено метод синтезу масштабуючих пристроїв у зазначених системах.

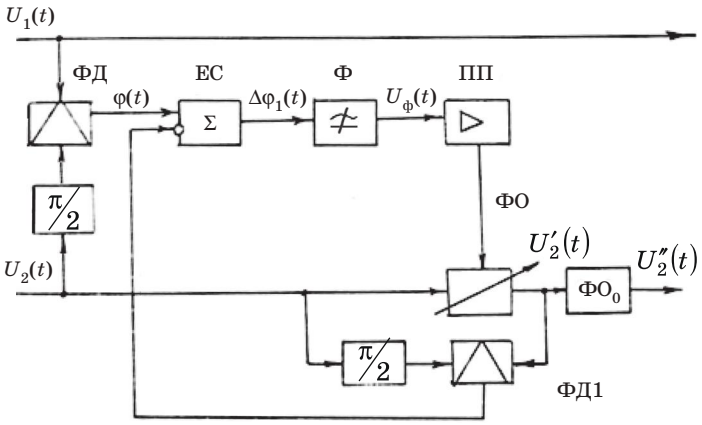
Ключові слова: масштабуючий пристрій; статична система; астатична система; синтез; фазове автопідстроювання.

Вступ

Системи фазового автопідстроювання (ФАП), призначені для ідентифікації фаз змінних напруг і усунення фазового набігу в підсилювачах, широко використовуються в радіолокації, електромеханіці, телемеханіці та інших галузях, де потрібно забезпечити синфазність напруг змінного струму в усталених режимах [1]. Використання неодиничного зворотного зв'язку в статичних системах ФАП дозволяє підвищити порядок астатизму на одиницю. Утім не лише поодинокий зворотний зв'язок впливає на перехідний процес. Такого самого ефекту можна досягти введенням масштабування керованої величини (фази вхідного сигналу керованого фазообертача) або задавального впливу (різниці фаз порівнюваних напруг).

Основна частина

З'ясуємо особливості масштабування систем ФАП, розглянувши подану на рисунку функціональну схему системи ФАП із масштабуючим коефіцієнтом у колі керованої величини, що дасть змогу здійснити синтез відповідного керуючого пристрою (КП).



Функціональна схема системи ФАП із масштабуючим коефіцієнтом у колі керованої величини

Згідно зі схемою маємо:

$$\begin{gathered}\Delta\varphi_1(t)=\alpha(t)-\beta(t);\\ \beta(t)=W_\Phi(p)W_{ПП}(p)W_{ФО}(p)\Delta\varphi_1(t);\\ \Delta\varphi(t)=\alpha(t)-\beta_1(t);\\ \beta_1(t)=K_M\beta(t).\end{gathered} \qquad (1)$$

Тут $W_\Phi(p)=\dfrac{K_\Phi}{T_\Phi p+1}$; $W_{ПП}(p)=\dfrac{T_{ПП}}{T_{ПП}p+1}$; $W_{ФО}(p)=1$; K_M — масштабуючий коефіцієнт, $K_M=\dfrac{K_0+1}{K_0}$; $K_0=K_\Phi K_{ПП}$.

Керовану величину $\beta(t)$ можна визначити так:

$$\beta(t)=\frac{W_P(p)}{1+W_P(p)}K_M\alpha(t)=W_{ЕЗ}(p)\alpha(t), \qquad (2)$$

де $W_P(p)=W_\Phi(p)W_{ПП}(p)W_{ФО}(p)$; $W_{ЕЗ}(p)$ — еквівалентний оператор замкненої системи ФАП, $W_{ЕЗ}(p)=\dfrac{W_P(p)}{1+W_P(p)}K_M$.

З урахуванням виразу (2) подамо еквівалентний оператор системи ФАП щодо помилки у вигляді

$$W_{\Delta\varphi E}(p)=1-W_{E3}(p)=\frac{1+W_P(p)(1-K_M)}{1+W_P(p)}. \quad (3)$$

Система ФАП без масштабуючого коефіцієнта ($K_M = 1$) є статичною ($\upsilon = 0$). У такій системі мають місце статична складова помилки і складові помилки, зумовлені першою та наступними похідними від задавального впливу $\alpha(t)$.

При $K_M = \frac{K_0+1}{K_0}$ згідно з (3) дістаємо:

$$W_{\Delta\varphi E}(p)=\frac{(T_\Phi p+1)(T_{ПП}p+1)+K_0\left[1-\frac{K_0+1}{K_0}\right]}{(T_\Phi p+1)(T_{ПП}p+1)+K_0}=\frac{T_\Phi T_{ПП}p^2+(T_\Phi+T_{ПП})p}{T_\Phi T_{ПП}p^2+(T_\Phi+T_{ПП})p+1+K_0}= \quad (4)$$

$$=\frac{a_2p^2+a_1p}{c_2p^2+c_1p+c_0}=\frac{D_{\Delta\varphi_0}(p)p^\upsilon}{F_{\Delta\varphi}(p)},$$

де $D_{\Delta\varphi_0}(p)=a_2p^2+a_1$; $F_{\Delta\varphi}(p)=c_2p^2+c_1p+c_0$.

Як випливає з (4), система ФАП із масштабуючим коефіцієнтом K_M у колі керованої величини $\beta(t)$ є астатичною з астатизмом першого порядку ($\upsilon = 1$), тобто порядок астатизму зростає на одиницю.

Важливою особливістю системи ФАП із масштабуючим коефіцієнтом є те, що її стійкість не залежить від цього коефіцієнта, у чому легко переконатись порівнянням характеристичних поліномів.

Реалізувати масштабуючий коефіцієнт у колі керованої величини можна включенням у це коло коригуючого пристрою — фазообертача, який забезпечує постійний фазовий зсув виду $\frac{(K_0+1)}{K_0}$.

Як уже зазначалося, масштабування можна реалізувати також включенням масштабуючого пристрою в коло задавального впливу.

Нехай маємо такі рівняння елементів системи ФАП:

$$\begin{aligned}\Delta\varphi(t)&=\alpha(t)-\beta(t);\\ \beta(t)&=W_P(p)\Delta\varphi_1(t);\\ \Delta\varphi_1(t)&=\alpha_1(t)-\beta(t);\\ \alpha_1(t)&=\alpha(t)K_M.\end{aligned} \quad (5)$$

Еквівалентний оператор системи ФАП набирає вигляду

$$W_{\Delta\varphi E}(p)=\frac{1+W_P(p)(1-K_M)}{1+W_P(p)}. \quad (6)$$

Вираз (6) збігається з виразом (3), а отже, у системах можна досягти однакових результатів стосовно підвищення точності в усталених режимах. При цьому масштабування не впливає на стійкість замкненого контура системи ФАП.

Масштабування можна реалізувати, по-перше, включенням у коло сигналу $U_1(t)$ чи $U_2(t)$ пристрою постійного зсуву фаз — фазообертача ФО; а по-друге, включенням у коло сигналу $\alpha(t)$ на виході фазового дискримінатора ФД подільника напруги з передатним коефіцієнтом K_M.

Слід зазначити, що рівність нулю коефіцієнта помилки D_0 при масштабуванні можлива в разі виконання певної умови. Якщо загальний коефіцієнт підсилення ФАП нестабільний, то з'являється додаткова статична помилка. Оцінимо її значення, скориставшись виразом (3).

Нехай $K_M = \frac{K_0+1}{K_0} = \text{const}$. Тоді рівняння для $W_{\Delta\varphi}(p)$ за умови, що загальний коефіцієнт підсилення K_0 має приріст ΔK_0, набирає вигляду

$$W_{\Delta\varphi}(p)=\frac{T_\Phi T_{ПП}p^2+(T_\Phi+T_{ПП})p+1+(K_0+\Delta K_0)(1-K_M)}{T_\Phi T_{ПП}p^2+(T_\Phi+T_{ПП})p+1+K_0+\Delta K_0}. \quad (7)$$

Відомо, що масштабуючі пристрої використовуються для підвищення порядку астатизму в статичних системах автоматичного управління [2]. Проте в системах ФАП є змога значно істотніше підвищити порядок астатизму. Річ у тім, що методику розрахунку оператора масштабуючого пристрою можна використовувати для того, аби досягти будь-якого необхідного порядку астатизму системи ФАП.

Справді, оскільки вирази

$$W_{З}(p)=\frac{\beta(t)}{\alpha(t)}=\frac{W_{КП}(p)W_{Р}(p)}{1+W_{Р}(p)}$$

і

$$W_{З}(p)=\frac{\beta(t)}{\alpha(t)}=1-\frac{W_{КП}(p)W_{Р}(p)}{1+W_{Р}(p)}$$

однакові, то методи синтезу КП, розташованого в каналі задавального впливу, згідно з умовою підвищення порядку астатизму (підвищення точності в усталених режимах) будуть такі самі, як і методи синтезу КП, розташованого в каналі керованої величини [3; 4].

Висновки

• Важлива особливість систем ФАП із масштабуючим коефіцієнтом полягає в тому, що вони не лише забезпечують підвищення точності в усталеному режимі, а й досягнута при цьому стійкість не залежить від масштабуючого коефіцієнта.

• Масштабування можна реалізувати включенням масштабуючого пристрою або в коло задавального впливу, або в коло керованої величини.

• Запропоновано метод синтезу оператора масштабуючого пристрою згідно з умовою підвищення порядку астатизму системи ФАП, якщо фізична його реалізація взагалі можлива.

Список використаної літератури

*1. **Стеклов, В. К.** Синтез многоконтурных итерационных систем фазовой автоподстройки в установившихся режимах / В. К. Стеклов, Д. В. Охрущак, В. И. Стасюк // Радиоэлектроника.— 2003.— 46, № 8.— С. 21–26.*

*2. **Бесекерский, В. А.** Теория систем автоматического управления / В. А. Бесекерский, Е. П. Попов.— СПб.: Профессия, 2004.— 752 с.*

*3. **Захарченко, Н. В.** Системы фазовой синхронизации, малочувствительные к изменениям параметров / Н. В. Захарченко, Г. Д. Созонник, В. К. Стеклов.— Одесса: ОЭИС, 1986.— 45 с.*

*4. **Игнатов, В. А.** Коррекция нелинейных автоматических систем / В. А. Игнатов, В. К. Стеклов, Р. В. Уваров.— К.: Техника, 1993.— 192 с.*

Рецензент: доктор техн. наук, професор **С. В. Козелков**, Державний університет телекомунікацій, Київ.

Н. В. Руденко

РАЗРАБОТКА МЕТОДА МАСШТАБИРОВАНИЯ СИСТЕМ ФАП

Предложены эффективные подходы к масштабированию систем ФАП — статичных и астатичных, а также рассмотрена возможность использования дифференциальных связей по фазе входного сигнала для повышения точности в установившихся режимах. Приведен метод синтеза масштабирующих устройств в указанных системах.

Ключевые слова: масштабирующее устройство; статичная система; астатичная система; синтез; фазовая автоподстройка.

N. V. Rudenko

DEVELOPMENT OF THE METHOD AUTOMATIC PHASE CONTROL SYSTEMS WITH A SCALE DEVICE

In the article the technique of synthesis of scalable devices in static and astatic automatic phase control systems is considered and the possibility of using differential connections along the phase of the input signal for increasing accuracy in steady-state modes. The proposed method for synthesizing scalable devices in static and astatic automatic phase control systems.

Keywords: scalable device; static system; astatic system; synthesis; automatic phase control.

УДК 004.77:004.424
В. В. ВАСИЛЕНКО, аспірант,
Державний університет телекомунікацій, Київ

ВІРТУАЛІЗАЦІЯ ХМАРНИХ ОБЧИСЛЕНЬ І ПИТАННЯ БЕЗПЕКИ В ХМАРНІЙ СИСТЕМІ

Наведено опис сучасних технологій віртуалізації та проаналізовано механізми захисту, необхідні для досягнення надійної ізоляції віртуальних машин, їх опосередкованого спільного використання та налагодження безпечного зв'язку між ними, що має зрештою гарантувати захист приватного трафіку у віртуальних мережах.
Ключові слова: хмарні технології; інформаційні мережі; інформаційна безпека; віртуальна машина.

ВСТУП

Постановка задачі. Хмарні технології виступають сьогодні як представники потужної обчислювальної парадигми. Ідеться про засади нового покоління мережної обчислювальної системи (*Infrastructure as a Service* — **IaaS**), яка підтримує програмне і апаратне забезпечення власних ресурсів, а також надання різноманітних інтернет-послуг. Проте з міркувань безпеки користувачам заборонено ухвалювати хмарні рішення щодо багатьох критично важливих бізнес-обчислень. Адже через спільне використання ресурсів хмари, розрахованих на багатьох користувачів, постають значні загрози її безпеці. Тому останніми роками ця проблематика привертає до себе дедалі більшу увагу науковців-теоретиків і розробників обладнання.

Аналіз останніх досліджень і публікацій. Сучасний стан щодо формування методів аналізу і синтезу хмарних технологій нерозривно пов'язаний із працями таких учених, як O. Sheyner, P. Ammann, X. Ou, L. Wang, H. Poolsappasit, A. Рой.

Мета статті — подати огляд сучасних технологій віртуалізації, спрямованих на захист і забезпечення безпеки приватного трафіку, притаманного віртуальним мережам.

ОСНОВНА ЧАСТИНА

Загальні положення

Віртуалізація являє собою основну технологію хмарних обчислень. Обчислювальна потужність, як і спосіб зберігання інформації в мережі, підлягає віртуалізації для спільного використання в системі IaaS. Ця важлива технологія перетворює абстрактну інфраструктуру й ресурси на такі, що доступні для користувачів у вигляді *ізольованих віртуальних машин* (*VM*) та *віртуальних мереж* (*VNs*). А проте, вона підвищує вразливість системи до атак, оскільки всі користувачі хмари поділяють між собою, а можливо, і нападниками наявні в ній ресурси.

Механізм захисту дає змогу забезпечувати суворо ізоляцію віртуальних машин одна від одної у процесі опосередкованого спільного їх використання, підтримуючи безпечний зв'язок між ними. Окрім того, постає потреба в технологіях із запобігання та виявлення аномального трафіку і захисту нормального трафіку у *VNs*.

Віртуалізація на основі гіпервізора

Гіпервізор, відомий також як *монітор віртуальних машин* (*VMM*), являє собою невеликий фрагмент програмного або програмно-апаратного забезпечення, який працює поверх апаратного забезпечення машини.

Основні функції гіпервізора такі:

- виявлення пасток і реагування на захищені або привілейовані операції, виконувані кожною віртуальною машиною;
- диспетчеризація.

Зауважимо, що адміністративна операційна система (ОС), відома також як *домен привілеїв* (наприклад, dom0 у гіпервізорі Xen), працює поверх гіпервізора так само, як віртуальні машини, відповідаючи за управління віртуальними машинами на одному сервері та працюючи з гіпервізором [1].

Існують два типи гіпервізорів: тип I і тип II. Гіпервізор типу I має бути запущений над апаратними засобами для управління ними та гостьовою ОС. Він відповідає також за більшість комунікацій між усіма гостьовими ОС і апаратними засобами. До представників цього типу окрім згадуваного вже гіпервізора Xen належать VMware ESX Server і Microsoft Hyper-V.

Гіпервізор типу II працює як додаток у рамках хоста ОС, відповідаючи за надання драйверів введення/виведення і управління гостьовою ОС віртуальних машин.

Наприклад, VMware Workstation, VMware Server і VirtualBox — представники архітектури віртуалізації на основі гіпервізора типу II.

Повна віртуалізація

Така віртуалізація передбачає, що гіпервізор містить код, який при потребі емулює базове обладнання, дозволяючи немодифікованим ОС працювати поверх гіпервізора [1]. Одне з відомих програмних забезпечень повної віртуалізації —

VMWare ESX Server — використовує версію Linux (відому як ConsoleService) у ролі своєї адміністративної ОС. Гіпервізор на сервері VMWare ESX, відомий під назвою VMkernel, являє собою гіпервізор товстого шару, якому належить драйвер апаратного забезпечення VMs для кожної віртуальної машини.

На базі повної віртуалізації немодифікована ОС виконує програму користувача, що емулює машину, на якій працює гостьова ОС. Як перевагу цього підходу слід розглядати той факт, що віртуалізована архітектура може повністю відрізнятися від архітектури приймальної. Наприклад, QEMU може імітувати процесор MIPS на хості IA-32 та багато інших чипів [2].

Паравіртуалізація

Тип віртуалізації Xen означає, що створюється тонкий і компактний гіпервізорний шар, який працює безпосередньо поверх апаратного забезпечення, а також надає послуги віртуалізованій ОС. Цей тонкий шар гіпервізора, на відміну від товстого шару, характеризується повною віртуалізацією. Згідно з Xen тільки гіпервізор володіє повними правами, причому він покладається на надійність оцінки ОС, щоб забезпечити апаратні драйвери, ядро та призначений для користувача простір. Відповідний домен управління — згадуваний вже домен 0 (dom0), використовує власне ядро Linux для підтримання свого адміністративного середовища.

Домен 0 як перший домен, створений автоматично при завантаженні системи, має особливі привілеї управління, делеговані гіпервізору. Цей привілейований домен дозволяє гіпервізору отримувати доступ до пристроїв і виконувати функції управління. Усі інші гостьові домени (domUs) не мають привілеїв і перебувають під управлінням dom0. Апаратне середовище для всіх гостей не змодельовано, воно функціонує в їхніх власних ізольованих доменах так, неначе кожний гість працює в окремій системі. Проте гостьова ОС має бути спеціально модифікована, щоб працювати в цьому середовищі.

Паравіртуалізація може забезпечити підвищення продуктивності порівняно з іншими підходами, оскільки операційна система модифікації дозволяє безпосередньо зв'язуватися з гіпервізором і, отже, не зазнає жодних накладних витрат, пов'язаних з емуляцією, що потрібно для інших видів віртуалізації на базі гіпервізора.

Віртуалізація на рівні ядра

Для цього типу віртуалізації гіпервізор не потрібен, але він працює на спеціально модифікованому ядрі Linux, що містить розширення, призначене для управління кількома віртуальними машинами, кожна з яких включає гостьову.

Як приклад технологій віртуалізації на рівні ядра згадаємо користувальницький режим Linux (UML) і режим VM на основі ядра (KVM). Режим UML підтримувався в ядрах Linux досить довгий час, але вимагав спеціального складання ядра Linux для гостьових ОС. Саме тому було введено KVM 2.6.20. Режим UML не потребує будь-якого окремого адміністративного програмного забезпечення для виконання відповідних дій або управління віртуальними машинами, що може бути здійснено з командного рядка Linux. Режим KVM використовує драйвер пристрою в ядрі хоста для зв'язку між основним Linux ядром і віртуальною машиною, вимагаючи підтримки процесорів із метою віртуалізації (Intel VT або AMD-V Pacifica) та використовуючи модифікований процес QEMU як дисплей виконання контейнера для своїх віртуальних машин. Багато в чому віртуалізація KVM на рівні ядра є спеціалізованою версією повної віртуалізації, де ядро Linux використовується як гіпервізор [1].

Віртуалізація з апаратною підтримкою

Віртуалізація з апаратною підтримкою — це спосіб підвищення ефективності апаратної віртуалізації. Вона включає в себе використання спеціально розроблених процесорів і апаратних компонентів, які допомагають поліпшити експлуатаційні характеристики в гостьовому середовищі [1]. Гіпервізор на основі систем, таких як Xen і VMWare ESX Server, а також технології віртуалізації на рівні ядра, такі як KVM, можуть скористатися апаратною підтримкою віртуалізації. Останнє покоління Intel (Intel-VT) і AMD (AMD-V) процесорів підтримують апаратну віртуалізацію. Віртуальні машини в середовищі віртуалізації здатні працювати на немодифікованих операційних системах, оскільки гіпервізор може використовувати підтримку обладнання для віртуалізації та обробки привілейованих і захищених операцій та запитів доступу до обладнання, а також спілкуватися з віртуальними машинами та керувати ними.

Віртуальні мережні архітектури

Мережа є важливим ресурсом обчислювальної і комунікаційної системи. Хмарна система забезпечує не просто надання обчислювальних послуг або ресурсів, вона також слугує каналом зв'язку між усіма віртуальними машинами на одному сервері або на зовнішніх мережних пристроях. Важливе питання полягає в тому, як убезпечити й ізолювати ці канали зв'язку для кожної окремої VM на одному сервері. Далі розглянемо деякі з існуючих архітектур віртуальних мереж, що їх використовують постачальники хмарних платформ.

LinuxEthernetBridge

LinuxEthernetBridge — це спосіб з'єднання двох Ethernet-сегментів разом із протоколом. Пакети

передаються на основі Ethernet-адреси, а не IP-адреси (наприклад, маршрутизатор). Оскільки пересилання здійснюється на рівні 2, всі протоколи можуть іти прозоро через міст [3]. Код моста Linux реалізують стандарти ANSI/IEEE 802.1d [4]. Спочатку LinuxEthernetBridge було задіяно в Linux 2.2, причому код для мостів було інтегровано в серії ядер 2.4 і 2.6.

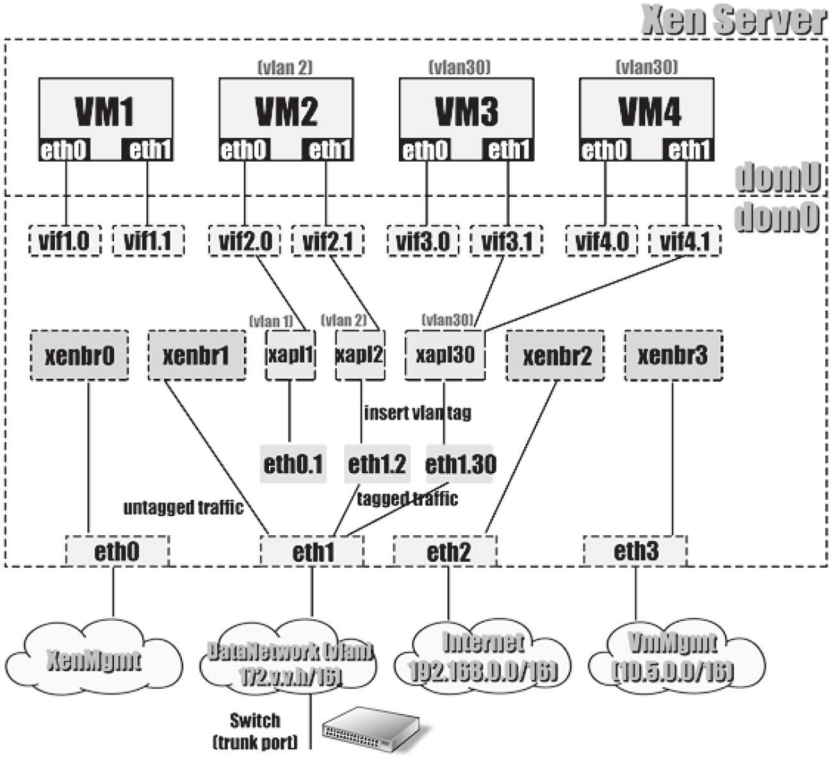
У хмарній системі зв'язок відбувається за участю віртуальних машин на одному хості або віртуальних машин, розташованих на різних комп'ютерах. Цей трафік проходить через віртуальні мережі до віртуального мережного інтерфейсу віртуальної машини або фізичного мережного інтерфейсу хоста. У віртуальній мережі системи Xen гіпервізор підтримує два режими роботи віртуальних мереж: режим моста і режим маршруту. У режимі моста dom0 створює програмне забезпечення Ethernet. При цьому міст є віртуальним інтерфейсом віртуальної машини для пересилання трафіку. Окрім того, він надає віртуальний інтерфейс віртуальної машини до фізичного інтерфейсу на хості для зв'язку із зовнішньою мережею та інтернетом.

У режимі маршруту dom0 створює таблицю маршрутизації, яка включає в себе набір MAC і IP-адрес, заздалегідь забезпечених зв'язком точка-точка між dom0 і кожною віртуальною машиною. В обох режимах dom0 створює віртуальний інтерфейс (vif) для кожного мережного інтерфейсу віртуальної машини. Наприклад, vif1.0 прикріплюється до eth0 з VM1, vif2.1 прикріплюється до eth1 з VM2, і т. д., що ілюструє рисунок.

Конфігурації VLAN

Для управління віртуальними машинами і надання виділених каналів зв'язку для групи віртуальних машин віртуальна локальна мережа (VLAN) здійснює стандартизацію в хмарі. Конфігурація VLAN у системі Xen контролюється та перебуває під управлінням dom0. Структуру VLAN в хмарній системі унаочнює рисунок. Для кожної VLAN dom0 створює унікальний міст XAPI # і відповідний віртуальний інтерфейс eth1. #. Символ # означає ідентифікатор карти VLAN і eth1 на фізичному порті Ethernet-хоста.

Усі мости в системі Xen ґрунтуються на реалізації стандартного моста Linux. XAPI # призначається тільки для внутрішнього використання мережі в dom0. Коли dom0 присвоює VLAN для VM, він пов'язує віртуальний інтерфейс (vif #. #) віртуальної машини до XAPI моста VLAN. Відеозаписи всіх віртуальних машин на віртуальній локальній мережі підімкнено до одного моста. Коли VLAN трафік приходить до моста, він спрямовується до відповідного віртуального інтерфейсу ETH #. #. Віртуальний інтерфейс потім вставляє VLAN тег у кадрі Ethernet відповідно до протоколу 802.1. Теги VLAN трафіку проходять через фізичний порт Ethernet із dom0, передаючи в собі порт зовнішнього фізичного комутатора. Якщо фізичний комутатор дозволяє порту зовнішньої лінії не встановлювати жодного рідного ідентифікатора VLAN (за замовчуванням VLAN ID) або встановити за замовчуванням VLAN ID у невикористовувану VLAN ID, позначений трафік буде проходити через комутатор і залишатиме інформацію тега



Налаштування віртуальної мережі з LinuxBridge

недоторканою. Ідентифікатор VLAN трафіку передається ще до однієї VLAN на інший сервер VPS на основі технології Xen або навіть на віддалений сайт.

Порт, позначений VLAN трафіком, обробляється dom0, а пакети передаються до відповідного віртуального інтерфейсу Eth #. # на підставі VLAN ID. Цей віртуальний інтерфейс буде «здирати» ідентифікатор мітки, а потім передавати пакети тільки за призначенням. Таким чином, призначення мережі VLAN, установлення міток і нормалізація — усе виконується в dom0. VM не знає, до якого VLAN вона належить, і їй не дозволено змінити VLAN тег. Проте в цьому разі можна не маркувати трафік із VLAN-VM, хоча цей тип трафіку буде підмикатися відразу до іншого типу моста xenbr1 і до фізичного порту Ethernet з dom0.

Постачальник послуг, як правило, налаштовує мережні ресурси з різними мережами VLAN для виділення та поділу каналів зв'язку, а також трафіку між різними групами клієнтів у хмарній системі. VLAN забезпечує механізм поділу мережних ресурсів на кілька неперетинних логічних, широкомовних доменів [5]. Трафік може переходити від однієї VLAN до іншої тільки через маршрутизатор. Утім VLAN у хмарному середовищі стикається з багатьма уразливостями від віртуальних машин і серверів. Водночас традиційні питання мережної безпеки не втрачають актуальності.

Позитивні характеристики та недоліки

Linux на базі платформи хмари з убудованою підтримкою LinuxEthernetBridge виступає як комутатор програмного забезпечення для віртуальних машин (на одному сервері є XenServer і KVM компанії Citrix). Міст Linux більш потужний, ніж простий апаратний міст, оскільки він може фільтрувати й формувати трафік. Його легко налаштувати за допомогою команди brctl. Нові можливості моста Linux не припиняють розвитку, можливі майбутні удосконалення: призначені для користувачів простору STP фільтрації, інтерфейс Netlink для управління мостами, підтримка RSTP\MSTP та інші розширення 802.1d STP.

Цей трафік передається безпосередньо з віртуальної машини VM, причому він ніколи не подорожує по фізичному проводу, тому мережні адміністратори не мають змоги контролювати його [6].

Open vSwitch

Відкриття vSWITCH (OVS) [7] являє собою OpenFlow на основі перемикача багатошарового програмного забезпечення, із ліцензією на відкритий вихідний код Apache 2. Це перемикач програмного забезпечення, який слугує для реалізації багатьох хмарних систем, наприклад Citrix XenServer [8] і OpenStack [9]. OVS надає стандартні інтерфейси управління і видимість віртуального мережного рівня. Його було розроблено для підтримки між кількома фізичними серверами. Усі розподілені віртуальні комутатори, такі як NOX/POX, RYU тощо, централізовано керуються мережним контролером на основі OpenFlow. OVS підтримує багато технологій Linux на основі віртуалізації, включаючи Xen, XCP, KVM і VirtualBox.

Open vSWITCH використовує граничний комутатор, який наближає до розв'язання проблеми віртуального мережного управління. Відповідний підхід використовує переваги, що випливають із наявності моста гіпервізора, оскільки компонент гіпервізора може безпосередньо пов'язувати мережні пакети з віртуальними машинами та їх конфігураціями. Граничні комутатори розширюють можливості щодо видимості й контролю, доступні раніше тільки в корпоративних комутаторах високого класу. Вони підвищують видимість між трафіком VM завдяки стандартним методам, таким як NetFlow і віддзеркалення. Додаткові крайові комутатори здійснюють політику трафіку для забезпечення безпеки та якості в обслуговуванні (QoS) [6]. Для того щоб керувати численними перемикачами, сучасні крайові комутатори підтримують централізовану конфігурацію політики. Це дозволяє адміністраторам управляти багатьма мостами на окремих гіпервізорах. Політика та конфігурації централізовано поширюються на віртуальні інтерфейси, мігруючи з їхніми віртуальними машинами.

Open vSWITCH сумісний із мостом Linux, причому він використовує багато Linux на основі гіпервізора для граничного комутатора. Це дозволяє йому бути заміненим у багатьох віртуальних середовищах. OVS надає безліч функцій мережного управління та моніторингу. Щодо видимості монітора, то він підтримує NetFlow, SFlow, протоколи дзеркального відображення (SPAN/RSPAN/ERSPAN). OVS може бути налаштований для перенесення моніторингу трафіку на віддалений колектор або аналізатор. Керованість OVS забезпечує централізоване управління по протоколу OpenFlow [10]. Це те саме, що й комутатор OpenFlow під контролем NOX на основі контролера для режиму руху потоку. Від контролера OVS системний адміністратор проводить список контролю доступу та політики QoS.

Для функцій переадресації OVS підтримує багато протоколів, зокрема **LACP** (*Link Aggregation Control protocol*), з'єднаних портів для балансування навантаження, 802.1Q модель VLAN із магістральним доступом до портів, 802.1ag управління несправностями підімкнення, а також кілька протоколів **GRE** (*Generic Routing Encapsulation*). За протоколами GRE для двох просторово рознесених мостів різної хмарності сервера віртуальні машини, підімкнені до цих мостів, можуть утворити двошарові з'єднання, розташовані навіть у різних

місцях і такі, що мають різні загальнодоступні IP-адреси.

Проблеми безпеки у віртуальному середовищі

У хмарних системах джерелом ураження для каналу зв'язку можуть бути віртуальні машини, сервер хмари, а також процес підімкнення до фізичної мережі.

Розглянемо головні механізми ураження.

Атаки з віртуальної машини. Віртуалізація виступає ключовою технологією в хмарних обчисленнях. При цьому головний осередок проблем щодо безпеки хмарної системи припадає на VM з'єднання [11]. Найбільшу небезпеку становлять такі ситуації.

• VM Hopping — процес переходу з однієї VM на іншу. Тоді зловмисник, перебуваючи на одній VM, може отримати несанкціонований доступ через іншу VM;

• VM Escape — доступ до VM через гіпервізор (VMM) із нападом на іншу частину віртуальних машин. Зловмисник, отримавши доступ до вузла запуску кількох віртуальних машин, може отримати доступ до ресурсів, які є спільними для інших віртуальних машин;

• VM mobility — вміст VM зберігається у файлі зображення на гіпервізорі. Зазначений файл можна перемістити (або скопіювати) в інше місце. Зловмисник, модифікувавши вміст цього файла, зможе змінити діяльність віртуальної машини;

• VM Template — VM клонують за допомогою шаблона, аби прискорити створення хмарної системи. Точніше, якщо шаблон використовують, зловмисник може змінити налаштування деякої VM, щоб стежити за всіма віртуальними машинами.

Атаки на основі віртуальної мережі. Обидва режими моста і режим маршруту dom0 відіграють тут певну роль.

• Sniffing: у режимі моста VM здатна «нюхати» віртуальну мережу на тому самому мості, використовуючи Sniffing інструменти, такі як Wireshark.

• Spoofing: VM-нападниця може скласти протокол дозволу адрес (ARP), аби перехоплювати пакети та прослуховувати трафік потерпілої VM.

На додаток до можливих засобів ураження віртуальної мережі слід згадати таку дію, як компрометація dom0 (Compromised dom0). Це важливе питання безпеки в мережі хмарної системи. Адже dom0 може контролювати всі зв'язки між VM і підмикатися до зовнішньої мережі.

Тільки-но dom0 скомпрометовано, зловмисник може змінити трафік у віртуальній мережі і заволодіти важливою інформацією.

Зазначені атаки тягнуть за собою такі загрози:

• усі віртуальні машини контролюються VM-нападницею;

• зв'язок між віртуальними машинами контролюється зловмисниками;

• Denial of Service (DoS) проти хмарних сервісів.

Безпека VLAN

Для підвищення безпеки VLAN реалізовано у плані посилення ізоляції мережі, а також розширення можливостей управління системою. Проте з реалізацією VLAN кожне повідомлення, як і раніше, може охопити всі частини однієї і тієї самої мережі. Це означає, що повідомлення можуть бути прочитані будь-яким хостом на тій самій VLAN. Тоді зловмисник може пасивно підслуховувати пакети, що проходять через мережу. Окрім того, слід пам'ятати, що Ethernet являє собою систему мовлення, яка не передбачає механізму для перевірки справжності відправника. Це дозволяє зловмисникові генерувати нові пакети або відтворювати раніше підслухані [12].

Найчастіше відомі атаки проти кінцевих хостів у мережі рівня 2 спираються на Medium Access Control (MAC), Addressspoofing чи Address Resolution Protocol (ARP).

Це формує основу багатьох атак, таких як DoS і Man-In-The-Middle. Інші можливі атаки у VLAN на основі мережі [13] включають у себе:

• MAC flooding attack — це напад, пов'язаний з обмеженням перемикачів, що працюють, і мостів. Вони володіють кінцевою таблицею апаратних засобів для зберігання вихідних адрес усіх прийнятих пакетів. Коли ця таблиця заповнюється, трафік, спрямований на адреси, які не можуть бути вилучені, буде постійно повний;

• 802.1Q tagging attack — атака, що відбувається через неправильні настроювання перемикачів, які встановлюють порт комутатора як небажаний порт з'єднувальної лінії. Таку ситуацію називають VLAN leaking, що дозволяє користувачеві VLAN дістати несанкціонований доступ до іншої VLAN;

• Double-Encapsulated 802.1Q/ VLAN атаки — атаки, що відбуваються через неправильне настроювання перемикачів, які встановлюють рідний ідентифікатор VLAN магістрального порту, так само як VLAN ID порту доступу зловмисника. Зловмисник може інкапсулювати цільовий ідентифікатор VLAN як внутрішній шар протоколу 802.1Q. Після того як зовнішній тег відігнано, відбувається неправильний вибір параметра комутатора, а через це комутатор просто пересилає пакети за призначенням підробленого внутрішнього тега. Таким чином, зловмисник на VLAN може отримати несанкціонований доступ до іншої VLAN, що згадується як VLAN Hopping;

• ARP-атаки — це атаки, пов'язані з ARP-запитом і відповіддю, які несуть інформацію про ідентичність шару 2 (MAC-адресу) та ідентифікатор рівня 3 (IP-адресу) хоста. Зловмисник може обдурити комутатор у переспрямовуванні пакетів

на пристрій або хост в іншій мережі VLAN, посилаючи ARP-пакети, що містять підроблені тотожності.

Варто наголосити, що в тій самій VLAN так звані ARP-атаки є дуже ефективний спосіб обдурювання кінцевих станцій або маршрутизаторів для вивчення підробки ідентичних пристроїв. Це може дозволити зловмисникові поставити людину як посередника та виконавця своїх намірів.

ВИСНОВКИ

Віртуалізація є основною технологією хмарних обчислень, згідно з якою обчислювальна потужність мережі підлягає віртуалізації для спільного використання в системі IaaS. Ця важлива технологія перетворює абстрактні інфраструктури та ресурси на доступні для користувачів у ролі ізольованих віртуальних машин (VM) та віртуальних мереж (VNs). Проте віртуалізація підвищує уразливість і можливість атак у системі, оскільки всі користувачі у хмарі поділяють наявні ресурси з іншими користувачами або навіть із нападниками. Механізм захисту слугує для забезпечення суворої ізоляції, опосередкованого спільного використання та безпечного зв'язку між віртуальними машинами. При цьому постає потреба в технологіях для виявлення аномального трафіку та захисту нормального трафіку у віртуальних мережах.

Отже, забезпечення безпеки та захист приватного трафіку у віртуальних мережах, із запобіганням зловмисному трафіку в спільних ресурсах — це головна проблематика безпеки в хмарній системі.

Список використаної літератури

1. ***Hagen, W.*** *Professional Xen Virtualization / W. Hagen.— Wiley Publishing, Inc., 2008.*

2. ***Takemuraand, C.*** *The Book of XEN / C. Takemuraand, L. Crawford.— No Starch Press, 2009.*

3. ***The Linux*** *Foundation [Електронний ресурс] // Linuxbridge, 2012.— Режим доступу:*
http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge;

4. ***IEEE 802.1d*** *standard, 2012 [Електронний ресурс].— Режим доступу:*
https://standards.ieee.org/about/get/802/802.1.html;

5. ***Saha, A.*** *Thinking out side the box: extending 802.1x aut hentication to remote «splitter» ports by combining physical and data linklayer techniques / A. Saha and M. Molle // 28th Annual IEEE International Conference on Local Computer Networks, 2003.LCN'03. Proceedings, 2003.— P. 324–333.*

6. ***Pettit, J.*** *Virtual switching in anera of advanced / [J. Pettit a. o.] // 2nd Workshop on Data Center — Converged and Virtual Ethernet Switching (DC-CAVES), ITC.— 2010.— Vol. 22.*

7. ***Open*** *Switch project [Електронний ресурс].— Режим доступу:*
http://openvswitch.org, May 2012.

8. ***Citrix*** *Xen Server [Електронний ресурс].— Режим доступу:*
http://www.citrix.com/xenserver

9. ***Open*** *Stack [Електронний ресурс].— Режим доступу:*
http://www.openstack.org/

10. ***Open*** *flow [Електронний ресурс].— Режим доступу:*
http://www.openflow.org/wp/learnmore/

11. ***Wu, H.*** *Network security for virtual machine in cloud computing / [H. Wu, Y. Ding, C. Winer and L. Yao] // Computer Sciences and Convergence Information Technology (ICCIT), 2010. 5th International Conferenceon, Dec. 2010.— P. 18 –21.*

12. ***Kumar, S.*** *Service cloaking and authentication at data link layer / S. Kumar // 2nd International Symposium on Advanced Networks and Telecommunication Systems, 2008. ANTS'08, 2008.— P. 1–3.*

13. ***Cisco*** *Systems. Virtuallan security best practices, 2002 [Електронний ресурс].— Режим доступу:*
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwpwp.pdf

Рецензент: доктор техн. наук, професор **В. В. Вишнівський**, Державний університет телекомунікацій, Київ.

В. В. Василенко

ВИРТУАЛИЗАЦИЯ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ И ВОПРОСЫ БЕЗОПАСНОСТИ В ОБЛАЧНОЙ СИСТЕМЕ

Приведено описание современных технологий виртуализации и проанализированы механизмы защиты, необходимые для обеспечения строгой изоляции, опосредованного совместного использования и безопасной связи между виртуальными машинами с целью обеспечения безопасности частного трафика в виртуальных сетях.

Ключевые слова: облачные технологии; информационные сети; информационная безопасность; виртуальная машина.

V. V. Vasylenko

VIRTUALIZATION AND CLOUD COMPUTING SECURITY ISSUES IN CLOUD SYSTEM

Description of the currently existing types of virtualization technologies, and the analysis of defense mechanisms that are necessary to ensure strict isolation mediated sharing and secure communications between virtual machines to provide security and protection of private traffic on the virtual networks.

Keywords: cloud; information networks; information security; virtual machine.

УДК 656.8.001
Л. О. ЯЩУК, доктор техн. наук, професор, заслужений діяч науки і техніки України,
Одеська національна академія зв'язку ім. О. С. Попова

Застосування решітчастих поштових маршрутів — шлях до радикального підвищення живучості мережі поштового зв'язку України

Розглянуто переваги застосування магістральних поштових маршрутів (ПМ) у вигляді прямокутних решіток, що дозволяють радикально підвищити живучість мережі поштового зв'язку (МПЗ) України, скоротити загальну кількість і загальну протяжність ПМ.

Ключові слова: МПЗ; живучість МПЗ; об'єкти поштового зв'язку (ОПЗ); ПМ; горизонтальні ПМ (ГПМ); вертикальні ПМ (ВПМ); схема магістральних перевезень пошти (СМПП); поштові одиниці (ПО); поштові потоки (ПП); транзитні вузли (ТВ); нормативні строки (НС) пересилання ПО; показники тонно-кілометрів (ТКМ) пересилання ПО; шляхи пересилання пошти (ШПП); відновлення ОПЗ; відновлення РПМ; відновлення ШПП.

Вступ

Для здійснення магістральних перевезень ПО найчастіше застосовуються радіально-вузлові ПМ (РВПМ) або кільцеві ПМ (КПМ). Пропонується доповнити ці ПМ *решітчастими ПМ* (*РПМ*). Використання ПМ у вигляді прямокутних решіток не тільки природно поєднується з поданням міжвузлових ПП у матричній формі, а й дозволяє радикально підвищити живучість МПЗ у надзвичайних ситуаціях, скоротити сумарну кількість і сумарну протяжність ПМ, а також спростити їх синхронізацію.

Схема магістральних перевезень пошти із РПМ

Зобразимо СМПП у вигляді матриці вузлів розміром $n \times m = 6 \times 4 = 24$ (рис. 1). Ця матриця може наближено подавати 24 обласні вузли, з'єднані з використанням $n = 6$ двосторонніх (12 односторонніх) ВПМ і $m = 4$ двосторонніх (8 односторонніх) ГПМ, за допомогою яких пересилаються $nm(nm - 1) = 24 \cdot 23 = 552$ міжобласні ПП в Україні.

За умов застосування РПМ поштові потоки між парами вузлів із початковими координатами $(x_п, y_п)$ і кінцевими координатами $(x_к, y_к)$ може пересилатися одним із трьох способів:

- одним ГПМ при $y_к = y_п$;
- одним ВПМ при $x_к = x_п$;
- одним ГПМ і одним ВПМ через ТВ із координатами $(x_п, y_к)$ або через ТВ із координатами$(x_к, y_п)$.

Приклади з'єднання вузлів СМПП:

вузли (2,2) і (2,4) з'єднуються одним ГПМ 3;

вузли (2,4) і (2,2) з'єднуються одним ГПМ 4;

вузли (2,3) і (3,3) з'єднуються одним ВПМ 5;

вузли (3,3) і (2,3) з'єднуються одним ВПМ 6;

вузли (2,2) і (3,4) з'єднуються одним ГПМ 3 і одним ВПМ 7 через ТВ (2,4) або одним ВПМ 3 і одним ГПМ 5 через ТВ (3,2);

вузли (3,4) і (2,2) з'єднуються одним ГПМ 6 і одним ВПМ 4 через ТВ (3,2) або одним ВПМ 8 і одним ГПМ 4 через ТВ (2,4).

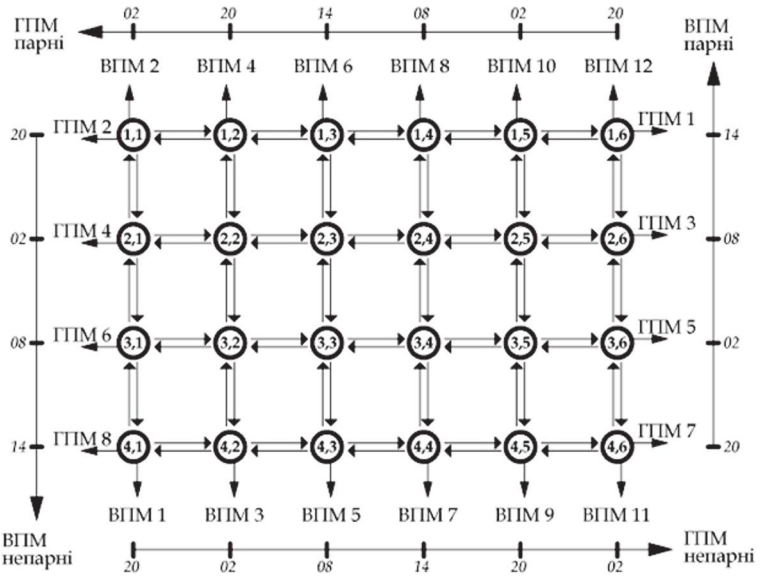


Рис. 1. СМПП із РПМ

Нормативні строки пересилання ПО і показники ТКМ у СМПП із РПМ

Розраховані значення НС пересилання ПО і показників ТКМ у пропонованій СМПП наведено відповідно в табл. 1 і 2.

Зауважимо, що НС і ТКМ пересилання внутрішньообласних ПО, подані діагональними елементами табл. 1 і 2, вважаються невизначеними.

Таблиця 1

Нормативні строки пересилання ПО, днів

Вузли відправлення	Вузли призначення																							
	1,1	1,2	1,3	1,4	1,5	1,6	2,1	2,2	2,3	2,4	2,5	2,6	3,1	3,2	3,3	3,4	3,5	3,6	4,1	4,2	4,3	4,4	4,5	4,6
1,1		1	1	2	2	2	2	2	2	2	2	2	1	2	2	2	3	3	2	2	2	3	3	3
1,2	1		1	2	2	2	2	2	2	2	2	2	2	1	2	3	3	3	2	2	2	3	3	3
1,3	1	1		2	2	2	2	2	2	2	2	2	2	2	1	2	2	3	2	2	2	3	3	3
1,4	2	2	2		1	1	2	2	2	1	2	2	2	2	2	1	2	2	2	3	3	3	3	3
1,5	2	2	2	1		1	2	2	2	1	2	2	3	3	2	2	2	2	3	3	3	3	3	3
1,6	2	2	2	1	1		3	2	2	2	2	1	3	3	3	2	2	1	3	3	3	3	3	3
2,1	2	2	2	2	2	3		1	2	2	2	2	1	2	2	2	2	2	3	3	3	3	3	3
2,2	2	2	2	3	3	2	1		1	2	2	2	2	1	2	2	2	2	3	3	3	3	3	3
2,3	2	2	2	3	3	2	2	1		2	2	2	2	2	1	2	2	2	3	3	3	3	3	3
2,4	2	2	2	2	2	2	2	2	2		1	1	2	2	2	2	2	2	3	3	3	3	3	3
2,5	2	2	2	2	2	2	2	2	2	1		1	2	2	2	2	2	2	3	3	3	3	3	3
2,6	2	2	2	2	2	2	2	2	2	1	1		2	2	2	2	2	2	3	3	3	3	3	3
3,1	2	2	2	2	2	2	2	2	2	2	2	2		1	2	2	2	2	3	3	3	3	3	3
3,2	2	2	2	3	3	2	1	2	2	2	3	3	1		2	2	2	2	3	3	3	3	3	3
3,3	2	2	2	3	3	2	2	2	2	2	2	2	1	1		2	2	2	3	3	3	3	3	3
3,4	3	3	3	2	2	2	2	2	2	1	2	2	2	2	2		1	2	3	3	3	3	3	3
3,5	3	3	3	2	2	2	2	2	2	2	1	2	2	2	2	1		1	3	3	3	3	3	3
3,6	3	3	3	2	2	2	2	2	2	2	2	1	2	2	2	2	1		3	3	3	3	3	3
4,1	2	2	2	3	3	3	1	2	2	2	3	3	1	2	2	3	3	3		1	1	2	2	2
4,2	2	2	2	3	3	3	2	1	2	2	3	3	2	1	2	3	3	3	1		1	2	2	2
4,3	2	2	2	3	3	3	2	2	1	2	3	3	2	2	1	2	3	3	1	1		2	2	2
4,4	3	3	3	2	2	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2	2		1	1
4,5	3	3	3	2	2	2	3	2	2	2	1	2	3	3	2	2	1	2	2	2	2	1		1
4,6	3	3	3	2	2	2	3	2	2	2	2	2	3	3	3	2	2	1	2	2	2	1	1	

Таблиця 2

Значення показників ТКМ

Вузли призначення

Вузли відправлення	1,1	1,2	1,3	1,4	1,5	1,6	2,1	2,2	2,3	2,4	2,5	2,6	3,1	3,2	3,3	3,4	3,5	3,6	4,1	4,2	4,3	4,4	4,5	4,6
1,1		1	2	3	4	5	1	2	3	4	5	6	2	3	4	5	6	7	3	4	5	6	7	8
1,2	1		1	2	3	4	2	1	2	3	4	5	3	2	3	4	5	6	4	5	4	5	6	7
1,3	2	1		1	2	3	3	2	1	2	3	4	4	3	2	3	4	5	5	4	2	4	5	6
1,4	3	2	1		1	2	4	3	2	1	2	3	5	4	3	2	3	4	6	5	4	3	4	5
1,5	4	3	2	1		1	5	4	3	2	1	2	6	5	4	3	2	3	7	6	5	4	3	4
1,6	5	4	3	2	1		6	5	4	3	2	1	7	6	5	4	3	2	8	7	6	5	4	3
2,1	1	2	3	4	5	6		1	2	3	4	5	1	2	3	4	5	6	2	3	4	5	6	7
2,2	2	1	2	3	4	5	1		1	2	3	4	2	1	2	3	4	5	3	2	3	4	5	6
2,3	3	2	1	2	3	4	2	1		1	2	3	4	2	1	2	3	4	4	3	2	3	4	5
2,4	4	3	2	1	2	3	3	2	1		1	2	4	3	2	1	2	3	5	4	3	2	3	4
2,5	5	4	3	2	1	2	4	3	2	1		1	5	4	3	2	1	2	6	5	4	3	2	3
2,6	6	5	4	3	2	1	5	4	3	2	1		6	5	4	3	2	1	7	6	5	4	3	2
3,1	2	3	4	5	6	7	1	2	3	4	5	6		1	2	3	4	5	1	2	3	4	5	6
3,2	3	2	3	4	5	6	2	1	2	3	4	5	1		1	2	3	4	2	1	2	3	4	5
3,3	4	3	2	3	4	5	3	2	1	2	3	4	2	1		1	2	3	3	2	1	2	3	4
3,4	5	4	3	2	3	4	4	3	2	1	2	3	3	2	1		1	2	4	3	2	1	2	3
3,5	6	5	4	3	2	3	5	4	3	2	1	2	4	3	2	1		1	5	4	3	2	1	2
3,6	7	6	5	4	3	2	6	5	4	3	2	1	5	4	3	2	1		6	5	4	3	2	1
4,1	3	4	5	6	7	8	2	3	4	5	6	7	1	2	3	4	5	6		1	2	3	4	5
4,2	4	3	4	5	6	7	3	2	3	4	5	6	2	1	2	3	4	5	1		1	2	3	4
4,3	5	4	3	4	5	6	4	3	2	3	4	5	3	2	1	2	3	4	2	1		1	2	3
4,4	6	5	4	3	4	5	5	4	3	2	3	4	4	3	2	1	2	3	3	2	1		1	2
4,5	7	6	5	4	3	4	6	5	4	3	2	3	4	5	3	2	1	2	4	3	2	1		1
4,6	8	7	6	5	4	3	7	6	5	4	3	2	6	5	4	3	2	1	5	4	3	2	1	

Для розрахунку НС пересилання ПО використано схему проходження ГПМ і ВПМ, наведену на рис. 1. Нормативні строки пересилання ПО розраховано відповідно до реальних відстаней між сусідніми обласними центрами (ОЦ), що становлять близько 250 км. Для проходження такої відстані із середньою швидкістю 50 км/год потрібно 5 год, і ще 1 год знадобиться на обмінювання ПО в обласних вузлах, усього 6 год. Прийнятий час відправлення пошти з обласних вузлів — 20^{00}, що забезпечує повернення всіх внутрішньообласних ПМ в обласні вузли і проведення вечірнього виймання ПО з поштових скриньок в ОЦ. До того ж ураховано, що за чинними нормативами ПО доставляються в ОЦ у день прибуття ПМ, якщо вони надходять в обласні вузли до 10^{00}. Для надійності цей норматив включає в себе резерв 2 год, тобто вважається, що ПО доставляються в ОЦ у день прибуття ПМ, якщо вони надходять в обласні вузли до 08^{00}.

Із двох можливих шляхів, що з'єднують обласні вузли з координатами $(x_п, y_п)$ і $(x_к, y_к)$ через транзитні вузли з координатами $(x_п, y_к)$ або $(x_к, y_п)$, обрано той, що забезпечує менший НС або більш раннє надходження до $(x_к, y_к)$.

Наприклад, шлях пересилання пошти

В (4,1) (Д+0, 20^{00}) – ГПМ 7 – ТВ (4,6) (Д+2, 02^{00} – Д+2, 20^{00}) – ВПМ 12 – В (1,6) (Д+3, 14^{00})

забезпечує НС Д+4; натомість ШПП

В (4,1) (Д+0, 20^{00}) – ВПМ 2 – ТВ (1,1) (Д+1, 14^{00} – Д+1, 20^{00}) – ГПМ 1 – В (1,6) (Д+3, 02^{00})

— НС Д+3; отже, обрано ШПП через ТВ (1,1); так само ШПП

В (1,3) (Д+1, 14^{00}) – ГПМ 2 – ТВ (1,1) (Д+2, 02^{00} – Д+2, 20^{00}) – ВПМ 1 – В (3,1) (Д+3, 08^{00})

забезпечує НС Д+3; що ж до ШПП

В (1,3) (Д+0, 20^{00}) – ВПМ 5 – ТВ (3,3) (Д+2, 08^{00} – Д+2, 14^{00}) – ГПМ 6 – В (3,1) (Д+3, 02^{00}),

то він також забезпечує НС Д+3, але з більш пізнім надходженням до вузла (3,1).

Проаналізуємо наведені в табл. 1 НС пересилання ПО за допомогою 8 + 4 = 12 двосторонніх (16 + 8 = 24 односторонніх) РПМ і порівняємо їх із НС пересилання ПО за допомогою РВПМ, що з'єднують ОЦ України з Києвом в існуючій СМПП. Серед НС пересилання ПО між усіма 552 парами обласних вузлів, наведених у табл. 1, 87 НС = 1; 310 НС = 2; 155 НС = 3, а середній НС пересилання ПО (математичне сподівання) становить $(87 \cdot 1 + 310 \cdot 2 + 155 \cdot 3)/552 = 2{,}123$ дні, тоді як в існуючій СМПП за допомогою 23 двосторонніх (46 односторонніх) РВПМ, що з'єднують обласні вузли між собою через Київ, установлений НС пересилання ПО становить 3 дні. Отже, завдяки застосуванню РПМ кількість ПМ скорочується в $46/24 = 1{,}917$ раза, а НС пересилання ПО — в $3/2{,}123 = 1{,}413$ раза, і це при тому, що норматив часу надходження ПМ до обласних вузлів, за яким забезпечується доставляння ПО в день надходження ПМ, зменшено з 10^{00} до 08^{00}. Більш того, застосування РПМ забезпечує незрівнянно вищу живучість МПЗ у надзвичайних ситуаціях за рахунок можливості створення величезної кількості обхідних шляхів перевезення ПО між обласними вузлами України.

Незалежно від виду СМПП, значення показників ТКМ визначаються як

$$\text{ТКМ} = \sum_{i=1}^{n} \sum_{\substack{j=1 \\ j \neq i}}^{m} p_{ij} l_{ij},$$

де p_{ij} і l_{ij} — значення відповідно міжвузлових потоків і міжвузлових відстаней між відповідними парами вузлів СМПП.

Для спрощення розрахунків прийнято $p_{ij} = 1$ ($i = 1, 2, ..., m$; $j = 1, 2, ..., n$; $j \neq i$). За розрахункову одиницю протяжності ПМ взято відстань між двома сусідніми вузлами, тобто відстань між двома заданими вузлами з координатами $(x_п, y_п)$ і $(x_к, y_к)$ вимірюється кількістю ділянок ПМ, що входять у шляхи пересилання ПО між цими вузлами.

Розподіл значень ТКМ між парами вузлів СМПП наведено в табл. 3.

Таблиця 3

Розподіл значень ТКМ між парами вузлів СМПП

Значення ТКМ	1	2	3	4	5	6	7	8	**Усього**
Кількість пар вузлів СМПП	76	116	124	104	72	40	16	4	**552**

Середнє значення (математичне сподівання) показника ТКМ

$$\text{ТКМ}_{ср} = (76 \cdot 1 + 116 \cdot 2 + 124 \cdot 3 + 104 \cdot 4 + 72 \cdot 5 + 40 \cdot 6 + 16 \cdot 7 + 4 \cdot 8)/552 = 3{,}333;$$

сумарне його значення

$$\text{ТКМ}_{\Sigma} = \sum_{i=1}^{n} \sum_{\substack{j=1 \\ j \neq i}}^{m} l_{ij} = 522 \quad \text{ТКМ}_{ср} = 1840.$$

Ураховуючи, що фактична відстань між сусідніми вузлами СМПП становить близько 250 км, знаходимо фактичне значення ТКМ між двома довільними вузлами: $3{,}333 \cdot 250 = 833{,}25$; далі обчислюємо фактичне значення сумарного ТКМ, що дорівнює $1840 \cdot 250 = 460\,000$.

В існуючій СМПП загальна кількість односторонніх РВПМ, що з'єднують 23 ОЦ із Києвом, дорівнює 46, а середня протяжність одного одностороннього ПМ, тобто середня відстань між ОЦ і Києвом, становить 435 км. Кожним із цих ПМ у кожному напрямі перевозиться по 23 ПП (по одному ПП від даного ОЦ до кожного з решти 23 ОЦ на прямому ПМ і по одному ПП від кожного з решти 23 ОЦ до даного ОЦ на зворотному ПМ). Звідси сумарне значення ТКМ в існуючій СМПП дорівнює $46 \cdot 23 \cdot 435 = 460\,230$, тобто практично збігається зі значенням сумарного ТКМ у СМПП із використанням РПМ.

Проблеми живучості мереж поштового зв'язку з решітчастими поштовими маршрутами

Живучість — одна з найважливіших властивостей МПЗ, яка визначає можливість функціонування МПЗ за умов виникнення надзвичайних ситуацій.

До надзвичайних ситуацій належать природні (повені, підтоплення, землетруси, ожеледиці, снігопади, зсуви) та техногенні (радіоактивне забруднення, викиди горючих, отруйних та вибухових речовин, аварії, катастрофи) катаклізми, навмисні дії (перекриття шляхів демонстрантами та страйкарями, терористичні акти), реконструкція і ремонт шляхів, ДТП, «завали» ОПЗ, зумовлені несвоєчасним вивезенням із них поштових посилок, які безсистемно укладаються в багаторядні штабелі, що займають усі основні та допоміжні приміщення, унеможливлюючи доступ до окремих посилок, а отже, їх оброблення та відправлення.

Як випливає з наведених далі міркувань, найвищою живучістю характеризуються МПЗ із РПМ.

Основними методами підвищення живучості МПЗ із РПМ виступають:

- відновлення ОПЗ;
- відновлення РПМ;
- відновлення ШПП.

Відновлення ОПЗ передбачає введення в дію законсервованих резервних ОПЗ, використання мобільних і пересувних ОПЗ, передавання зон обслуговування ушкоджених ОПЗ розташованим поблизу неушкодженим ОПЗ (наприклад, Миколаїв — Херсон, Рівне — Луцьк, Дніпро — Запоріжжя), застосування авіатранспорту для перевезень пошти.

Відновлення РПМ передбачає створення обхідних напрямів перевезення пошти, наприклад заміну перевезення пошти на ушкодженій ділянці горизонтального РПМ обхідними шляхами зверху чи знизу (рис. 2, *а*), або заміну перевезення пошти на ушкодженій ділянці вертикального РПМ обхідними шляхами ліворуч чи праворуч (рис. 2, *б*).

Відновлення РПМ доцільно проводити при ушкодженні незначної частини РПМ.

Відновлення ШПП передбачає аналіз усіх можливих шляхів з'єднання визначених вузлів МПЗ між собою і пошук серед них неушкоджених шляхів.

Відновлення ШПП доцільно проводити при ушкодженні значної частини РПМ.

Можливість з'єднання всіх вузлів МПЗ навіть при повному вилученні *трьох із чотирьох горизонтальних* або *п'яти з шести вертикальних* РПМ ілюструє рис. 3, *а* і 3, *б*.

а *б*

Рис. 2. Приклади створення обхідних РПМ

а *б*

Рис. 3. Ілюстрації можливості з'єднання вузлів МПЗ при ушкодженні значної частини РПМ

Живучість МПЗ тісно пов'язана з поняттям ***розрізу графа*** МПЗ — ненадмірного переліку його ребер, вилучення яких, скажімо через їх ушкодження, поділяє його на два не зв'язані між собою підграфи.

Сформулюємо три твердження стосовно поняття розрізу графа.

Твердження 1. Кожне з ушкоджених ребер, які потрапили в розріз графа, належить обом підграфам розрізаного графа.

Твердження 2. Межі підграфів розрізаних графів у місцях їх розрізів проходять по їхніх ушкоджених ребрах.

Твердження 3. Наявність ушкоджених ребер, які не відповідають твердженням 1 і 2, свідчить про надмірність переліку ушкоджених ребер графа, а через це такий перелік не може роглядатися як сукупність ребер, що становить розріз графа.

Оскільки існуючу МПЗ побудовано за радіально-вузловим принципом і з міркувань зменшення витрат на перевезення пошти виконано у вигляді графа-дерева, то вилучення будь-якого ребра цього

графа поділяє його на два не зв'язані між собою підграфи, а отже, структурна живучість такої МПЗ мінімальна.

При застосуванні кільцевих поштових маршрутів (КПМ) для перевезень пошти поділ графа МПЗ на два не зв'язані між собою підграфи потребує вилучення двох ребер у одному кільці, а отже, структурна живучість такої МПЗ значно вища.

При застосуванні РПМ для перевезень пошти кількість ребер, які необхідно вилучити для поділу графа МПЗ на два не зв'язані між собою підграфи, залежить від місць розташування відповідних вузлів МПЗ.

Слід особливо наголосити, що з'єднання вузлів МПЗ при ушкодженні значної частини РПМ відбувається не за рахунок уведення нових РПМ, а за рахунок використання існуючих РПМ, тобто за рахунок структурної надмірності існуючих МПЗ із РПМ. До того ж загальна кількість РПМ (4 горизонтальні і 6 вертикальних) значно менша, ніж сумарна кількість поштових маршрутів в існуючій МПЗ (23 поштові маршрути, що з'єднують обласні центри України з Києвом, і 13 поштових маршрутів, що з'єднують їх з регіональними сортувальними центрами).

Пов'яжемо ймовірності ушкодження МПЗ з імовірностями ушкодження відповідних ребер.

Згідно з відомою схемою Бернуллі, якщо при проведенні n незалежних випробувань імовірність p події A постійна, то ймовірність того, що подія A відбудеться рівно k разів, подається виразом

$$P_{k,n} = C_n^k p^k (1-p)^{n-k},$$

де $C_n^k = \dfrac{n!}{k!(n-k)!}$ — кількість сполучень з n по k, що визначає сумарну кількість випадків появи k подій A в процесі проведення n незалежних випробувань.

Увівши змінну i, що набуває значень від одиниці до k ($i = 1, 2, ..., k$), дістанемо сумарну ймовірність ушкодження МПЗ, обчислену за схемою Бернуллі:

$$P_{\Sigma,n} = \sum_{i=1}^{k} C_n^i p^i (1-p)^{n-i}.$$

Утім серед ушкоджень МПЗ слід ураховувати лише ті, за яких відповідний граф поділяється на два не зв'язані між собою підграфи, а тому кількість відповідних сполучень

$$B_n^k << C_n^k.$$

Так, $C_n^1 = C_{24}^1 = 24$, тоді як $B_{24}^1 = 0$ (ушкодження одного ребра не призводить до ушкодження МПЗ із РПМ);

$C_n^2 = C_{24}^2 = 276$, тоді як $B_{24}^2 = 8$, коли ушкоджено такі ребра:

(1,1) – (1,2), (1,1) – (2,1); (4,1) – (3,1), (4,1) – (4,2);
(4,6) – (4,5), (4,6) – (3,6); (1,6) – (2,6), (1,6) – (1,5);

$C_n^3 = C_{24}^3 = 2024$, тоді як $B_{24}^3 = 60$, коли ушкоджено такі ребра:

(1,2) – (1,1), (1,2) – (2,2), (1,2) – (1,3); (1,3) – (1,2), (1,3) – (2,3), (1,3) – (1,4);
(1,4) – (1,3), (1,4) – (2,4), (1,4) – (1,5); (1,5) – (1,4), (1,5) – (2,5), (1,5) – (1,6);
(4,2) – (4,1), (4,2) – (3,2), (4,2) – (4,3); (4,3) – (4,2), (4,3) – (3,3), (4,3) – (4,4);
(4,4) – (4,3), (4,4) – (3,4), (4,4) – (4,5); (4,5) – (4,4), (4,5) – (3,5), (4,5) – (4,6);
(2,1) – (1,1), (2,1) – (2,2), (2,1) – (3,1); (3,1) – (2,1), (3,1) – (3,2), (3,1) – (4,1);
(2,6) – (1,6), (2,6) – (2,5), (2,6) – (3,6); (3,6) – (2,6), (3,6) – (3,5), (3,6) – (4,6);
(1,1) – (2,1), (1,2) – (2,2), (1,2) – (1,3); (1,1) – (1,2), (2,1) – (2,2), (2,1) – (3,1);
(3,1) – (2,1), (3,1) – (3,2), (4,1) – (4,2); (4,1) – (3,1), (4,2) – (3,2), (4,2) – (4,3);
(4,5) – (4,4), (4,5) – (3,5), (4,6) – (3,6); (3,6) – (2,6), (3,6) – (3,5), (4,6) – (4,5);
(2,6) – (3,6), (2,6) – (2,5), (1,6) – (1,5); (1,6) – (2,6), (1,5) – (2,5), (1,5) – (1,4).

Розглянемо докладніше можливості відновлення ШПП на прикладі ШПП найбільшої протяжності між вузлами (1, 1) (верхній лівий) і (4, 6) (нижній правий).

Зазначимо, що загальна кількість ШПП між двома довільними вузлами з початковими координатами ($x_п$, $y_п$) і кінцевими координатами ($x_к$, $y_к$) визначається згідно зі співвідношенням

$$C_{x+y}^x = C_{x+y}^y,$$

де $x = |x_к - x_п|$, $y = |y_к - y_п|$.

У розглядуваному прикладі

$$x = |4 - 1| = 3,\ y = |6 - 1| = 5,$$
$$C_{x+y}^x = C_{x+y}^y = C_8^3 = C_8^5 = 56.$$

Для аналізу ШППП скористаємось ілюстраціями, наведеними на рис. 4.

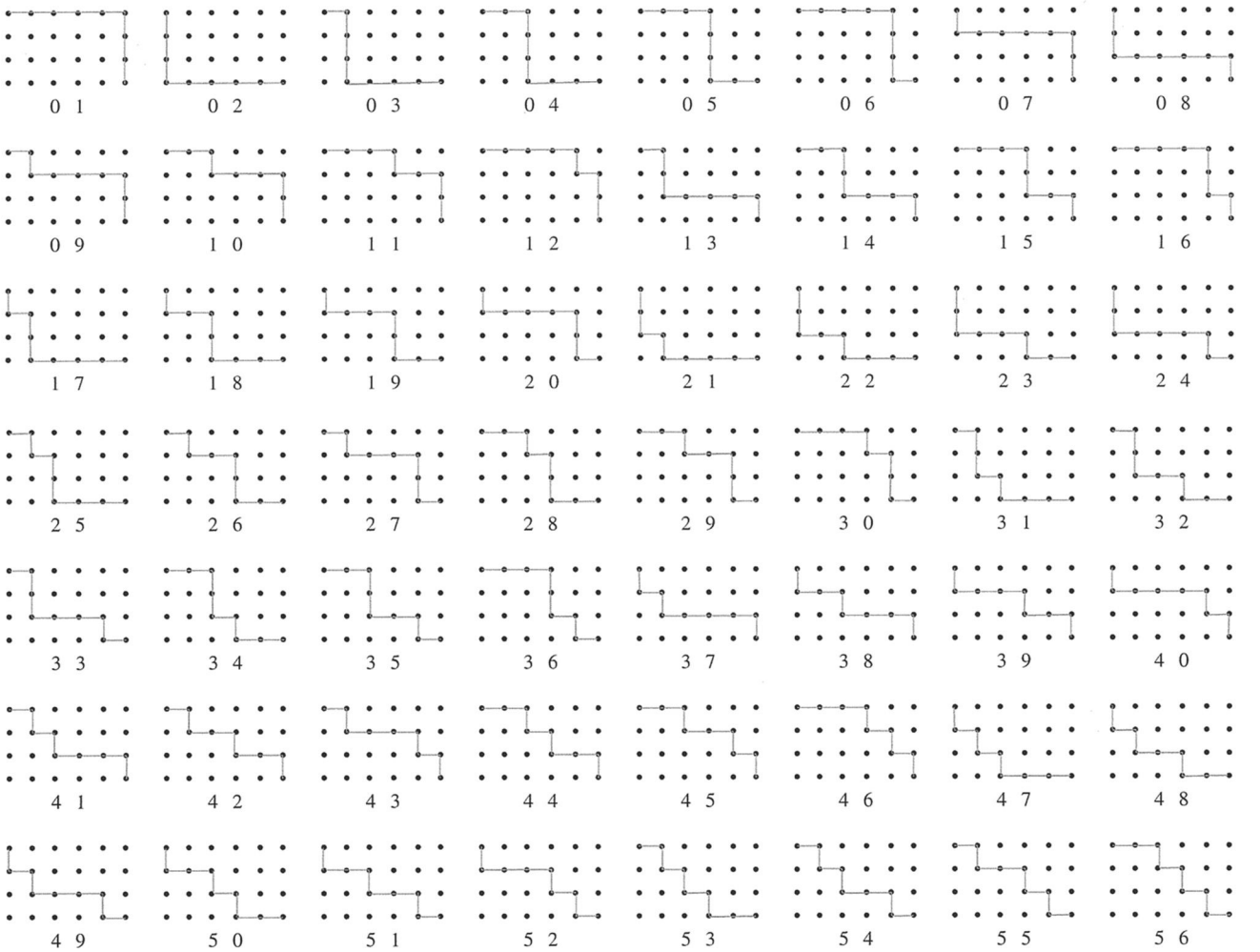


Рис. 4. Ілюстрації ШППП між вузлами (1, 1) і (4, 6)

Основні техніко-економічні показники СМПП із РВПМ, КПМ і РПМ подано в табл. 4. При розрахунку кількості поштових автомобілів (ПА) враховано щоденне курсування ПМ; добовий пробіг ПА — не більш ніж 1 000 км; розподіл ОЦ по зонах СМПП із РВПМ (4 ОЦ близької зони по 1 ПА, 16 ОЦ середньої зони — по 2 ПА, 3 ОЦ далекої зони — по 3 ПА); 6 ПМ одного напряму (12 ПМ зустрічних напрямів) у СМПП із КПМ; 4 ПА на кожному ГПМ і 2 ПА на кожному ВПМ у СМПП із РПМ.

Таблиця 4

Технико-економічні показники СМПП

Показник	РВПМ	КПМ	РПМ
Структура СМПП	46 ПМ, що з'єднують ОЦ між собою через Київ	Сукупність кількох КПМ	Решітка 6 × 4 РПМ
Протяжність ПМ, км	46 · 435 = 100 010	1 КПМ — 1 · 6 000 · 6 = 36 000 2 КПМ — 2 · 3 000 · 3 = 18 000 3 КПМ — 3 · 2 000 · 2 = 12 000	6 · 1500 · 2 + 4 · 2 500·4 = 28 000
Кількість ПА без урахування ТО і ремонту, од.	4 · 1 + 16 · 2 + 3 · 3 = 45	6 (в односторонніх), 12 (у двосторонніх) КПМ	6 · 2 + 4 · 4 = 28
НС пересилання ПО	Д + 3, Д + 2	1 КПМ — Д + 6 (Д + 3) 2 КПМ — Д + 6 (Д + 3) 3 КПМ — Д + 4 (Д + 2)	Д + 3, Д + 2, Д + 1
Живучість СМПП	Мінімальна	Низька	Висока

Висновки

1. СМПП із РПМ мають істотні переваги порівняно зі схемами на базі РВПМ і КПМ за живучістю і НС пересилання ПО, і мають проміжні характеристики за протяжністю ПМ і необхідною кількістю ПА.

2. Застосування РПМ для магістральних перевезень пошти найдоцільніше на територіях компактного розташування ОЦ.

3. На відміну від СМПП із РВПМ і КПМ, в яких необхідна живучість забезпечується за рахунок уведення додаткових ПМ, у схемах із РПМ необхідна живучість досягається за рахунок структурної надмірності самих цих схем.

4. Маючи високу структурну надмірність, СМПП із РПМ продовжують функціонувати навіть у разі виходу з ладу $m-1$ з m ВПМ або $n-1$ з n ГПМ.

5. У СМПП із РПМ забезпечується пересилання ПО прямими маршрутами або маршрутами з одним перевантаженням.

Рецензент: доктор техн. наук, професор **О. В. Барабаш**, Державний університет телекомунікацій, Київ.

Л. Е. Ящук

ИСПОЛЬЗОВАНИЕ РЕШЕТЧАТЫХ ПОЧТОВЫХ МАРШРУТОВ — ПУТЬ К РАДИКАЛЬНОМУ ПОВЫШЕНИЮ ЖИВУЧЕСТИ СЕТИ ПОЧТОВОЙ СВЯЗИ УКРАИНЫ

Рассмотрены преимущества использования магистральных почтовых маршрутов (ПМ) в виде прямоугольных решеток, позволяющих существенно повысить живучесть сети почтовой связи (СПС), сократить общее количество и общую протяженность ПМ.

Ключевые слова: СПС, живучесть СПС; объекты почтовой связи (ОПС); ПМ; горизонтальные ПМ (ГПМ); вертикальные ПМ (ВПМ); схема магистральных перевозок почты (СМПП); почтовые единицы (ПЕ); почтовые потоки (ПП); транзитные узлы (ТУ); нормативные сроки (НС) пересылки ПЕ; показатели тонно-километров (ТКМ) пересылки ПЕ; пути пересылки почты (ППП); восстановление ОПС; восстановление РПМ; восстановление ППП.

L. O. Yashchuk

USE OF GRATING MAIL ROUTES — THE WAY TO A RADICAL INCREASE IN THE SURVIVABILITY OF THE UKRAINIAN POSTAL NETWORK

The problems of using the main postal routes (PR) in the form of rectangular, which allow to significantly increase the surviva-bility of the postal communication network (PCN), reduce the total number and total length of the PR.

Keywords: PCN; survivability of PCN; PR; horizontal PR (HPR); vertical PR (VPR); main mail transport scheme (MMTS); postal units (PU); postal flows (PF); transit nodes (TN); normative terms (NT) of forwarding PU; indicators of tonna-kilometers (TKM) forwarding PU; mail forwarding routes (MFR); restoration of PCO; restoration of GPR; restoration of TPR.

УДК 004.055

Ю. В. МЕЛЬНИК, канд. техн. наук, ст. наук. співробітник;
К. П. СТОРЧАК, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

Побудова узагальненої нейромережної моделі ієрархічного управління мережею зв'язку

Визначено узагальнену математичну модель ієрархічного управління, а також модель об'єкта контролю і діагностики в разі нечітких умов щодо впливів і управління.

Ключові слова: критерії управління; модель управління; нечітка множина; система контролю; мережа зв'язку.

Вступ

Математичний аналіз реального явища, процесу чи системи починається з побудови відповідної математичної моделі. Дедалі зростаюча складність сучасних об'єктів дослідження та їх унікальність унеможливлюють явне відстеження причинно-наслідкових зв'язків у пізнавальному плані, що змушує дослідника при виборі або побудові математичної моделі діяти за умов невизначеності, яка виникає через неповноту вихідних даних (знань) [1].

Для усунення цих труднощів американський математик Л. А. Заде ввів нове математичне поняття — ***нечітка множина*** як узагальнення поняття звичайної множини [2; 3]. На відміну від традиційної математики та математичної логіки, що на кожному кроці моделювання вимагає точних і однознач-

них формулювань кожної з використовуваних закономірностей, нечітка логіка пропонує зовсім інший спосіб мислення, завдяки якому творчий процес моделювання відбувається на значно вищому рівні абстракції, за якого достатньо лише мінімального набору певних закономірностей.

Основна частина

Згідно з рекомендаціями МСЕ управління телекомунікаційними мережами здійснюється за чотирирівневою схемою, що включає в себе рівень управління елементами мережі; рівень управління мережею; рівень управління послугами; рівень управління бізнесом.

Критеріями рівня управління бізнесом можуть бути, наприклад, прибутковість П мережі та її інвестування І за певний проміжок часу [4].

Критеріями рівня управління послугами можуть бути, скажімо, обсяг V_S використання послуг і якість Q_S наданих за час ΔT послуг.

Критеріями рівня управління мережею можуть бути ступінь продуктивності ρ мережі в цілому і продуктивності її ρT по трактах, рівень завантаження Y (трафіку) мережі, ступеня $K_{\text{Г}}$ її готовності, ремонтопридатності $K_{\text{Р}}$ і контролепридатості $K_{\text{К}}$, ступінь (обсяг) поновлення таблиць маршрутизації $V_{\text{М}}$, час ΔT_R зміни конфігурації мережі з моменту зміни мережної ситуаційної обстановки S_N, ступінь S_e безпеки щодо несанкціонованого доступу та достовірність Д передавання даних у мережі.

Критеріями рівня управління елементами мережі (канал, тракт, лінія зв'язку, вузол комутації, маршрутизатор, склад та стан їх програмного забезпечення тощо) є міри роботоздатності $O_{\text{Р}}$ (залежно від стану W_E зазначених елементів), які формуються на основі вимірюваних характеристик e_q (атрибутів, параметрів), притаманних конкретним елементам, ступеня $K_{\text{К}}$ їх контролепридатності, що залежить від вектора $\vec{e}$ контрольованих параметрів елементів мережі (NE_i). При цьому розглядувані стани можна розбити на три класи: $W_{\text{Р}}$ — роботоздатні, $W_{\text{ПВ}}$ — передвідмовні, $W_{\text{В}}$ — відмовні.

Останні два класи можуть виникати через блокування, зумовлене різким підвищенням навантаження, випадковими порушеннями та ушкодженнями d, що виникають у платах, блоках і складових частинах елементів мережі.

Вочевидь, із погляду управління, щоб досягти правильного функціонування мережі, необхідно своєчасно знати точний її стан і своєчасно усувати передвідмовні $W_{\text{ПВ}}$ і відмовні $W_{\text{В}}$ стани, маючи на меті мінімізувати втрати якості Q_S послуг і досягти максимуму щодо утримання обсягу V_S обслуговування послуг.

Таким чином, ефективність і якість управління мережею істотно залежать від ефективності функціонування рівня управління елементами. З огляду на це побудуємо формальні залежності критеріїв рівнів управління від чинників впливу [5].

На 1-му рівні:

$$O_{\text{Р}_j} = f\left(W_{E_j}\right),\ j = \overline{1, m}; \tag{1}$$

$$K_{\text{К}_j} = f(\vec{e}),\ K_{\text{К}_j} \in [0, 1], \tag{2}$$

де m — кількість елементів мережі, $K_{\text{К}_j}$ — коефіцієнт контролепридатості елемента мережі, залежний від кількості контрольованих параметрів та їх інформативності.

На 2-му рівні

$$S_N = f\left(O_{\text{Р}_1}, O_{\text{Р}_2}, ..., O_{\text{Р}_m}\right);\ K_{\text{Р}} = f\left(\vec{O}_{\text{Р}}, K_{\text{К}}\right);\ K_{\text{Г}} = f\left(K_{\text{Р}}, K_{\text{К}}\right);\ \rho = f\left(\vec{O}_{\text{Р}}, Y, K_{\text{Г}}\right); \tag{3}$$

$$\Delta T_R = f(S_N, K_{\text{Г}});\ V_{\text{М}} = f(S_N, \Delta T_R, K_{\text{Г}});\ S_e = f(O_{\text{Р}}, K_{\text{К}});\ \text{Д} = f(S_N, K_{\text{Г}}, S_e). \tag{4}$$

На 3-му рівні

$$V_S = f(\rho, V_{\text{М}}, K_{\text{Г}});\ Q_S = f(\rho, S_e, Y, \text{Д}, K_{\text{Г}}). \tag{5}$$

На 4-му рівні

$$\text{П} = f(V_S, Q_S);\ \text{І} = f(\text{П}, Q_S). \tag{6}$$

Узагальнену модель управління з урахуванням (1)–(6) подано на рис. 1.

Узагальнену математичну модель управління подамо у вигляді такої впорядкованої множини:

$$M_{\text{УП}} = <T, X, Y, U, Q, Z, L, F, \varphi, P, C, A, B>, \tag{7}$$

де $T = \{t\}$ — множина моментів управління (керування);

$X = \{x\}$ — множина вхідних впливів на КТС;

$Y = \{y\}$ — множина вихідних відгуків КТС;

$U = \{u\}$ — множина керуючих впливів на КТС;

$Q = \{q\}$ — множина внутрішніх станів;

$Z = \{z\}$ — множина цілей;

L, F — оператори переходу відповідно станів і виходів:

$$L: T\times X\times Q\to Q,\ \ F: T\times X\times Q\to Y;$$

φ — оператор алгоритму керування;

$P=\{p(q)\}$ — множина ймовірнісних мір;

$C=\{c(u)\}$ — множина складових вартості управління;

$A=\{\alpha(u)\},\ B=\{\beta(u)\}$ — множина помилок управління відповідно першого і другого роду.

Рис. 1. Узагальнена модель управління телекомунікаційною системою

В основу будь-якого управління покладено інформацію, яку можна подати впорядкованою парою множин $In=<X_{\text{К}}, Y_{\text{К}}>$, тоді саме управління являє собою деяку залежність від алгоритму $U=\varphi(In, Z)$, де Z — підмножина вибраних цілей управління, а φ — оператор, який формує керування U, $\varphi: In\times Z\to U$.

Згідно з викладеним модель управління можна подати у вигляді такої залежності:

$$Y=F(T, X, U, \Xi), \tag{8}$$

де Ξ — зовнішній неконтрольований вплив.

Оператор F визначається як $F=St, b$, де St — структура КТС; b — вектор досліджуваних параметрів.

Нехай, наприклад, $Y=b_0+b_1T+b_2X+b_3U+b_4\Xi$.

Згідно з рекомендаціями MCE та концепцією TMN чотирирівневе управління мережею зв'язку з урахуванням елементів мережі та елементів корекції нижче розташованого рівня управління з боку верхніх рівнів маємо ієрархічну схему управління, зображену на рис. 2.

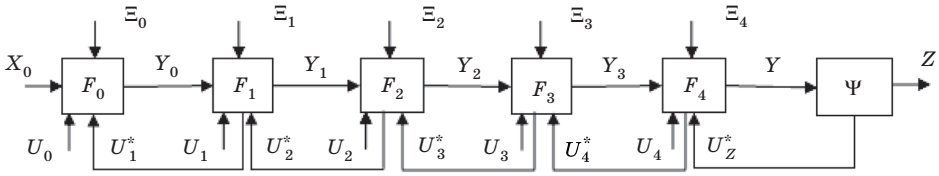


Рис. 2. Конвеєрно-адаптивне управління: F_i — оператор елемента мережі; X_0 — відомі впливи навколишнього середовища; U_i^* — управління з вищого рівня; U_Z^* — корекція значення Y виходу 4-го рівня; Ξ — зовнішній неконтрольований вплив

Узагальнена математична модель для даної схеми управління набирає вигляду

$$Y=F_4\Big(F_3\Big(F_2\Big(F_1\Big(F_0\Big(X_0, U_0, U_1^*, \Xi_0\Big)U_1, U_2^*, \Xi_1\Big)U_2, U_3^*, \Xi_2\Big)U_3, U_4^*, \Xi_3\Big)U_4, U_Z^*, \Xi_4\Big), \tag{9}$$

де Ξ_i — невідомий вектор впливу на кожному рівні управління.

З огляду на те, що телекомунікаційна мережа є складною розподіленою структурою, її модель управління можна подати у вигляді графа, зображеного на рис. 3.

Узагальнена математична модель ієрархічного управління має вигляд:

$$Y=F_4\left(F_{3q\Sigma k}\left(F_{2k\Sigma j}\left(F_{1j\Sigma i}\left(F_{0i}^{(j)}\left(X_{0i}^{(j)}, U_{0i}^{(j)}, U_{1i}^{(j)^*}, \Xi_{0j}^{(j)}\right), U_{1j}, U_{2j}^*, \Xi_{1j}\right), U_{2k}, U_{3k}^*, \Xi_{2k}\right), U_3, U_4^*, \Xi_3\right), U_4, U_Z^*, \Xi_4\right),$$

$$i=1, \ldots, n;\ j=1, \ldots, m;\ k=1, \ldots, q,$$

де $F_{0i}^{(j)}$ — оператор мережного елемента NE_i підмережі j; $F_{1j\Sigma i}$ — оператор агрегування за i 1-го рівня управлення мережею; $F_{2k\Sigma j}$ — оператор агрегування за k 2-го рівня управління мережею; $F_{3q\Sigma k}$ — опе-

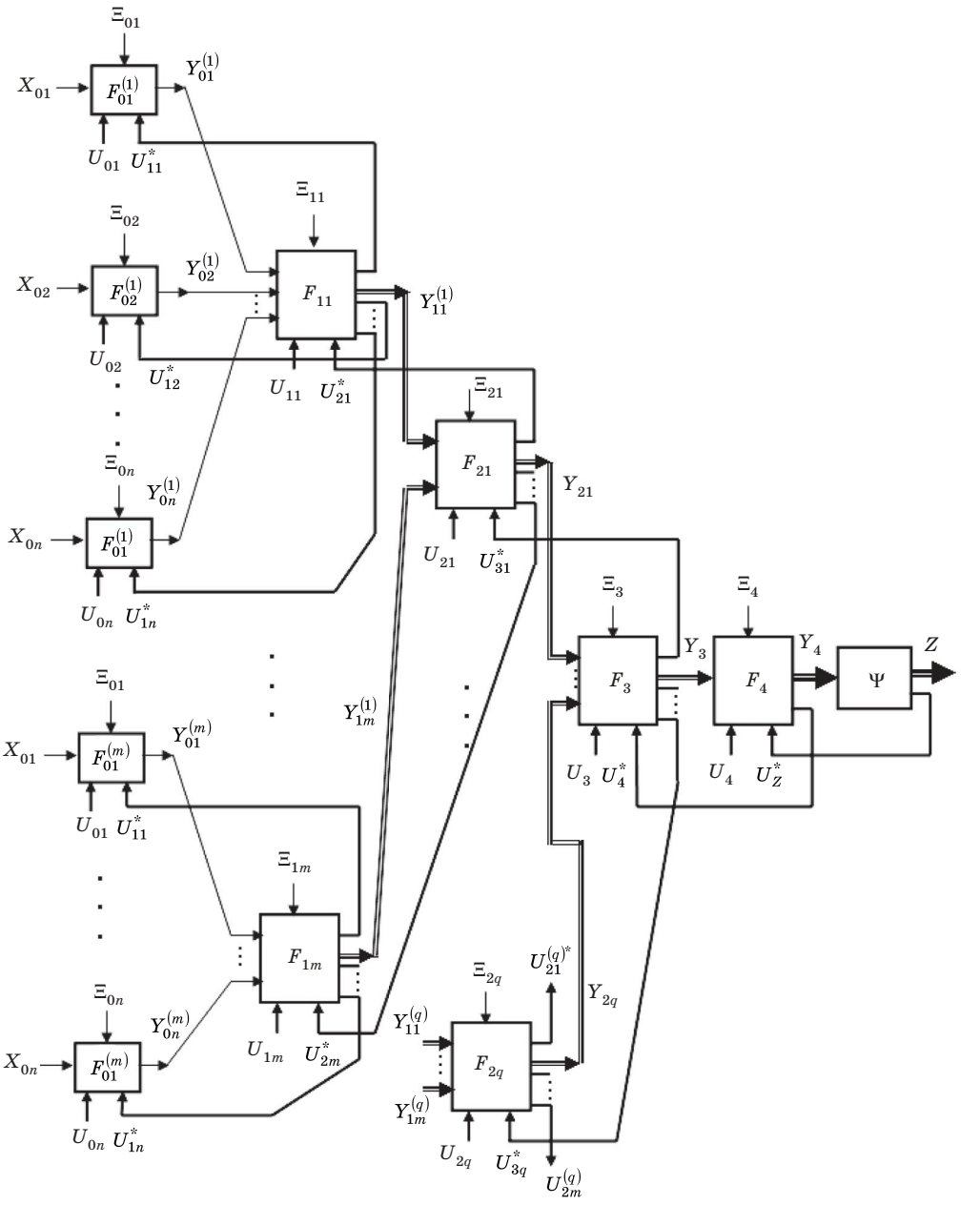


Рис 3. Ієрархічна модель управління телекомунікаційною мережею: F_{1m}, F_{2q}, F_3 — агрегуючі оператори відповідних рівнів; Y_{ij} — вихідні вектори значень відповідних рівнів; U_i — вектори управлінь

ратор агрегування за q 3-го рівня управління мережею; F_4 — оператор 4-го рівня управління мережею; n — кількість мережних елементів NE в підмережі j; m — кількість підмереж NE в мережі k; q — кількість мереж, обслуговуваних реальною TMN.

Складовою будь-якої складної системи управління є контроль і діагностика (КД) або моніторинг стану об'єкта управління (ОУ). Система контролю і діагностики ОУ забезпечує спеціальний вид управління з підтримання регламентованого технічного стану об'єкта спостереження. Агреговану модель системи КД можна подати як упорядковану систему множин:

$$M_{\text{КД}} = < T^*, E, \Theta, \Pi, \Phi, P, C, A, B >,$$

де $E = \{\vec{e}_i\}_{i=1}^m$ — множина технічних станів об'єкта управління, $E \subset Q$; $\vec{e} = (e_{i1}, e_{i2}, ..., e_{in})$, e_{ij} — узагальнена ознака i-го агрегованого стану, $j = 1, ..., n$; $\Theta = \{e_{ij}\}$, $i = 1, ..., m$ — множина ознак усіх технічних станів; $\Pi = \{\pi_i\}_{j=1}^n$ — множина перевірок для відповідної ознаки j, $\Pi \subset U$; $T^* = \{t\}$ — множина моментів контролю t, $T^* \subset T$; Φ — оператор виходу, Φ: $T^* \times E \times \Pi \to \Theta$; $P = \{p(e_i)\}_{i=1}^m$ — множина ймовірнісних мір; $C = \{c(\pi_j)\}_{j=1}^n$ — множина цін перевірок; $A = \{\alpha_j\}_{j=1}^n$, $B = \{\beta_j\}_{j=1}^n$ — множина помилок першого α_j і β_j другого роду перевірок π_j.

Модель об'єкта контролю і діагностики включає в себе математичні моделі справного і несправного стану технічного об'єкта:

$$Y = F_0(X, Q, T),$$
$$Y_i = F_i(X, Q, T),\ i \in Def,$$

де F_0, F_i — оператори відповідно справного і несправного стану ОУ; $Def = \{d_i\}$ — множина несправностей, причому $Def = \Psi(E_d)$, де E_d — множина несправних станів, $E_d \subset E$.

Як відомо контроль і діагностика в структурі управління складною системою розв'язують три основні завдання.

1. Перевірка роботоздатності об'єкта управління. За результатом цієї перевірки відбувається перехід або до застосування ОУ за прямим призначенням, або до аналізу його стану.

2. Пошук дефектних елементів в ОУ. Ідеться про встановлення первинної причини відмови або відшукання дефектних елементів.

3. Прогнозування технічного стану ОУ.

За результатами контролю та діагностики розв'язуються завдання управління. При цьому основними факторами будь-якого управління виступають

- мета управління Z^*;
- інформація In про стан об'єкта і навколишнього середовища;
- вплив на об'єкт U;
- алгоритм управління φ, $U = \varphi(In, Z^*)$.

Проте в реальних умовах ефективно та в повному обсязі знаходити розв'язання завдань управління об'єктом через їх складності, а також неповноту інформації про навколишнє середовище і стан об'єкта, неточно сформульовану мету управління, обмеженість ресурсів, дефіцит часу на ухвалення рішення та з інших причин неможливо. Саме тому складові моделі управління можуть бути сформульовані в концепціях теорії нечітких множин. Тоді залежно від конкретної ситуації модель управління можна подати як систему множин:

$$M_{\text{УП}} = < T, X, Y, U, \tilde{Q}, Z, L, F, \varphi, G, C, A, B >, \quad (10)$$

де $\tilde{Q} = \{q/\mu(q)\}$ — нечітка множина станів; $\mu(q)$ — нечітка функція належності, $\mu(q) \in [0,1]$; $G\{g(q)\}$ — множина нечітких мір, $g(q) \in [0,1]$,

або

$$M_{\text{УП}} = < T, X, Y, \tilde{U}, \tilde{Q}, \tilde{Z}, L, F, \varphi, G, C, A, B >, \quad (11)$$

де $\tilde{U} = \{u/\mu(u)\}$ — нечітка множина управляючих впливів; $\tilde{Z} = \{z/\mu(z)\}$ — нечітка множина цілей,

або

$$M_{\text{УП}} = < T, X, Y, \tilde{U}, \tilde{Q}, \tilde{Z}, L, F, \varphi, G, \tilde{C}, A, B >, \quad (12)$$

де $\tilde{C} = \{c/\mu(c)\}$ — нечітка множина витрат.

Ієрархічна модель об'єкта управління з нечіткими складовими набирає вигляду

$$Y = F_4\left(F_3\left(F_2\left(F_1\left(X_1, \tilde{U}_1, \Xi_1\right), \tilde{U}_2, \Xi_2\right), \tilde{U}_3, \Xi_3\right), \tilde{U}_4, \Xi_4\right). \quad (13)$$

Узагальнена математична модель системи контролю і діагностики у складі системи управління за нечітких умов подається як упорядкована множина:

$$M_{\text{КД}} = < T^*, \tilde{E}, \Theta, \Pi, \Phi, G, \tilde{C}, A, B >,$$

де $\tilde{E}$ — множина нечітких станів об'єкта управління; $\tilde{C}$ — множина нечітких цін перевірок або обмежень; $\tilde{G}$ — множина нечітких мір.

Висновки

♦ З огляду на те, що контрольовані та неконтрольовані впливи й стани телекомунікаційної мережі можна, як правило, описати лише в термінах нечітких множин, уперше визначено узагальнену математичну модель ієрархічного управління та модель об'єкта контролю і діагностики за нечітких умов щодо впливів і управління.

♦ Сучасна телекомунікаційна мережа включає в себе величезну кількість пасивних та активних мережних елементів. Тому наступним кроком дослідження буде визначення підходів до побудови узагальнених моделей управління мережними елементами.

Список використаної літератури

*1. **Нечеткие** множества в моделях управления искусственного интеллекта / [А. Н. Аверкин, И. З. Батыршин, А. Ф. Блишун, В. Б. Силов, В. Б. Тарасов]; под ред. Д. А. Поспелова.— М.: Наука, 1986.— 312 с.*

*2. **Заде, Л. А.** Основы нового подхода к анализу сложных систем и процессов принятия решений / Л. А. Заде // Математика сегодня.— М.: Знание, 1974.— С. 5–49.*

*3. **Zadeh, L. A.** Fuzzy sets / L. A. Zadeh // Information and Control.— 1965.— P. 338–353.*

*4. **Підручник** для студентів вищих навчальних закладів за напрямком «Телекомунікації» з дисциплін СП, ТОТСМ, ТЕСЗ.-К ДУТ 2014-700с з. іл. Бібліогр. в кінці розд. ISDN 966-575-039-9 [Електронний ресурс].— Режим доступу:*

http://www.dut.edu.ua/ua/lib/1/category/1116/view/684

*5. **Narendra, K. S.** Bck propagation in dynamical systems containing neural networks [Електронний ресурс] / K. S. Narendra, K. Parthasarathy.— Режим доступу:*

https://ac.els-cdn.com/0888613X9290014Q/1-s2.0-0888613X9290014Q-main.pdf?_tid=7c90fedc-f5d8-11e7-b7aa-00000aab0f6c&acdnat=1515569761_83620b6a11dd5631dff6b78324e61b2e

Рецензент: доктор техн. наук, професор **В. В. Вишнівський**, Державний університет телекомунікацій, Київ.

Ю. В. Мельник, К. П. Сторчак

ПОСТРОЕНИЕ ОБОБЩЕННОЙ НЕЙРОСЕТЕВОЙ МОДЕЛИ ИЕРАРХИЧЕСКОГО УПРАВЛЕНИЯ СЕТЬЮ СВЯЗИ

Определена математическая модель иерархического управления, а также представлена модель объекта контроля и диагностики при нечетких условиях воздействий и управления.

Ключевые слова: критерии управления; модель управления; нечеткое множество; система контроля; сеть связи.

Yu. V. Melnik, K. P. Storchak

CONSTRUCTION OF A GENERALIZED NEURAL NETWORK MODEL OF HIERARCHICAL CONTROL OF A COMMUNICATION NETWORK

The article defines a mathematical model of hierarchical control and a model of the object of control and diagnostics under fuzzy conditions of impacts and control.

Keywords: management criteria; management model; fuzzy set; control system; communication network.

УДК 004.8+65.05+681.5

В. В. ВИШНІВСЬКИЙ, доктор техн. наук, професор;
Ю. І. КАТКОВ, канд. техн. наук, доцент;
С. О. СЄРИХ, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

Роль і місце інформаційної інфраструктури під час виникнення явища критичності організаційної системи

Розглянуто загальні положення щодо організаційних систем із критичною інфраструктурою та умови реорганізації як напрямку дослідження невідповідності інфраструктури організаційної системи в результаті впливу можливих викликів або загроз, які можуть призвести до критичного стану будь-який важливий елемент цієї системи або інших систем. Виконано аналіз термінів для опису впливу на організаційну систему з критичною інфраструктурою, що викликають необхідність її реорганізації. Подано математичну модель оцінювання рівня критичності організаційної системи з критичною інфраструктурою.

Ключові слова: організаційні системи з критичною інфраструктурою; інфраструктура організаційної системи; виклики; загрози; реорганізація.

Вступ

Уся історія розвитку людського суспільства є процес удосконалення організаційних форм його діяльності, ускладнення структури організації людей і засобів виробництва внаслідок розвитку поділу суспільної праці, забезпечення органами управління взаємодії елементів складних організаційних (організаційно-технічних або організаційно-соціальних) систем через обмін ресурсами та інформацією між ними.

Початок XXI сторіччя характеризується новим явищем у розвитку організаційних систем — революційним упровадженням засобів телекомунікації, автоматизації та інтелектуалізації в усі процеси управління. Природно, що за умов інформатизації та інтелектуалізації суспільства виникають виклики та загрози безпосередньо для інформаційної інфраструктури будь-яких організаційних систем. Виклики та загрози стосуються деяких уразливих об'єктів (елементів організаційної системи), наслідком чого є її нестійкій стан у вигляді кризових ситуацій її функціонування. Так, для систем управління

енергетикою це яскраво ілюструють події з відімкнення підстанцій у Нью-Йорку чи Москві. Економічні збитки внаслідок відмови уразливого об'єкта вартістю в кілька тисяч сягають сотень мільйонів. Вочевидь, це змушує чинити протидію цим викликам та загрозам, забезпечуючи захист уразливих об'єктів або вдаватись до асиметричних дій щодо джерел цих викликів та загроз.

Постановка завдання

Під час розв'язання завдань системою управління складними організаційними системами за умов впливу викликів та загроз на уразливі елементи інфраструктури організаційних систем постає необхідність автоматизації розробки варіантів управлінських рішень, скажімо з прискорення адаптації (скорочення часу адаптації або зменшення витрат матеріальних ресурсів) до нових умов функціонування на основі впровадження новітніх інформаційних технологій (телекомунікаційних, технологій автоматизації, інтелектуальних, штучного інтелекту тощо) та організації відповідної системи інформаційної безпеки для запобігання кризовим явищам. Відомо, що для автоматизації прийняття рішень необхідно розв'язати проблему формалізації процесів адаптації складної організаційної системи до нових умов функціонування з урахуванням імовірних загроз і впливів. Це дасть змогу визначати методи оцінювання показників критичності та створювати рекомендації з протидії критичним ситуаціям. Звідси виникає необхідність формалізації явища критичності для складної організаційної системи та розробки методів оцінювання показників критичності за допомогою моделі інформаційної безпеки складної організаційної системи з критичною інфраструктурою (ОСКІ). Це завдання особливо актуальне для розробки моделей управління інтелектуальними системами управління.

Аналіз останніх публікацій

Постановка такого завдання вже неодноразово пропонувалася в теорії організації складних систем [1–5]. Дослідженню управлінської діяльності керуючих органів присвячено багато праць, де пропонуються різноманітні моделі управління об'єктом керування. Наприклад, здійснено дослідження моделей ієрархічних систем управління [7], моделей загальної теорії систем [7; 8], моделі організації систем [2; 4], моделі самоорганізації в нерівноважних системах [9; 10], моделі стійкості системи [11], моделі адміністративної поведінки [12], моделі структурної організації та стратегічного управління [13–18]. Аналогічні питання розглянуто у [19], але для інфраструктури національної безпеки без урахування інтелектуалізації суспільства. Проте рівень інтелектуалізації суспільства необхідно враховувати, коли йдеться про визначення критичності складної організаційної системи. Аналіз праці у галузі забезпечення безпеки складної організаційної системи показав, що загальної кількісної оцінки та моделі, яка одночасно враховувала б інформатизацію та інтелектуалізацію, не існує.

Основна частина

Для формалізації процесів адаптації складної організаційної системи до нових умов функціонування, що характеризується інформатизацією та інтелектуалізацією, для створення математичних моделей аналізу ситуацій протидії інформаційним викликам і загрозам та розробки варіантів рішень на основі відповідного математичного апарату необхідно введення низки взаємозв'язаних понять.

Організаційна система **(ОС)** — це сукупність дієвих чинників і засобів, організована у вигляді системної структури для виконання заданого переліку функцій (завдань) при досягненні встановлених цілей [21]. Для розвитку процесу поділу суспільної праці в певній галузі виробництва створюється відповідна інфраструктура.

Інфраструктура — це комплекс взаємозв'язаних обслуговуючих структур, що становлять і/або забезпечують основу для розв'язання проблеми (задачі). Наприклад, інфраструктура, що забезпечує загальні умови функціонування економіки, включає в себе енергетичні, транспортні, телекомунікаційні мережі, інформаційні, логістичні системи тощо.

Криза організаційної структури — це небезпечний і нестійкий перехідний стан, коли наявна організаційна структура, призначена для розв'язання певних завдань, стає неадекватна цим завданням, що призводить до непередбачуваних ситуацій. Характерними ознаками кризи є порушення відповідності між попитом і пропозицією, між потребами і їх задоволенням. Природа кризи приховується в наявності уразливого об'єкта щодо певної загрози.

Загроза — це потенційні або реальні дії, що можуть спричинити порушення існуючого стану функціонування організаційної системи через збої в технології управління. Загроза може бути передумовою виникнення порушення одного чи кількох аспектів безпеки, неприпустимого ризику під час прийняття керуючих рішень.

Уразливий об'єкт — це слабка ланка в організаційній системі, нездатна протистояти шкідливим впливам (загрозам), дія яких порушує технологію управління. Якщо цей об'єкт посідає важливе місце

в системі, то його пошкодження (втрата) може призвести до катастрофічних наслідків. Розрізняють людську, технічну та інформаційну уразливість. Людська уразливість виникає внаслідок психологічних впливів. Технічна — результат виникнення несправності в механізмах управління системою. Інформаційна уразливість є наслідком непередбачуваного впливу інформації на процес прийняття рішень. Загроза і уразливий об'єкт — це передумови виникнення критичного стану інфраструктури.

Критичній стан інфраструктури (організаційної системи) виникає тоді, коли її потенційно уразлива структура внаслідок дії середовища раптово втрачає задані властивості та набуває інших властивостей, які не могли бути передбачені при її проектуванні. Для запобігання кризовому стану в організаційній системі здійснюються заходи з її реформування завдяки застосуванню методів цільового управління і відповідних технологій управління.

Реформування — це перетворення, удосконалення законодавчим шляхом будь-якої галузі державного або суспільного життя. Передбачає два напрямки дій: нормативно-правовий і організаційно-технічний. Нормативно-правовий напрямок пов'язаний зі змінами в нормативно-правових актах, а організаційно-технічний напрямок передбачає перебудову системи управління, модернізацію всієї інфраструктури, зміну її організаційної структури, технічне переоснащення, зміну способів застосування тощо. Реформування організаційних систем є еволюційною формою вирішення керівництвом множини нових завдань за допомогою заходів вдосконалення організаційних відносин у діючих структурах.

Реорганізація — це процес перетворення, перебудови, зміни структури та функцій установи (організації), удосконалення організаційних відносин у діючих структурах, пристосування технологій управління до потреб цільового управління. Реорганізація виступає організаційно-технічним напрямком реформування. Особливість процесів реорганізації — їх поступовість і неухильність щодо вдосконалення організаційно-технічних відносин у постійно діючих структурах організаційної системи при нейтралізації можливих наслідків прояву загрози, що може створити критичний стан цієї системи. Нейтралізація негативних наслідків такого стану тягне за собою низку нових завдань, які наявна структура здебільшого не здатна вирішувати в межах існуючих організаційно-штатних структур постійно діючої організаційної системи. Тому її результатом є зміни в цих організаційно-штатних структурах.

Зрештою поняття «реорганізація» передбачає вдосконалення організаційних відносин у діючих структурах за допомогою нейтралізації можливого прояву негативної дії виклику або загрози на технологію управління в кібернетичному просторі. Реорганізація доцільна тільки в такій організаційній системі, де існує можливість появи критичного стану інфраструктури, тобто кризи в організаційній структурі. Звідси пропонується реорганізацію пов'язувати з передумовами виникнення критичного стану елементів системи, а при висвітленні цього явища йтиметься про згадувану вже *організаційну систему з критичною інфраструктурою*.

Система з критичною інфраструктурою, або критична система, — це сукупність фізичних або віртуальних систем і засобів, настільки важливих для держави, що їх вихід із ладу або знищення може призвести до згубних наслідків у сфері оборони, економіки, охорони здоров'я та безпеки нації [20]. Це поняття охоплює ключові сектори, де є уразливі об'єкти: органи управління; інформаційні і телекомунікаційні системи та мережі; енергетику; транспорт; фінансові системи тощо. Їх стан має вплив на рівень воєнної, економічної, екологічної та інших видів безпеки.

Кібернетичний простір (вид інформаційного простору) — середовище, що перебуває під юрисдикцією держави (установи, фірми) і в якому здійснюється створення, зберігання та поширення інформації. Наприклад, основними складовими захищеного інформаційного простору держави можуть бути інформаційна інфраструктура виробничого об'єднання з відповідними показниками захищеності, а також елементи та засоби інформаційної інфраструктури.

Інформаційна інфраструктура — це система організаційних структур (комплекс систем, установ, служб, частин і підрозділів, необхідних для функціонування органів управління), що забезпечують функціонування і розвиток інформаційного простору країни (установи, фірми) і засобів інформаційної взаємодії. Зазначена інфраструктура включає в себе сукупність інформаційних центрів, банків даних і знань, систем зв'язку, що забезпечує доступ споживачів до інформаційних ресурсів, необхідних для управління організаційними системами, сервісні та інтелектуальні підсистеми. Наприклад, вона може складатись із підсистем, поданих на рис. 1.

Інформаційна інфраструктура, як випливає з рис. 1, має частинні структури, що відповідають за другорядні функції: за створення, накопичення, зберігання та поширення інформаційної продукції; за її виробництво та поширення: за виробництво інформаційних технологій; за сервісне та інтелектуальне обслуговування елементів інфраструктури. Результатом функціонування інформаційної інфраструктури є створення захищеного інформаційного простору для організаційних структур.

Рис. 1. Складові інформаційної інфраструктури

Матеріально-технічною основою процесів інформатизації та інтелектуалізації органів управління в сучасних умовах правомірно вважати інформаційну систему (ІС).

Інформаційна система — це множина взаємозв'язаних матеріальних і програмних об'єктів (засобів і комплексів інформатизації, засобів їх забезпечення, засобів інтелектуалізації, сервісів), що безпосередньо беруть участь у забезпеченні надання інформаційних послуг користувачам для прийняття рішення. Поняття ІС об'єднує множину взаємозв'язаних об'єктів (автоматизовані аналітичні, розрахункові, довідкові, телекомунікаційні, інтелектуальні системи інформаційної інфраструктури сучасної організаційної системи), що безпосередньо беруть участь у наданні інформаційних та інтелектуальних послуг в інформаційному просторі.

Уразливість в інформаційній системі є подією, за якої компрометується один або кілька аспектів безпеки інформації (доступність, конфіденційність, цілісність і достовірність). Наявність уразливого об'єкта створює слабку ланку, що може призвести до порушення безпеки інформації. Природно, що впливи загрози на технологію управління можуть викликати критичний стан будь-якої організаційної системи, яка через це стає ОСКІ. Звідси правомірно передбачати залежність безпеки будь-якої організаційної системи від рівня інформаційної безпеки. Тому сьогодні під час реорганізації організаційних систем необхідно враховувати процеси, пов'язані з упровадженням новітніх інформаційних технологій.

Безпека ОСКІ — це стан правових норм і відповідний їм стан організаційно-технічних заходів, що гарантує відсутність неприпустимого ризику, пов'язаного з ухваленням стратегічних рішень та захистом ресурсів у всіх ланках управління.

Об'єктом забезпечення безпеки в ОСКІ є ефективне функціонування соціальних і технічних складових ОСКІ. Соціальними об'єктами є політичний устрій, суспільні установи тощо. Технічними об'єктами є матеріальні та інформаційні ресурси, інфраструктура, інформаційні технології, інформаційні системи, що застосовуються в системі управління. Для забезпечення безпеки створюється система безпеки ОСКІ.

Система безпеки ОСКІ — це організована сукупність суб'єктів (органів управління та посадових осіб, об'єднаних цілями та завданнями щодо захисту інтересів у заданій сфері (політичній, економічній, інформаційній, воєнній), об'єктів захисту та об'єктів забезпечення, що здійснюють узгоджену діяльність на основі прийнятих вимог, методів і засобів.

Функції системи безпеки ОСКІ включають у себе захист інтересів у певній сфері; захист інтересів об'єкта (установи, фірми, суспільства, держави) від внутрішніх та зовнішніх викликів і загроз; упровадження сучасних інформаційних технологій; забезпечення безпеки інформаційних і телекомунікаційних систем, які створюють інформаційний простір для організаційних систем; запобігання впливу негативних чинників на функціонування інформаційних систем.

Отже, інформатизація з інтелектуалізацією стає системоутворюючим фактором. Але ці процеси породжують суперечності між поліпшенням умов удосконалення організаційних відносин у діючих структурах і необхідністю постійного адекватного реагування технологій управління на появу нових викликів та загроз, які призводять до кризи організаційних структур, дезорганізації технологій управління в процесах функціонування організаційної системи. Інформаційна інфраструктура стала ахіллесовою п'ятою сучасних організаційних систем і перетворила їх на системи з критичною інфраструктурою. Практично всюди, де є застосування засобів інформатизації органів управління небезпечними технологічними об'єктами, виникають принципово нові умови впливу і прояви загроз через уразли-

вість об'єктів інформаційних систем і, як наслідок, необхідність організації безпеки в ОСКІ. У таких системах стає актуальним поняття безпеки ОСКІ.

Для будь-якої ОСКІ можна визначити множину ознак при класифікації потенційних загроз її безпеці. Тут зазначимо, що загрози або створюють «вікно» небезпеки, або «відчиняють» вікна небезпеки для завдання шкоди зловмисником (або порушником) безпеки.

Вікно небезпеки системи з критичною інфраструктурою — це проміжок часу від моменту, коли з'являється можливість використати уразливі об'єкти в ОСКІ, і до моменту, коли вікно ліквідується. Тоді рівень безпеки можна тлумачити так, як це запропоновано на рис. 2.

Небезпека (рівень безпеки ОСКІ) — це ступінь відповідності системи цілям у ситуації, що склалася. Він характеризується кількісними та якісними показниками, взятими для його оцінювання.

Загальною кількісною оцінкою небезпеки ОСКІ можна запропонувати показник на основі відомого підходу Б. В. Васильєва [3], коли кількісний рівень безпеки ОСКІ має оцінюватися ступенем готовності організаційної системи до виконання поточного переліку завдань, тобто показник $\Phi_б$ визначає ефективність дії системи безпеки (рівень небезпеки).

$$\Phi_б = \frac{\Phi_г}{\Phi_{г0}}, \tag{1}$$

де $\Phi_г$ — показник готовності до застосування ОСКІ в реальних умовах; $\Phi_{г0}$ — значення того самого показника, але визначеного за умови, що система функціонує найкращим чином (ідеально).

Особливістю підходу Б. В. Васильєва є те, що показник $\Phi_б$ визначає ефективність дії системи безпеки (рівень небезпеки) і водночас аналітично пов'язаний із показником $\Phi_г$ ефективності функціонування ОСКІ. Це дає змогу на основі заданих вимог до готовності ОСКІ сформулювати вимоги до системи безпеки визначенням деякого мінімально припустимого рівня безпеки ОСКІ.

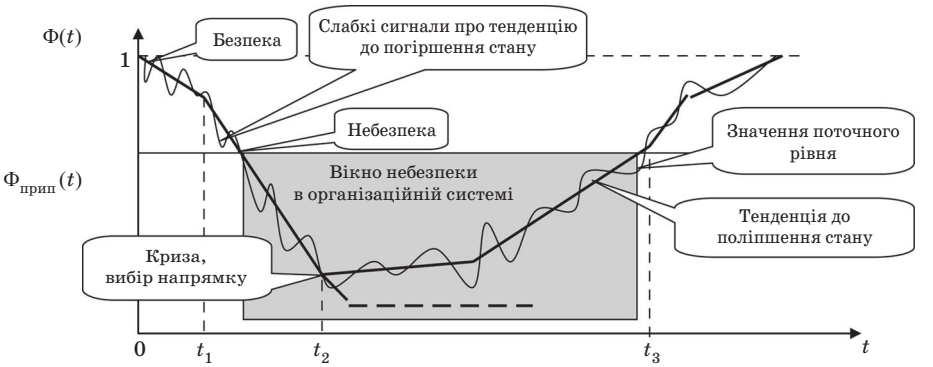


Рис. 2. Рівень безпеки $\Phi(t)$

Зазначимо, що рис. 2 ілюструє основні фази критичного стану. Вважається, що вікно небезпеки виникає випадково та існує протягом непередбачуваного часу. Адже за цей час неодмінно відбуваються такі події: стають відомими загрози та їх дія; знаходяться засоби їх нейтралізації або усунення; ці засоби мають бути встановлено в ОСКІ для її захисту. Також бачимо, що в моменти t_1 і t_3 нас цікавить стан системи, оцінювання якого здійснюється за обчисленим критерієм $\Phi_{прип}(t)$.

Цей критерій фактично визначає готовність до виконання завдань структурними елементами ОСКІ, а в критичний момент t_2 нас буде цікавити, як вийти з критичного стану, а це, по суті, інший за змістом показник, що встановлює якість керованості під час переходу. Звідси пропонується загальним показником вважати

$$\Phi_б(t) = \begin{cases} G(t), \text{ якщо } \Phi_б(t) \geq \Phi_{прип}, \\ \Phi(t), \text{ якщо } \Phi_б(t) < \Phi_{прип}. \end{cases} \tag{2}$$

Тут $G(t)$ — готовність до використання ОСКІ в поточному режимі функціонування (або експлуатації) для виконання відомого переліку завдань; $\Phi(t)$ — показник, що характеризує адаптацію ОСКІ до виконання нових завдань; $\Phi_{прип}(t)$ — припустиме значення, яке характеризує рівень безпеки ОСКІ.

Визначений зміст комплексного показника рівня безпеки $\Phi_б$ характеризує вплив загрози та ефективність заходів із реорганізації щодо її нейтралізації.

Висновки

♦ Вікна небезпеки і засоби їх виконання зловмисником в ОСКІ з'являються постійно; трактування проблеми безпеки ОСКІ для різних категорій суб'єктів і об'єктів може істотно різнитися; для кожної ОСКІ існує своя система забезпечення захисту; успіх стосовно організації безпеки ОСКІ може гарантувати тільки комплексний підхід, що поєднує різноманітні заходи, наприклад інформаційного, організаційного, процедурного характеру.

♦ В основу забезпечення безпеки будь-якої ОСКІ має бути покладено наукове обґрунтування таких положень: доктрини як сукупності концепцій; стратегії як сукупності способів досягнення цілей; концепції як компактної теорії, що застосовується для розробки політики безпеки, а також програм досягнення визначених цілей у системі забезпечення безпеки і профілів захисту складових ОСКІ. Тут виникає необхідність розгляду змісту реорганізації ОСКІ. Вирішення цього завдання передбачає визначення методології забезпечення реорганізації ОСКІ як логічної організації понять, показників, закономірностей, методів оцінювання рівня інформаційної безпеки і заходів із реорганізації, що мають вплив на рівень цієї безпеки. Практичним результатом є обґрунтування завдань, складу і принципів побудови системи забезпечення інформаційної безпеки держави (юридичної особи), яка знайде місце в доктринах, концепціях, політиках і програмах організації безпеки установ та організацій.

Список використаної літератури

1. ***Богданов, А.*** *Наука об общественном сознании: Краткий курс идеологической науки в вопросах и ответах / А. Богданов.— [3-е изд.].— Петроград, Москва: Книгоиздательское товарищество «Книга», 1923.— 314 с.*

2. ***Богданов, А. А.*** *Всеобщая организационная наука (Тектология) / А. А. Богданов: в 2-х кн.— М.: Книга, 1912; 2-е изд. 1925; переиздание 1989.— Книга 1.— 304 с. Книга 2.— 351 с.*

3. ***Месарович, М.*** *Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, И. Такахара; пер. с англ.— М.: Мир, 1970.— 340 с.*

4. ***Мильнер, Б. З.*** *Теория организаций / Б. З. Мильнер.— М.: ИНФРА-М, 1999.— 336 с.*

5. ***Иванова, Т. Ю.*** *Теория организации / Т. Ю. Иванова, В. И. Приходько и др.— СПб.: Питер, 2004.— 269 с.*

6. ***Месарович, М.*** *Основания общей теории систем / М. Месарович.— М.: Мир, 1966.— 244 с.*

7. ***Гиг, Дж. Ван.*** *Прикладная общая теория систем / Дж. Ван Гиг.— Кн. 1, 2.— М.: Мир, 1981.— 340 с.*

8. ***Боулдинг, К.*** *Общая теория систем — скелет науки / К. Боулдинг.— М.: Прогресс, 1969.— 224 с.*

9. ***Николос, Г.*** *Самоорганизация в неравновесных системах. От диссипативных структур к упорядоченности через флуктуации / Г. Николос, И. Пригожин.— М.: Мир, 1979.— 512 с.*

10. ***Хакен, Г.*** *Синергетика / Г. Хакен.— М.: Мир, 1980.— 404 с.*

11. ***Горский, Ю. М.*** *Основы гомеостатики (Гармония и дисгармония в живых, природных, социальных и искусственных системах) / Ю. М. Горский.— Иркутск: Изд-во ИГЭА, 1998.— 337 с.*

12. ***Саймон, Г.*** *Административное поведение / Г. Саймон, Дж. Марш; пер. с англ.— М.: Мир, 1974.— 245 с.*

13. ***Берталанфи, Л. фон.*** *Общая теория систем: критический обзор / Л. фон Берталанфи.— М.: Прогресс, 1969.— 382 с.*

14. ***Ансофф, И.*** *Стратегическое управление / И. Ансофф.— М.: Мир, 1980.— 340 с.*

15. ***Сетров, М. И.*** *Основы функциональной теории организации / М. И. Сетров.— Л.: Наука, 1972. — 187 с.*

16. ***Акофф, Р.*** *Планирование будущего корпорации / Р. Акофф; пер. с англ.— М.: Прогресс, 1985.— 230 с.*

17. ***Виханский, О. С.*** *Стратегическое управление / О. С. Виханский.— М.: Мир, 1986.— 230 с.*

18. ***Ансофф, И.*** *Стратегическое управление / И. Ансофф.— М.: Мир, 1980.— 340 с.*

19. ***Даник, Ю. Г.*** *Національна безпека: запобігання критичним ситуаціям: монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін.— Житомир: Рута, 2006.— 386 с.*

20. ***Лапин, Н. И.*** *Теория и практика социального планирования / Н. И. Лапин, Э. М. Коржева, Н. Ф. Наумова.— М.: Политиздат, 1975.— 245 с.*

Рецензент: доктор техн. наук, доцент **В. В. Онищенко,** Державний університет телекомунікацій, Київ.

В. В. Вишневский, Ю. И. Катков, С. А. Серых

РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ВОЗНИКНОВЕНИИ ЯВЛЕНИЯ КРИТИЧНОСТИ ОРГАНИЗАЦИОННОЙ СИСТЕМЫ

Рассмотрены общие положения об организационных системах с критической инфраструктурой. Исследован случай несоответствия инфраструктуры организационной системы в результате воздействия возможных вызовов или угроз, которые могут привести в критичное состояние любой важный элемент этой системы или других систем. Представлена математическая модель оценки уровня критичности организационной системы с критичной инфраструктурой.

Ключевые слова: организационные системы с критичной инфраструктурой; инфраструктура организационной системы; вызовы; угрозы; реорганизация.

V. V. Vyshnivskyi, Yu. I. Katkov, S. A. Serikh

ROLE AND LOCATION OF INFORMATION INFRASTRUCTURE IN THE EVE OF THE ORGANIZATIONAL SYSTEM CRITICALITY

This paper examines the general provisions of organizational systems with a critical infrastructure. Reasons for reorganization are shown. The direction of the study of the infrastructure of the organizational system is indicated after the impact of possible challenges or threats. A mathematical model for assessing the level of criticality of an organizational system with a critical infrastructure is provided.

Keywords: organizational systems with a critical infrastructure; infrastructure of the organizational system; challenges; threats; reorganization.

УДК 004.58
В. В. ОРТІКОВ;
Н. В. КОРШУН, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

БАЗОВІ ПРИНЦИПИ ТА ОСНОВНЕ ОБЛАДНАННЯ ДЛЯ ПЕРЕДАВАННЯ ДАНИХ ЗА ДОПОМОГОЮ СТРИМІНГУ В УКРАЇНІ

У статті розглянуто структуру побудови програмно-апаратної частини інтернет-стримінгу.
Ключові слова: інтернет-стримінг; жива трансляція; стримінгові сервіси; стрим-сервер; кодер; програма-плеєр; відеокодек; стандарт відеокомпресії; бітрейт; комп'ютер; якість інтернету; пристрій.

ВСТУП

У сучасному світі представники різноманітних професій та верств населення мають безліч відмінностей у сферах і засобах своєї діяльності, інтересах та шляхах їх задоволення, напрямках та меті докладання зусиль. Але всі вони мають спільні потреби, серед яких чи не найголовнішою є необхідність оперативного і точного отримання інформації.

Важливою складовою споживаної людством інформації є аудіовізуальні дані, або медіа-потік. При цьому збільшення щільності подій, обсягів і швидкості оновлення даних призводить до необхідності доступу широкого кола споживачів до найоперативнішої версії надання такої інформації: медіа-трансляції у режимі реального часу, або стримінгу. З урахуванням того, що найдоступнішим і найбільш гнучким каналом отримання даних є мережа Інтернет, має сенс передусім розглядати саме інтернет-стримінг.

Інтернет-стримінг широко використовується для оперативного й неупередженого висвітлення важливих подій; для трансляції музичних, спортивних та інших заходів; для бізнес- і наукових конференцій географічно віддалених учасників; для дистанційної освіти; для ведення військової розвідки; для приватного спілкування і ще для безлічі інших завдань, без яких важко уявити сучасне життя.

Передавання даних загалом та інтернет-стримінг зокрема належать до сегменту, який вкрай швидко розвивається та змінюється, тому дуже актуальним було б створення докладного огляду та систематизації наявних технологій і обладнання в цій галузі, а також окреслення можливих перспектив їх подальшої еволюції.

ОСНОВНА ЧАСТИНА

Для позначення терміна «інтернет-стримінг» сьогодні також використовуються такі терміни-синоніми:

- жива трансляція;
- потокове відео;
- лінійне мовлення;
- пряма трансляція в інтернеті;
- трансляція в реальному режимі часу;
- передавання потокового мультимедійного контенту;
- онлайн трансляція [1].

Поєднання ціни, якості та здатності адаптуватися до майже будь-яких умов робить інтернет-стримінг привабливим та доступним каналом поширення оперативної інформації. Немає потреби у професійній апаратурі та навіть не обов'язково бути медіа-професіоналом: стримером може стати будь-хто. Усе, що для цього потрібно — наявність Wi-Fi модуля, інтернету та будь-якого пристрою для зйомки (окрема камера або смартфон/планшет). Нині існує багато недорогих планшетів. Більш того, якщо у стримера немає модема, часто в місцях зйомки (наприклад, на прес-конференціях) є зона Wi-Fi.

Картинка з місця події — це завжди краще, ніж просто коментар журналіста. Необхідно усвідомити, що масовий глядач вже сформував попит на прямі ефіри, люди бажають бачити те, що відбувається саме зараз. Вони не хочуть чекати 2-3 години, поки сайти зроблять з події новину, або чекати на телевізійні випуски новин. Адже поки що невідомо, які канали там були і чиї новини дивитися. А так глядач може переглянути потокову трансляцію і відчути, що він сам перебуває на місці події.

Структуру побудови програмно-апаратної частини інтернет-стримінгу наведено на рисунку.

Структура побудови програмно-апаратної частини інтернет-стримінгу

Джерела потоку

Джерелами живої потокової трансляції, як правило, виступають відеокамери (професійні чи екшн-класу), або обладнані вбудованою відеокамерою мобільні пристрої (різні типи планшетів, смартфонів). На прикладі трансляції з камери: щоб організувати відправлення зображення, необхідно передусім захопити і кодувати відеосигнал програмою-кодером.

Кодер відправляє підготовлений потік на медійний сервер, який обслуговує процес трансляції стриму кінцевим користувачам.

За відсутності окремої екшн-камери основним пристроєм для проведення стрим-трансляції може стати смартфон або планшет із камерою та можливістю підімкнення до мережі Інтернет.

Досвід останніх років показує, що під час потокової трансляції доступ джерела з місця подій до мережі може обмежуватися через нестабільне або переривчасте з'єднання. У цьому разі може допомогти 4G-роутер (Yota).

Для того щоб транслювати відеосигнал через канали стільникового зв'язку (CDMA, LTE, 3G і 4G) або інші канали, такі як Wi-Fi, WiMax чи радіохвилі, необхідно додаткове обладнання, вартість якого часто велика.

Інфраструктура

Комбінація комп'ютерного обладнання і спеціального програмного забезпечення, яка використовується для обробки отриманого з початкової точки потоку медіа-трансляції та подальшого передавання відео- та аудіоданих зацікавленій аудиторії, називається стрим-сервером. Таке застосування апаратури і програмних додатків технічно є сервісом, але в галузях, пов'язаних з інтернетом, вже склалася інша традиція. Тому це програмне забезпечення можна називати сервером стримінгового передавання. Отже, функція стрим-сервера — приймати відеопотік від джерела і переспрямовувати його кінцевим отримувачам.

Альтернативою власному медіа-серверу є використання для потокових трансляцій існуючих стримінгових сервісів — тепер їх багато. Деякі з них платні, інші надають свої послуги за можливість розміщення в трансляції реклами. Серед найпомітніших на ринку варто відзначити: You Tube Live Events, Ustream, Bambuser, Twitch.tv, Periscope, UTrailMe, Smashcast.tv, Cybergame.tv.

Отримувачі трансляції

Віддалені користувачі під'єднуються до медіасервера і запитують трансляцію для перегляду. Кінцеві користувачі, залежно від ситуації, можуть отримувати потокове відео на різні пристрої:

- комп'ютер (стаціонарний або ноутбук);
- мобільний пристрій (планшет, смартфон тощо);
- телевізор із доступом до інтернету.

Телевізор із доступом до інтернету має все необхідне для роботи за замовчуванням, але у разі використання комп'ютера або планшета/смартфона користувачеві можуть знадобитися додаткові програмні інструменти (так звані відеоплеєри). Приклади популярних безкоштовних відеоплеєрів:

- **VLC Media Player** (гнучкий та легко адаптований плеєр, що підтримує переважну більшість форматів);
- **Kodi** (інструмент, що дозволяє як перегляд медіа-потоків, так і їх зберігання або подальшу ретрансляцію);
- **Media Monkey** (плеєр із потужною системою каталогізації та достатніми можливостями подальшої трансляції).

Під час онлайн трансляції вихідні медіа-дані зазнають перекодування: спочатку для зменшення обсягу (для оптимізації швидкості передавання), а потім (у кінцевого користувача) — для відновлення заданої якості програвання потоку. Програмне забезпечення для такої обробки даних називається кодеками.

Найбільш популярними стандартами відеокодеків (кодувальників відеопотоку) є **H.264**, **VP6**, **WMV**, **WebM**.

Для кодування аудіоданих здебільшого використовуються **AAC**, **MP3**, **Vorbis** [1].

Основним кодеком сучасного потокового відеомовлення є **H.264/MPEG-4 AVC** — міжнародний стандарт відеокомпресії. Стандарт H.264/AVC/MPEG-4 Part 10 забезпечує низку можливостей, що дозволяють значно підвищити ефективність стиснення відео порівняно з попередніми стандартами, гарантуючи більшу гнучкість застосування в різноманітних мережних середовищах та уможливлюючи:

- багатокадрове прогнозування (використання стиснених раніше кадрів як опорних — тобто із запозиченням частини матеріалу з них — куди більш гнучко, ніж у попередніх стандартах);
- просторове передбачення від країв сусідніх блоків для опорних кадрів;
- стиснення макроблоків без втрат;
- нові функції перетворення;
- спрощення розподілу бітрейту кодером;
- внутрішній фільтр деблокінгу в циклі кодування, що усуває артефакти блоковості;
- функції стійкості до помилок [2].

Високоякісний стримінг передбачає наявність ***високоякісного інтернету***. Якість інтернету — це його стабільність та швидкість. Наприклад, стандартний тест на швидкість інтернету Speedtest може показувати дуже хороші результати, але насправді, стрим буде переривчастим. Speedtest

демонструє максимальну швидкість, яку можна отримати з поточного підімкнення. Але він зовсім не означає, що така максимальна швидкість буде завжди. Трапляються стрибки, і якщо зазвичай стрибок швидкості з 20 до 10 Мбіт/с не відчувається, то за умов трансляції це відразу ж дасть гальмування стриму.

Для передавання даних за допомогою стримінгу важлива Upload швидкість, а не Download. Тобто швидкість віддачі, а не завантаження. Адже під час трансляції ми саме завантажуємо в мережу дані, а не скачуємо їх. Upload швидкість завжди нижча, ніж швидкість завантаження. Іноді це може бути всього кілька мегабіт, а іноді розбіжність може досягати кількох разів. У всіх провайдерів це відбувається по-різному.

Однак лише виміряти швидкість віддачі за допомогою стандартного теста не означає визначити показник якості. Але тест на швидкість може показати максимальну швидкість, і якщо ми поділимо це значення на 2 чи 3, то в більшості випадків отримаємо гарантовану стабільну швидкість віддачі.

Наприклад, якщо Speedtest показав Upload швидкість у межах 50 Мбіт/с, то ділимо це значення приблизно на 2,5 і дістаємо 20 Мбіт/с. Такий показник цілком відповідає умовам стабільного стриму з високою якістю (таблиця).

Орієнтовні показники мінімальної та прийнятної швидкості для стримінгу

Роздільна здатність відео	Мінімально припустима швидкість	Прийнятна швидкість
480p (стандартна якість, SD)	2 Мбіт/с	5 Мбіт/с та більше
720p (середня якість, low HD)	4 Мбіт/с	10 Мбіт/с та більше
1080p (висока якість, true HD)	6 Мбіт/с	20 Мбіт/с та більше

Мінімально припустима швидкість завантаження залежить від якості кадру (наприклад, 720p), обраного стрим-сервісу і спрямування медіа-потоку (наприклад, прямо в мережу або кілька потоків зі змінними швидкостями передавання даних через відеокодер). У будь-якому разі в наших умовах не рекомендовано намагатися проводити стримінг, якщо бітова швидкість менш ніж 5 Мбіт, незалежно від якості кадру [4].

ВИСНОВКИ

На сучасному етапі розвитку інформаційно-комунікаційних технологій стримінг упевнено ввійшов у ритм нашого життя. Адже завдяки йому можна передавати будь-яку подію у світі в режимі реального часу. Наприклад, прямі трансляції футбольних матчів, трансляції виступів під час конференцій, трансляція власного ТВ каналу, відеоконтенту і т. ін.

До основних компонентів інтернет-стримінгу входять джерела потоку (камера, смартфон або планшет); стрим-сервер (комп'ютер зі встановленим програмним додатком), який обслуговує потокову трансляцію на її шляху від джерела до кінцевого споживача; отримувачі трансляції (комп'ютер, мобільний пристрій, телевізор).

Для високоякісного передавання стримінгу потрібен високоякісний інтернет. Оскільки стримінг може проводитись із різних куточків планети, то основним джерелом відеопотоку виступають, як правило, смартфони або планшети. Досі технології мобільного зв'язку, які надають доступ до мережі Інтернет, ще не дійшли до такого рівня, аби забезпечити надшвидкий мобільний інтернет в будь-якій точці світу без використання додаткового підсилювального обладнання, котре, у свою чергу, багато коштує. Тому подальші розвідки технології стримінгу пов'язуються насамперед із розширенням покриття високошвидкісного мобільного інтернету по всій території України.

Список використаної літератури

*1. **Трофанюк, В.** Стриминг. Технологии на страже правды [Електронний ресурс] / В. Трофанюк.— URL:*

http://broadcast.net.ua/show/Infrastruktura/3975-striming_tehnologii_na_strazhe_pravdy_26.03.2014

*2. **Архипцев, С. В.** Сравнительный анализ методов видеокодирования стандартов ITU-T H.264-AVC [Електронний ресурс] / MPEG-4 Part-10 и H.265 HEVC / С. В. Архипцев, Д. П. Лукьянов.— URL:*

https://cyberleninka.ru/article/n/sravnitelnyy-analiz-metodov-videokodirovaniya-standartov-itu-t-h-264-avc-mpeg-4-part-10-i-h-265-hevc.

*3. **Что** такое скорость интернета и как ее проверить онлайн [Електронний ресурс].— URL:*

http://www.prostoweb.com.ua/internet_marketing/internet_dlya_chaynikov/stati/chto_takoe_skorost_interneta_i_kak_ee_proverit_onlayn

*4. **What** broadband speed do I need for streaming, vlogging, VoIP, the cloud and other online applications [Електронний ресурс] / L. Thompson.— URL:*

https://www.cable.co.uk/guides/what-broadband-speed-do-i-need-for-skype/

Рецензент: доктор техн. наук, ст. наук. співробітник **М. М. Степанов**, Державний університет телекомунікацій, Київ.

В. В. Ортиков, Н. В. Коршун

БАЗОВЫЕ ПРИНЦИПЫ И ОСНОВНОЕ ОБОРУДОВАНИЕ ДЛЯ ПЕРЕДАЧИ ДАННЫХ С ПОМОЩЬЮ СТРИМИНГА В УКРАИНЕ

В статье рассмотрена структура построения программно-аппаратной части интернет-стриминга.

Ключевые слова: интернет-стриминг; живая трансляция; стриминговые сервисы; кодер; программа-плеер; видеокодек; стандарт видеокомпрессии; битрейт; видеоконтент; качество интернета; устройство.

V. V. Ortikov, N. V. Korshun

BASIC PRINCIPLES AND MAIN EQUIPMENT FOR DATA TRANSFER WITH STRIMING IN UKRAINE

The structure of Internet streaming provision software / hardware complex is considered in the article.

Keywords: Internet streaming; live broadcast; streaming services; coder; player software; video codec; video compression standard; bit rate; video content; Internet connection quality; hardware.

ЗВ'ЯЗОК

Наукове видання

Редакційна обробка та коректура
О. П. Бондаренко, Т. В. Ількевич

Комп'ютерна верстка та дизайн
Г. С. Тимченко, О. Ю. Апухтіна

Відповідальний за випуск
І. І. Тищенко

Формат 60×84/8. Папір друкарський.
Гарнітура SchoolBookC, EuropeCond. Зам. 65
Наклад 300 прим.

Державний університет телекомунікацій
03110, м. Київ, вул. Солом'янська, 7
Тел. (044) 249-25-75
E-mail: *zviaz-ok@ukr.net*