МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

TP-LINK UKRAINE

TP-LINK®
The Reliable Choice

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 червня 2019 р.

м. Київ

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE
TP-LINK UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 4 – 6, 2019
Kyiv, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
TP-LINK UKRAINE

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 червня 2019 р.
м. Київ, Україна

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
НАЦИОНАЛЬНЫЙ АВИАЦИОННЫЙ УНИВЕРСИТЕТ
ГОСУДАРСТВЕННАЯ СЛУЖБА СПЕЦИАЛЬНОЙ СВЯЗИ
И ЗАЩИТЫ ИНФОРМАЦИИ УКРАИНЫ
TP-LINK UKRAINE

ТЕЗИСЫ

НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«ПРОБЛЕМЫ ЭКСПЛУАТАЦИИ И ЗАЩИТЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»

4 – 6 июня 2019 г.
г. Киев, Украина

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 4 – 6 червня 2019 р., Національний авіаційний університет. – К.: Вид-во ТОВ «Центр учбової літератури», 2019. – 70 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

УДК 621.39.005 (043.2)

В. В. Антонов, О. Є. Под'ячев
Національний авіаційний університет, м. Київ

ТРАНСПОРТНА МЕРЕЖА НА БАЗІ ОБЛАДНАННЯ SIEMENS ПЛАТФОРМИ SURPASS hiT 7070

Основне застосування SDH з моменту її появи – побудова транспортних мереж для передачі цифрових потоків. З розвитком комп'ютерних мереж, Інтернету, технологій передачі даних (FR, ATM і т.д.) інфраструктуру транспортних мереж на основі SDH все частіше застосовують для організації цифрових каналів мереж передачі даних (тобто будують накладені мережі поверх SDH). Недоліки використання «класичного» SDH для передачі даних найбільш гостро стали проявлятися при необхідності надання широкосмугових послуг зв'язку локальних мереж. Але є і більш вагомі обмеження, такі як:

- Мала варіація можливих швидкостей передачі даних, що значно обмежують можливості ефективного надання послуг.
- Обов'язкове перетворення інтерфейсів Ethernet до інтерфейів SDH.

Для подолання цих обмежень, SDH обладнання пішли по шляху створення систем SDH наступного покоління (Next Generation SDH, NG SDH). Устаткування NG SDH має інтегровані інтерфейси передачі даних (зокрема, Ethernet), а також використовує нові технології, які дозволяють більш ефективно виділяти необхідну смугу для служб даних і забезпечувати низьку вартість впровадження цих технологій у вже існуючі мережі, так як підтримка додаткової функціональності потрібно тільки на граничних вузлах мережі.

Системи SDH наступного покоління - багатофункціональні мультісервісниє платформи, що надають безліч послуг без дорожнечі і складності накладених мереж. В моєму проекті будуть розглянуті принципи побудови SDH транспортних мереж. Також будуть розглянуті питання щодо реконструкції та модернізації місцевого ділянки мережі регіонального оператора, що надає послуги телефонного зв'язку і послуг.

Чому саме Siemens SURPASS hiT 7070

Ця платформа дає можливість гнучкості пакетної комутації та передачу Ethernet, працюючи з надійністю, що властива SDH. Різні

мережеві елементи об'єднані і суміщені в єдиний компактний блок. Ефективність такого підходу, разом з широким використанням високо інтегрованих компонентів, дозволяє SURPASS hiT 70 series, домогтися більш низьких витрат у порівнянні з існуючими рішеннями.

Для постійно зростаючого середовища інформації з безліччю послуг необхідна єдина ефективна платформа, з хорошим масштабуванням, що має можливість для обробки пульсуючого пакетного трафіку плюс традиційний вузькосмуговий і широкосмуговий трафік. Як наступне покоління 10-гігабітних систем SDH, SURPASS hiT 7070, працює з TDM і матрицею пакетної комутації, що є ключовим фактором, що відрізняє його від існуючого обладнання SDHL.

УДК 621.39.005 (043.2)

В.С. Слюсаренко, Г.Ф. Конахович, Д.І.Бахтіяров,
Національний авіаційний університет, м. Київ

АНАЛІЗ МОДЕЛЕЙ РОЗПОВСЮДЖЕННЯ РАДІОХВИЛЬ В ПРИМІЩЕННЯХ ДЛЯ МОДЕЛЮВАННЯ КАНАЛУ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ

Не існує єдиної загальноприйнятої моделі обчислення поля в приміщенні. Рекомендації різних національних та міжнародних організацій суттєво не співпадають. Складність вибору моделі поширення радіосигналу та структури поля ускладнюється труднощами практичного визначення реальних параметрів моделі.

Зазвичай моделі для приміщень ділять на дві великі групи: емпіричні і детерміновані. Перші набули найбільшого поширення, зручні як для оцінок потужності сигналу в приміщенні, так і для прогнозування мінімальних і максимальних рівнів потужності при побудові систем зв'язку. Другі зазвичай використовують у вигляді пакетів прикладних програм для вивчення параметрів залежних від часу.

Для сучасних систем першочергово стоїть завдання дослідження загасання сигналу одночасно ззовні і всередині приміщень.

Наприклад, пристрій прослуховування знаходиться ззовні, а закладний пристрій - всередині приміщення. При моделюванні слід враховувати додаткові втрати сигналу через перехід сигналу ззовні всередину приміщення і навпаки.

В якості моделі для опису загасання сигналу між приміщенням і відкритим простором (поза-всередині приміщень) варто розглянути (рис.1.) відомий підхід. Зі змінами цю модель в якості однієї із складових можна використати в моделюванні каналу загроз за рахунок побічних електромагнітних випромінювань та наведень.

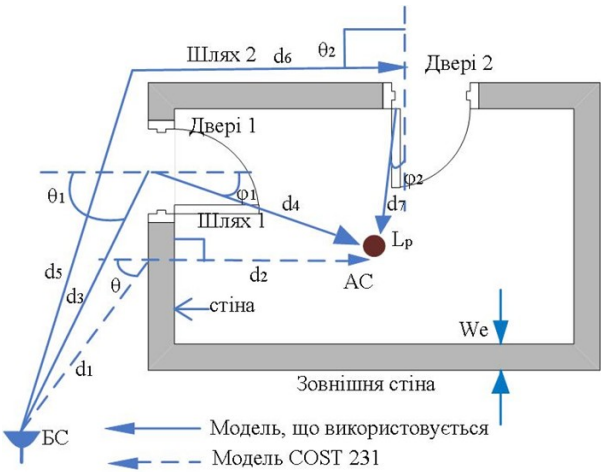


Рис. 1. Геометрична модель поширення сигналів між приміщенням і відкритим простором

Після проведення детального аналізу даних моделей було визначено, що моделі Хата і COST 231 Multi-Wall Model є найбільш універсальними і можуть бути використані для опису моделі загроз.

Оскільки зловмисник може знаходитись в приміщенні, а також ззовні, для визначення модел загроз слід створити наступні сценарії розповсюдження електромагнітних хвиль:

- зовнішньо – зовнішній;
- внутрішньо – зовнішній;
- внутрішньо – внутрішній.

При визначенні втрат сигналу у підлозі і стінах використовують фіксоване значення для всього діапазону частот. Втрати між суміжними поверхами є фіксованим, а втрати у стіні Lωі залежать від типу стіни, а не від частоти.

Але було встановлено, що значення сильно залежать від частоти, тому було вирішено створити методику модернізації моделі для обчислення вищенаведених параметрів.

УДК 621.39.005 (043.2)
Введите текст
В.С. Слюсаренко, Г.Ф. Конахович, Д.І.Бахтіяров,
Національний авіаційний університет, м. Київ

ВИЗНАЧЕННЯ КОНТРОЛЬОВАНОЇ ЗОНИ КАНАЛУ ВИТОКУ ЗА РАХУНОК ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ

Широке використання комп'ютерних технологій в системах обробки даних привело до загострення проблеми захисту інформації від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд специфічних особливостей, пов'язаних з тим, що інформація не жорстко пов'язана з носієм, і може бути скопійована і передана по каналах зв'язку.

Технічні засоби обробки інформації, які в процесі роботи здійснюють її обробку, зберігання і передачу, генерують електромагнітні випромінювання, які є побічними, тобто паразитними. Таким чином, в результаті нелінійних процесів в блоках технічного обладнання генеруються і випромінюються в навколишній простір побічні електромагнітні випромінювання і наведення (ПЕМВН), рівень яких може бути достатнім для прийому радіосигналу на певній відстані від технічних засобів. Отже, актуальним стає питання визначення оптимальної моделі опису загроз через канал витоку ПЕМВН, а також розмір контрольованої зони, в межах якої контролюються наявність сторонніх осіб і несанкціоноване перебування в об'єкті, і можливість використання розвідувального обладнання, тому що в цій зоні існує ймовірність перехоплення інформації.

Контрольовану зону було побудовано для наступного приміщення. Корпус п’ятиповерховий, блочно-панельний, висота кожного поверху з урахуванням міжповерхових перекриттів – 4 м.

В якості джерела випромінювання використовуємо закладний пристрій радіомікрофон з підвищеною чутливістю МР2, а в якості приладу виявлення радіовипромінювань використаємо АКОР-1. За отриманими результатами приведемо графічне зображення контрольованої зони.

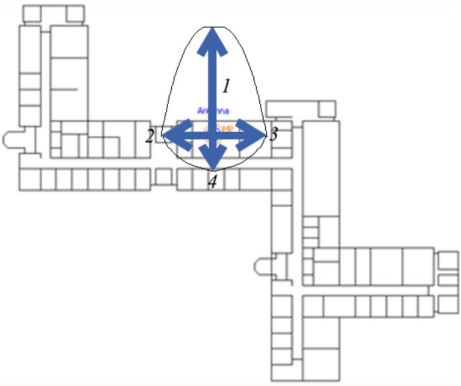


Рис.1. Контрольована зона за чотирма напрямами

Отже сигнал може бути зафіксований у межах:

- •перший напрямок – 24м;
- •другий напрямок – 10м;
- •третій напрямок – 10м;
- •четвертий напрямок – 8,5м .

Також було вирішено розробити власне програмне забезпечення, яке, по-перше, враховує модернізовану модель Хата і COST-231 MWM, а також працює за різними сценаріями розповсюдження – внутрішньо-внутрішній, внутрішньо-зовнішній.

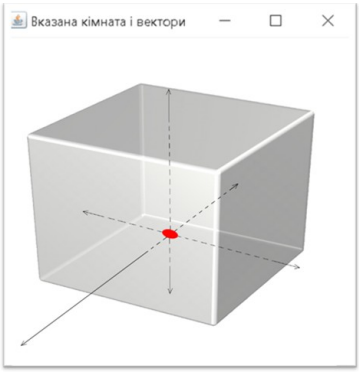


Рис.2. Приклад виконання программи

УДК 654.153 (043.2)

А.М. Пачес
Національний авіаційний університет, м. Київ

СИСТЕМА ЛОКАЛІЗАЦІЇ АБОНЕНТА В СТІЛЬНИКОВІЙ МЕРЕЖІ

Визначення місцезнаходження завжди було необхідною умовою будь-якої діяльності людини, пов'язаної з потребою відстеження рухомих об'єктів. З цього і виникла наука «навігація» і з'явилися різні навігаційні прилади та засоби.

Стаціонарна мережа оператора розділяється на систему комутації і систему базових станцій. Система комутації забезпечує встановлення з'єднання між абонентами. До складу цієї системи входять: центр MSC, шлюз GMSC, регістри HLR, VLR, EIR, центр AuC. Система базових станцій забезпечує зв'язок між центром комутації і мобільними станціями. До складу цієї системи входять контролери BSC і базові BTS. Систему комутації та контролери встановлюють в технічному центрі оператора. Базові станції, які розміщуються на великій території зв'язуються з контролерами через транспортну мережу.

Системи супутникового позиціонування засновані на розташуванні штучних супутників, які обертаються по визначених орбітах і безперервно передають сигнали, що використовуються мобільними терміналами задля виконання дальнометрії.

За своєю суттю це навігаційні системи, в той час як останні наземні системи призначені в основному для позиціонування. Система глобального позиціонування (GPS) в даний час в більшій мірі є глобальною навігаційною супутниковою системою (GNSS).

Наземні системи позиціонування використовують мережу наземних станцій. У минулому використовувалися кілька наземних систем для морської і авіаційної навігації: Decca, LORAN-C, TACAN і VOR / DME і безліч інших. Вони характеризуються дуже спеціалізованими областями застосування і високою вартістю установки і обслуговування. В довгостроковій перспективі деякі з них будуть замінені GNSS.

З іншого боку, сучасні наземні системи визначення місце розташування народилися як свого роду побічний продукт існуючих

бездротових систем зв'язку. Однією з основних відмінностей між сучасними супутниковими і наземними системами позиціонування є основна мета, для якої призначений сигнал, що йде від передавача до приймача: в супутниковій системі метою є дійсно позиціонування, тоді як в наземних системах позиціонування часто є допоміжної опцією по відношенню до передачі даних.

Через розмаїття наземних бездротових систем і методів модуляції до теперішнього часу були запропоновані різні підходи для можливості позиціонування в особистих телефонах і портативних пристроях. До них відносяться термінал-центровані і мережо-центровані процедури для стільникових мереж, для яких перші пропозиції вивчалися більше п'ятнадцяти років тому - процедури, спрямовані на модуляцію і протоколи для бездротових локальних мереж (WLAN), бездротові мережі великих міст (WMAN) і WSN.

GPS - це система глобального позиціонування, за допомогою якої можна точно визначати тривимірні координати об'єкта, оснащеного GPS приймачем: широту, довготу, висоту над рівнем моря, а також його швидкість, напрямок руху і поточний час.

Допоміжний GPS або розширений GPS (скорочено, як зазвичай A-GPS і рідше як a-GPS) - це система, яка часто значно покращує продуктивність запуску, тобто час до першого виправлення (TTFF), системи супутникового позиціонування GPS, A-GPS широко використовується в стільникових телефонах з підтримкою GPS, оскільки його розвиток було прискорене вимогою Федеральної комісії США по зв'язку США 911, щоб зробити дані про місцезнаходження стільникового телефону доступними для диспетчерів екстрених викликів.

Високочутливий GPS - це суміжна технологія, яка вирішує деякі з цих проблем, не вимагаючи додаткової інфраструктури. Однак, на відміну від деяких форм A-GPS, високочутливий GPS не може забезпечити миттєве виправлення, коли приймач GPS відключений протягом деякого часу.

Автономний GPS забезпечує першу позицію приблизно через 30-40 секунд. Він потребує орбітальної інформації супутників для розрахунку поточного становища. Швидкість передачі супутникового сигналу становить всього 50 біт / с, тому завантаження орбітальної інформації, такої як ефемерида і альманах, безпосередньо із супутників зазвичай займає багато часу, і якщо супутникові сигнали

губляться під час отримання цієї інформації, вона відкидається і автономна система повинна починатися з нуля .

УДК 621.391 (043.2)

В.В. Пунейко
Національний авіаційний університет, м. Київ

КОМП'ЮТЕРНІ МЕРЕЖІ У НАВЧАЛЬНОМУ ПРОЦЕСІ

На сьогоднішній день вже мало хто може уявити своє життя без бездротових технологій незалежно від сфери занять. Комп'ютери відіграють велику роль в навчальному процесі, так як з їх допомогою як вчителі, так і студенти здатні заощадити купу часу та ресурсів. Це лише одна з головних переваг бездротових технологій.

Зручність прокладання бездротових мереж не може не бути оціненою, адже сам процес не потребує багато часу, який був би змарнований на прокладання дротів до робочих місць та налаштування роботи при дротовому підключенні. Заощадження коштів та облаштування мережі бездротового зв`язку також вважається чималою перевагою. Звісно, сама бездротова структура може бути дорогою, ле це компенсується безпосередньо легкістю наштування та довготривалістю роботи.

У роботі розглянуто проблеми та способи їх вирішення наряду з аналізом зручності використання бездротових мереж у навчальних процесах. Сучасні стандарти безпровідних структур, а також їх топології було розглянуто у роботі задля їх потенційного використання.

Слід зауважити, що бездротові мережі мають свої недоліки. Основним з них є проблема безпеки бездротової мережі, а саме спрощений доступ до неї (порівняно з традиційними кабельними мережами типу Ethernet). Щоб включити Wi-Fi, потрібно просто знаходитися в межах сигналу, коли при дротовому підключенні необхідно отримати доступ до будівлі – фізичне підключення до внутрішньої мережі.

Майже всі корпоративні мережі захищають свої системи та конфіденційні дані, намагаючись заборонити зовнішній доступ. Якщо мережа не використовує шифрування, то включення технології бездротового підключення може знизити безпеку. Основним засобом запобігання доступу несанкціонованих користувачів є приховування імені точки доступу через відключення широкомовної передачі SSID.

Незважаючи на те, що таким чином досягається ефективність проти випадкового користувача, в будь-якому разі це є ненадійним методом забезпечення безпеки хоча б тому, що SSID передається у

чистому вигляді як відповідь для запиту клієнта. Ще одним способом є дозвіл підключатися до бездротової мережі Wi-Fi тільки ком`ютерам з відомими MAC-адресами. Тим не менш, в цьому випадку також присутня неабияка вразливість. Певні підслуховуючі пристрої можуть приєднатися до мережі, підмінивши авторизовану адресу. Шифрування Wired Equivalent Privacy (WEP) було розроблено для захисту від випадкового відстеження, але воно більше не вважається безпечним.

Бездротові точки доступу часто стають проблемною складовою роботи адміністраторів корпоративних мереж, адже не всі користувачі можуть запам`ятати паролі від точок. Тому аутентифікація клієнта займає певний час. Основні налаштування проводяться на сервері. На точці (клієнта) треба всього лише вибрати вид аутентифікації, порт сервера, IP адресу та пароль.

Для розподілу користувачів по групам використовуємо процес аутентифікації. Залежно від групи, повинні бути визначені права користувачів мережі задля розробки та подальшого аналізу процесу аутентифікації користувачв у мережі. Слід планувати групи з обмеженим доступом, аби інформація, що доступна в системі, правильно розподілялась між ними.

Розбираючи дану тему, слід визначити 3 типи користувачів: адміністратори, викладачі та студенти. Адміністратори отримують повний доступ до всієї мережі,управління роботою мережі та можливість вносити зміни у її функціонування. У свою чергу, викладачі здатні створювати, завантажувати, видаляти файли. Можливість перевіряти підвантажені роботи студентів стає одним з ключових моментів роботи. Як вже зрозуміло, студенти можуть завантажувати та передавати різн роботи, файли.

Таким чином, можна стверджувати, що робота є комплексною, адже в ній наявні дослідження проблем налаштування бездротової мережі зі сторін різних груп користувачів. У подальшому створена система оптимізуватиме навчальному процес, зменшуючи витрачений час на збір та обробку даних.

Дана мережа забезпечує доступ до сервера, де зберігаються інформація, дає можливість обмінюватися даними між користувачами. Цю мережу можна широко використовувати в навчальному процесі (для заліків та лабораторних робіт, зокрема).

УДК 621.39.005 (043.2)

Ж.М. Дараган
Національний авіаційний університет, м. Київ

УДОСКОНАЛЕННЯ МЕТОДИКИ ПРОГНОЗУВАННЯ ВТРАТ РАДІОСИГНАЛУ У ГІДРОМЕТЕОРАХ ДЛЯ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

Сьогодення постійно вимагає удосконалення мобільного зв'язку. Ось чому активно починає впроваджуватись технологія 5G.

За рахунок зміни планетарного клімату необхідно підлаштувати цю систему під вплив гідрометеорів,які в свою чергу є значною перешкодою для високочастотного 5G сигналу. Особливістю сучасних систем 5G є високі частоти (близько 27 ГГц) та направленість зв'язку. Погодні умови,на приклад дощі, мають великий вплив на затухання сигналу,що призводить до розсіювання. Чим більша частота тим більший вплив дощу,саме тому розрахунок втрат у гідрометеорах тісно пов'язаний з 5G .

Отже, виведення формули для прогнозування втрат у сучасному мобільному зв'язку є корисною для збереження часу інженерів у галузі телекомунікацій та науковців.

Зміст моєї роботи полягає в тому,щоб перенести графіки і номограми у аналітичний вигляд. Отже,основною задачею є виведення формули ,яка з мінімальною похибкою описувала б графік залежності коефіцієнту просторової нерівномірності дощу від протяжності інтервалу радіолінії і інтенсивності осадів. Для цього потрібно знайти коефіцієнти A,B,C,які допоможуть нам мінімізувати відхилення від значень, знайденими за графіком вручну.

$$K = K(J, R)$$

(1.1)

$$K = \exp\left[-A \cdot J^{B} \cdot {R_0}^{C}\right] \qquad (1.2)$$

$$Dev(A, B, C) = \sum_{r=1}^{rows(K)} \sum_{c=1}^{cols(K)} ¿¿¿¿$$

(1.3)

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = Minimize(Dev, A, B, C)$$

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 1.490 \times 10^{-3} \\ 0.981 \\ 0.56 \end{pmatrix}$$

Виведена формула з підставленими коефіцієнтами:

$$K = \exp\left(-1.49 \cdot 10^{-3} \cdot J^{0.981} \cdot R^{0.556}\right)$$

В ході роботи було синтезовано аналітичний опис обчислення втрат у радіосигналі, який з мінімальною похибкою буде описувати графік залежності коефіцієнту просторової нерівномірності дощу від протяжності інтервалу радіолінії і інтенсивності осадів. Обчисливши відхилення при використанні формули,можна зробити висновок, що дана формула для вдосконалення методики прогнозування втрат радіосигналу у гідрометеорах працює з мінімальними похибками і дозволяє подальше її використання в практичній та науковій діяльності.

УДК 004.733

А. С. Дегтяр
Національний авіаційний університет, м. Київ

МЕРЕЖА NGN НА БАЗІ ПЛАТФОРМИ U-SYS

За останній час на ринку телекомунікацій з'явилася інтенсивна конкуренція в порівнянні з попередніми десятиліттями і, як очікується, буде рости безперервно і швидко. Одною з основних проблем, що пов'язані з практичним впровадженням мереж наступного покоління NGN, є забезпечення наскрізної якості послуг QoS для мультимедійного трафіку. Сучасні методи проектування мереж NGN не дозволяють розрахувати основні характеристики мережі,а забезпечують лиш грубу оцінку продуктивності базових компонентів мережі.

Основними компонентами будь-якої мережі NGN є наступні функціональні об'єкти: медіашлюз MG (Media Gateway), сигнальні шлюзи SG (Signaling Gateway) та гнучкі комутатори (сервери викликів) CS (Call Server). Фізично медіашлюз та сигнальний шлюз можуть бути реалізовані в якості окремого обладнання та являють собою відповідно пункти концентрації сигнального та призначеного для користувача навантаження.

Сервер викликів зазвичай реалізується централізовано та використовується в основному для обробки групового сигнального трафіку. Взаємодія цих об'єктів мережі здійснюється за допомогою протоколів сигналізації через транспортну мережу. Параметри медіашлюз повинні розраховуватися,виходячи з пропущеного ним користувацького навантаження, а параметри серверу викликів – з навантаження обслуговуваних ним викликів та відповідного сигнального навантаження,пов'язаного з обробкою викликів. Параметри сигнального шлюзу повинні розраховуватися, виходячи з об'єму оброблюваного ними сигнального трафіку. Спочатку буде розглянута модель трафіку в мережі наступного покоління NGN,а потім – розрахунок параметрів мережевих елементів та вартості обслуговування мережі (витрати на обладнання і т.д.).

Ключовим параметром для розрахунку характеристик мережі NGN є навантаження (трафік) в мережі. Пропонується наступна модель розподілення трафіку в медіашлюзі: поступивший A_{ori} , обслужений A_{ter} , вихідний A_{out}, вхідний A_{in}, внутрішній A_{intra} та транзитний A_{tr}. Можна припустити, що вхідний трафік A_{ori} , доля внутрішнього трафіку P_{intra} та доля транзитного трафіку P_{tr} відомі,і вхідний трафік A_{ter} дорівнює по величині вихідному A_{ori} на стороні доступу медіашлюзу. Для визначення цих величин необхідно знати кількісний та якісний склад клієнтської бази кожного

медіашлюзу, розподілення користувачів по вузлам доступу та топологію зв'язку мережевих вузлів.

Таким чином, розгортання мережі NGN є достатньо вигідним економічно. Абоненту не потрібно буде подавати заявки на підключення до декількох компаній – він може замовити цілий пакет послуг, до яких буде мати однаковий доступ та гідну якість обслуговування – як в телефонії, так й Інтернет-послугах – як домашньому, так і мобільному.

УДК 621.391.7 (043.2)

Г.Д. Максимова
Національний авіаційний університет, м. Київ

СІЛЬСЬКА ТЕЛЕФОННА МЕРЕЖА

Розвиток мереж зв`язку на сучасному етапі є пріоритетним завданням усього світового співтовариства. На сьогоднішній день зв`язок відіграє першорядну роль у всіх сферах людської діяльності: в економіці й промисловості, науці й техніці, культурі, державному керівництві.

Розвиток електрозв`язку в нашій країні йде з деяким відставанням від розвинених закордонних країн. На сьогоднішній день телефонна щільність України нижче, ніж у розвинених закордонних країнах. Вітчизняні телефонні мережі складаються в основному з аналогових АТС: декадно-крокових, координатних, квазіелектронних. Дані типи АТС вже не відповідають сучасним стандартам і не можуть забезпечити абонентів сучасними видами послуг: ДВО, Internet, ISDN.

Для задоволення сучасних вимог в області електрозв`язку й повноцінного входження у світове телекомунікаційне співтовариство необхідних перехід до цифрової комутації. Значним кроком у розвитку телекомунікацій стала побудова цифрових систем комутації. На мережах нашої країни впроваджено досить багато типів ЦСК переважно зарубіжної розробки. Цифрова система комутації (ЦСК) середньої ємності «SI2000», розроблена словенською фірмою ISKRA-TEL, виробляється в кількох країнах, у тому числі в Україні спільним підприємством «Моніс» м.Харків.

ЦСК SI2000 має гнучку модельну архітектуру обладнання і програмного забезпечення (ПЗ), територіально розподілені абонентський доступ, комутацію і керування, централізовані експлуатацію і технічне обслуговування, інтегровану систему електроживлення, є економічною, добре пристосованою до обслуговування територій з малою щільністю населення і невибагливою до умов використання на мережі та до умов довкілля. (ЦСК) «SI2000» має широкі можливості використання на існуючих і перспективних місцевих мережах зв`язку, перш за все – телефонних мережах сільських адміністративних районів.

ЦСК SI2000 має обов`язкові функціональні підсистеми різного призначення, реалізовані апаратно-програмними засобами:

підсистема абонентського доступу; підсистема комутації; підсистема сигналізації; підсистема керування; підсистема лінійного доступу; підсистема технічної експлуатації; підсистема електроживлення; підсистема синхронізації.

На даному етапі цифровізації мережі передбачені заміни застарілих кінцевих телефонних станцій типу АТСК 50/200 на нове цифрове обладнання цифрової системи комутації (ЦСК) SI2000/V.5, встановлення обладнання широкосмугового доступу до мережі Internet (BAN), об`єднання деяких сільських АТС в кільця. При реконструкції ТМ САР мною було заплановане об`єднання деяких сільських телефонних станцій в вузлові райони. Також кроком до підвищення живучості та ефективності ТМ стало створення резервних напрямків з`єднувальних ліній за допомогою об`єднання сусідніх сільських АТС в транзитне кільце, заміна малоканальних систем ущільнення на нові цифрові системи передачі типу WATSON-5.

В ході виконання роботи мною були проведені розрахунки навантаження станцій мережі та кількості з`єднувальних ліній, що дозволяють провести остаточний перехід сільської мережі на цифрову основу. Дані результати можуть бути використані на практиці, тобто бути застосованими при побудові реальної цифрової телефонної мережі Миронівського району Київської області.

УДК 004.733

І.М. Барилюк
Національний авіаційний університет, м. Київ

КОНВЕРГЕНЦІЯ МІСЬКОЇ ТЕЛЕФОННОЇ МЕРЕЖІ

Мережа зв'язку наступного покоління (NGN) - концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями щодо їх управління, персоналізації та створенню нових послуг за рахунок уніфікації мережевих рішень, що передбачає реалізацію універсальної транспортної мережі розподілену комутацією, винесення функцій надання послуг кінцевим мережам вузлів та інтеграцію з традиційними мережами зв'язку.

Основними компонентами будь-якої мережі NGN є такі функціональні об’єкти,як : медіашлюз MG (Media Gateway),сигнальні шлюзи SG (Signaling Gateway),та гнучкі комутатори (сервери викликів) CS (Call Server).

При побудові NGN слід враховувати ряд специфічних властивостей системи телефонного зв'язку. Серед змін в ТМЗК необхідно виділити перехід до пакетних технологій передачі і комутації, стимулюючих розробку нових принципів побудови мережі. Одне з найважливіших завдань, сприяюча формуванню і реалізації цих принципів, – розробка

методів розрахунку характеристик, які дозволяють аналізувати якість обслуговування трафіку в NGN в цілому, а також в її окремих фрагментах.

Розрахунок кількості абонентів кожної категорії виконується виходячи із заданого процентного співвідношення від ємності станції: абонентів квартирного сектора - 66%; народно-господарського сектора - 29%; таксофонів - 5%; аналогових модемів - 21% на абонентських лініях квартирного і народно-господарського сектора; факсимільних апаратів - 22% на абонентських лініях народно-господарського сектора.

Виникаюче місцеве навантаження розраховується за формулою:

$$A_{voz\_m} = \sum_{i=1}^{5} \alpha_i \cdot P_p \cdot (a_i \cdot N_i) + a_{ISDN} \cdot N_{ISDN} \text{ Ерл}$$

де: i - категорія джерела навантаження;

a_i - питоме навантаження від абонентів і-ої категорії;

N_i - кількість джерел і-ої категорії;

$\alpha_i = \int (T_i, P_p)$, визначається з НТП 112.2000;

T_i - тривалість розмови, визначається з НТП 112.2000 залежить від процентного відношення квартирного сектора;

Висновок:

Перспективна архітектура мереж наступного покоління (NGN) передбачає створення мультисервісної мережі з винесенням функціональності послуг в граничні вузли мережі, створення спеціальної підсистеми управління послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення обладнання постачальників послуг.

Особливістю послуг, що надаються на мультисервісної мережі, є їх незалежність від способу доступу, що припускає появу мереж доступу як самостійного класу мереж зв'язку. Такі мережі повинні забезпечувати доступ не тільки до ресурсів мультисервісної мережі, а й до ресурсів існуючих мереж зв'язку. Такий підхід дозволить здійснити гнучку політику при переході від однієї мережі зв'язку до іншого при наданні однотипних послуг.

УДК 621.39.005 (043.2)

О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

Проблематика забезпечення авіаційного супутникового зв'язку на трансконтинентальних маршрутах

Сучасні рейси повітряних суден ЦА з аеропорту «Бориспіль» здійснюються зокрема за далекомагістральними маршрутами, наприклад, рейс PS231 «Київ – Нью-Йорк» (JFK), FDB730 «Київ – Дубаї» (DXB), та інші рейси. При цьому стає неможливим безпосередній зв'язок ПС та наземних станцій в деяких маршрутних точках, наприклад над малозаселеними та океанічними районами.

В таких ситуаціях існує необхідність здійснення надійного зв'язку між ПС та службами КПР над малозаселеними та океанічними районами. В таких випадках зв'язок може бути забезпечено супутниковими системами зв'язку, або КХ радіозв'язком. Розглянемо проблему на прикладі рейсу «Київ – Нью-Йорк».

Рис. 1. Маршрут рейсу «Київ – Нью-Йорк»

До найбільш використовуваних систем супутникового зв'язку, що використовуються у цивільній авіації, належать низькоорбітальна система Iridium та геостаціонарна система INMARSAT.

Iridium – це низькоорбітальна супутникова система зв'язку, яка покриває всю поверхню Землі та налічує в собі 75 супутників (66 основних та 9 резервних). Особливістю супутників цієї системи в тому, що вони постійно рухаються, таким чином 1 супутник робить повний оберт навколо Землі за 100 хвилин. При цьому підтримка зв'язку між супутником та ПС триватиме до 10 хвилин, тому для

подальшого зв’язку з наземними станціями необхідне переключення систем зв’язку ПС на інший супутник у зоні видимості.

Особливої уваги заслуговує місцеположення супутника відносно абонента, яке визначається кутом місця (El). Найбільша потужність сигнала на вході приймача в радіоканалі «ПС-ШСЗ» буде забезпечено при значенні кута місця 90˚, а зі зменшенням цього значення зв'язок буде погіршуватися. Таким чином при малому значенні кута місця, як правило, до 5˚, супутник не буде обрано для встановлення зв'язку з ПС.

Залежність енергетики лінії зв'язку від кута місця можна пояснити двома факторами.

Першим фактором є те, що кут місця визначає нахил під яким радіохвилі входять в атмосферу, а зі збільшенням цього нахилу збільшується ділянка, необхідна для проходження атмосфери, відповідно затухання при її проходженні збільшується.

Другий фактор – кут входу супутникового радіосигналу у верхні шари атмосфери.

Кут місця, El	Рівень сигналу на вході приймача, дБм	Потужність сигналу на вході приймача, Вт
0,05	-116,385	$2,3 \cdot 10^{-15}$
14	-108,96	$1,26 \cdot 10^{-14}$
23,5	-106,92	$2,03 \cdot 10^{-14}$
90	-100,8	$8,255 \cdot 10^{-14}$

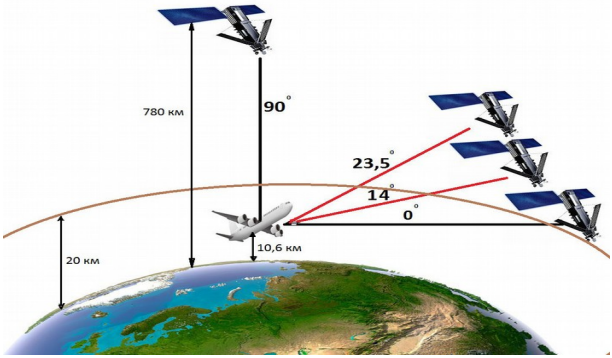


Рис. 2. Залежність енергетики лінії зв’язку від значення кута місця

УДК 004 (043.2)

О.О. Домарацький, В.В. Антонов
Національний авіаційний університет, м. Київ

ЗАХИЩЕНА МЕРЕЖА IP-ТЕЛЕФОНІЇ

IP-телефонія є одним із пріоритетних напрямків розвитку телефонного зв'язку. З кожним роком кількість абонентів, які використовують IP-телефонію (VoIP – Voice Internet Protocal) для проведення голосових переговорів, збільшується. Це пов'язано, насамперед, з меншою вартістю передачі даних за допомогою мережі Інтернет. Вже не тільки окремі користувачі, але й цілі підприємства намагаються використовувати Інтернет як основний засіб міжміського зв'язку. Оскільки комерційна інформація звичайно є конфіденційною, питання безпеки такого зв'язку є все більш актуальним.

На відміну від класичної телефонії, де використовується комутація каналів, IP-телефонія базується на мережевих протоколах з комутацією пакетів. У процесі передачі даних по IP-мережі вони проходять через певну кількість недостатньо захищених серверів, до того ж з'єднаних між собою незахищеними каналами. Одночасно IP-телефонія певним чином відрізняється і від звичайної передачі даних IP-мережами. Це пов'язано з необхідністю виконання аналого-цифрових перетворень даних в реальному часі. Зважаючи на необхідність дотримання вимог щодо якості зв'язку, такі перетворення, включаючи стискання, шифрування та інше., повинні відбуватися за мінімально короткий час. Від того, наскільки існуючі системи відповідають усім цим вимогам, залежать, значною мірою, перспективи подальшого розвитку IP-телефонії.

Все це показує, що IP-телефонія є перспективною, швидко розвивається послугою телекомунікацій, яка буде поступово витісняти традиційні телефонні технології з деяких сегментів ринку і в першу чергу, корпоративного, зацікавленого у створенні недорогих в експлуатації власних телефонних мереж. Системи IP-телефонії в даний час застосовуються організаціями самих різних форм власності та напрямків діяльності. Оборот капіталу IP-телефонії збільшується на 30%, а за деякими напрямками і на 50% в рік. Технологія IP не тільки володіє швидкою окупністю, а й приносить значний прибуток організаціям, в яких вона була впроваджена, за рахунок підвищення

якості обслуговування абонентів, підвищення ефективності роботи співробітників.

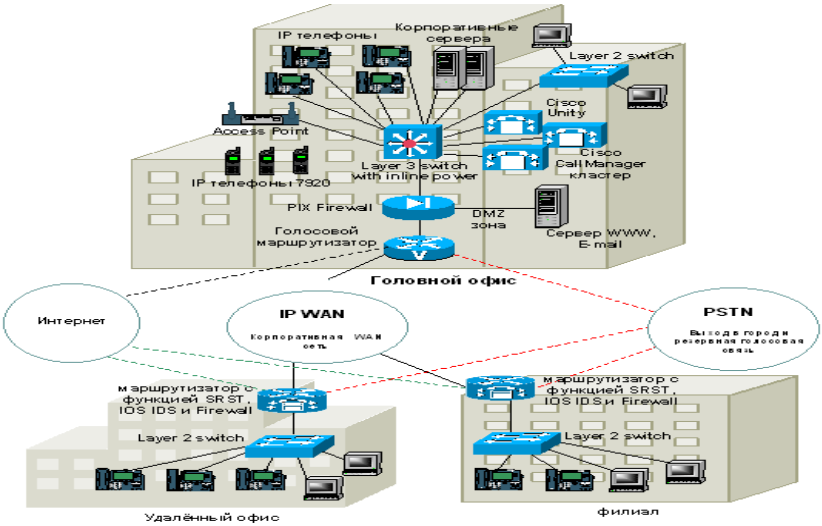


Рис.1. Архітектура захищеної мережі

У даній роботі на основі технології AAA порівняно протоколи аутентифікації TACACS + і RADIUS. Після дослідження протоколів аутентифікації, однією з основних складових захищеності, зроблено висновок, що в адміністративних мережах для захисту інформації краще використовувати протокол TACACS+, враховуючи особливості кожної мережі. Для мережі більшого масштабу краще використовувати протокол RADIUS.

У роботі проведено класифікацію загроз порушення конфіденційності у каналах телефонного зв'язку та запропоновано методологію усунення несанкціонованого зняття інформації.

Комплексне використання ряду перелічених технічних засобів дозволяє запобігти використанню каналів зв'язку для підслуховування телефонних розмов та прослуховування приміщень, через які вони проходять.

УДК 004 (043.2)

М.Ф. Єрьоменко, В.Є. Курушкін, В.В. Антонов
Національний авіаційний університет, м. Київ

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ЦИФРОВОЇ АТС

В світовому рейтингу найбільш технологічно ємних напрямків діяльності сучасного суспільства по праву посідає провідне місце галузь телекомунікацій. Світ переживає справжній бум розробки та впровадження все нових і нових методів та технологій передачі та обробки інформації, результатом чого за останні 10-15 років є глобалізація телекомунікаційних мереж, стирання національних кордонів та створення єдиного світового інформаційного простору.

Лавиноподібне і революційне впровадження різноманітних технологій в методи та технології передачі та обробки інформації в телекомунікаційних мережах, змушують принципово по-новому розглядати роль та значення технічного захисту інформації.

Узагальнюючою назвою таких мереж зв‘язку державних відомств та недержавних структур в сучасній термінології є відомчі або корпоративні телекомунікаційні мережі (мережі зв‘язку). Їх технічну основу традиційно складають комутаційні системи, реалізовані в виробничо-відомчих АТС, і саме тому вони є однієї з основних сфер уваги системи технічного захисту інформації в Україні.

В підтвердження цього зазначена Концепція серед основних загроз інформаційній безпеці особо відмічає, що "комутаційне обладнання іноземного виробництва, яке використовується у мережах зв‘язку, передбачає дистанційний доступ до його апаратних та програмних засобів, в тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв‘язку та змістом повідомлень, які пересилаються”.

Актуальність роботи визначається наступними факторами:

1. Нормативні документи системи ТЗІ в Україні, якими визначена методологія створення системи ТЗІ ЦАТС і оцінки захищеності її інформацій-них ресурсів, впроваджені в 90-х роках минулого століття. За період майже в п‘ять років технології ЦАТС розвивались вкрай динамічно, внаслідок чого традиційна АТС перетворилась в комутаційну платформу, на якій формується розгалужений комплекс програмно-апаратних аплікацій і цифрового абонентського сервісу. До таких рішень, які стали складовими

компонентами ЦАТС за зазначений період, перш за все можна віднести центри обробки викликів (Call Center), системи обробки абонентських голосових, електронних і факсимільних повідомлень, безпроводовий абонентський радіодоступ в стандарті DECT.

Однак, цей розвиток технологій ЦАТС поки що не знайшов свого відображення в НД СТЗІ в Україні. Якщо розвиток телекомунікаційних і інформаційних технологій йде шляхом розробки і впровадження інтегрованих рішень, таких як, наприклад, аплікації комп‘ютерно-телефонної інтеграції (CTI), то в НД СТЗІ ці технологій є предметом двох самостійних і несумісних напрямків захисту інформації в комп’ютерному і телекомунікаційному обладнанні.

2. Стан нормативної бази системи ТЗІ в Україні безпосередньо впливає на ефективність державної експертизи СТЗІ ЦАТС і її спроможність забезпечити власників корпоративних мереж зв‘язку вичерпною інформацією щодо реалізованої в ЦАТС системи ТЗІ і організаційно-технічним заходам по усуненню "слабких місць" в ній, особливо за умов використання різноманітних програмно-апаратних аплікацій ЦАТС.

3. Визначення методів і напрямків технічного захисту ЦАТС часто відокремлюється від телекомунікаційних і інформаційних технологій, з якими вони взаємодіють в корпоративних мережах зв‘язку і через які можуть реалізовуватись інформаційні атаки на ЦАТС.

4. На теперішній час, в технічній літературі (у відкритій і спеціальній) практично відсутні публікації з викладенням принципів побудови системи ТЗІ ЦАТС, які були б ув‘язаний з технічною реалізацією апаратно-програмної побудови конкретних моделей ЦАТС. Це об‘єктивно обґрунтовується серед іншого і тим, що виробники ЦАТС практично не розповсюджують необхідний для цього деталізований опис компонентів ЦАТС, особливо тих, що безпосередньо формують СТЗІ ЦАТС, і не зацікавлені у наявності у відкритих джерелах інформації щодо їхньої корпоративної політики безпеки, що знаходить реалізацію в СТЗІ ЦАТС.

В цій роботі робиться спроба визначити сучасні інформаційні загрози корпоративним ЦАТС і методи протидії ним на підставі аналізу, в основному, апаратно-програмної побудови цифрової телекомунікаційної системи.

УДК 004 (043.2)

Д.М. Збаровський, В.В. Антонов
Національний авіаційний університет, м. Київ

МОДЕЛЬ БЕЗПРОВОДОВОГО ДОСТУПУ ДО ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА ТЕХНОЛОГІЄЮ WIMAX

Моделювання – це один з найпоширеніших методів рішення завдань, при використанні якого досліджувана система замінюється більш простим об'єктом, званою моделлю, що описує реальну систему з точки зору досліджуваних критеріїв і характеристик.

Моделювання застосовується у випадках, коли проведення експериментів з реальною системою неможливо або недоцільно: наприклад, з причини крихкості або дорожнечі створення прототипу або з-за тривалості проведення експерименту в реальному масштабі часу.

Особливим видом математичних моделей є імітаційні моделі. В більшості випадків проектування мереж WiMax є досить складним і неоднозначним процесом. Розрахунок покриття відбувається на основі вимірювань рівня завад на місцевості, що потребує значних витрат коштів та часу. В даній роботі пропонується метод оцінки параметрів системи WiMax на основі математичної моделі, створеної в середовищі системи MatLab. Даний математичний апарат, в деякій мірі, може полегшити процес розрахунку покриття. Комп'ютерна Simulink-модель представляється у вигляді блок-схеми, що містить типові функціональні блоки систем управління та керованих об'єктів. В блоки включені комп'ютерні програми, обчислюють математичні функції. Значки на блоках представляють формули аналітичних виразів передатних функцій як відношення вихідної інформації до вхідної.

В даній роботі розглянуто актуальні проблеми однієї із найсучасніших широкосмугових радіотехнологій – WiMax. Основна увага приділялась оцінці факторів, що впливають на радіус дії системи. Було наведено дві основні стратегії покриття території – на основі максимальної густини потоку даних та на основі максимального покриття території, серед яких стратегія максимального покриття території була вибрана, як оптимальна для території України.

Серед основних чинників, що впливають на дальність передачі інформації, були окремо розглянуті вплив виду модуляції, чутливість приймача, коефіцієнт системного підсилення, вплив інтерференції та ряд інших факторів і параметрів. Через неможливість дослідження реальної системи передачі побудовано та налаштовано імітаційну модель фізичного рівня безпроводового доступу за технологією WiMax в середовищі MatLab.

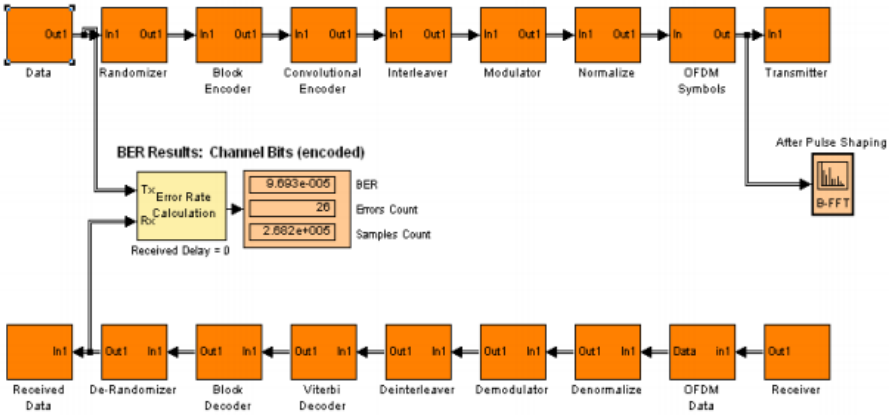


Рис. 1. Математична імітаційна модель стандарту IEEE 802.16 на основі методу WirelessMAN-OFDM

Таким чином, в рамках даної роботи магістра планується провести дослідження побудованої імітаційної моделі фізичного рівня безпроводового доступу за технологією WiMax.

Список літератури

1. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.

2. WiMAX – технология беспроводной связи: основы теории, стандарты, применение / В.С. Сюваткин, В.И. Есипенко, И.П. Ковалев та ін.; под ред. В.В. Крылова. – СПб.: БХВ-Петербург, 2005. – 368 с.

3. Вишневский В.М. Энциклопедия WiMAX: Путь к 4G/ В.М. Вишневский, С. Л. Портной, И.В. Шахнович. – М.: Техносфера, 2010. – 472 с.

УДК 621.397 (043.2)

О.Ю. Лавриненко
Національний авіаційний університет, Україна, м. Київ

СИСТЕМА ШИРОКОМОВНОЇ БАГАТОКАНАЛЬНОЇ ОБ'ЄКТНО-ОРІЄНТОВАНОЇ ДОСТАВКИ ВІДЕОКОНТЕНТУ В МОБІЛЬНИХ МЕРЕЖАХ

Проблема ефективної доставки відео контенту є актуальною задачею сьогодення. Бездротові мобільні мережі (WMN) у порівнянні з структурованими кабельними системами, стають перспективним рішенням для широкосмуговий доступу завдяки своїй гнучкості та доступності у залученні великої кількості користувачів. У WMN організовані Інтернет-шлюзи, маршрутизатори та вузли клієнта.

Потоки даних маршрутизуються між клієнтами і шлюзами із використанням бездротового зв'язку в режимі multi-hop. Головним викликом для WMN є надання підтримки мультикасту додаткам, які поширюються в Інтернеті протягом останнього десятиліття. До них відносять відеоконференції та потокове передавання медіафайлів. Такі додатки зазвичай обслуговують велику кількість користувачів і споживають високу пропускну здатність мережі.

Для вирішення цієї проблеми спочатку сформулюємо модель оптимальної системи передачі мультикасту в WMNs, з мульти-шлюзами і мульти-каналами. Передбачається дві різних технології фізичного рівня для вибору смуги частот в каналі, представлені двома відповідними моделями.

Перша модель базується на гнучких діапазонах частот (змінних частотах), як передбачено в програмно-конфігурованих радіостанціях SDR. Ця ідеальна модель радіоприймачів забезпечує оптимальну пропускну здатність мультикасту, яка може бути обчислена саме через класичну первинно-подвійну структуру оптимізації.
Друга модель досить схожа, але робить більш реалістичним припущення щодо частотних діапазонів сучасного стандарту IEEE 802.11: кожна передача має використовувати один з 13-ти попередньо визначених каналів.

Дві області потенціалу є фундаментальними для нашого формулювання проблеми мультикаст передачі: каналу та маршрутизації, на рівні MAC / PHY і мережевому рівні відповідно. Область каналу визначає набір, такий, що призначення каналу може підтримувати здатність вектора посилання. Область маршрутизації визначає набір такий, що вектор пропускної здатності може підтримуватися швидкістю потоку. Наприклад, два регіони не мають безпосереднього відношення до загальної структури оптимізації відповідно, де ми вибираємо оптимальні рішення з кожного регіону.

Пропускна здатність багатоадресної передачі для кожного сеансу вимірюється як швидкість прийому даних на приймачах та рівні для приймачів під час однієї сесію. Основне фізичне правило, яке встановлює зв'язок між областю маршрутизації і областю каналу полягає в тому, що агреговані швидкості потоку даних повинні бути обмежені відповідним посиланням потужностей. Крім того, ми дотримуємося умови у моделюванні пропускної спроможності, і приймають паралельну функціональність утиліти для пропускної здатності сеансу.

Багатоадресні програми потребують високої пропускної здатності. Були прийняті дві методики проектування системи: введення множини мережевих шлюзів для зменшення проблеми з вузьким місцем шлюзу і використання декількох бездротові канали для боротьби з проблемою збільшення ефективності доставки відео контенту. Загальна структура рішень є первісно-подвійною схемою, заснованою на формулюванні моделі оптимальної системи передачі мультикасту в WMN. Повторювальний перехід між вирішенням первинної проблеми для розподілу каналів і маршрутизації так як і подвійне оновлення змінної поступово прогресує до оптимальних або приблизно оптимальних рішень. Результати моделювання підтвердили запропоновані рішення в пропускній здатні вирішгити вище вказані проблеми, які спостерігалися при прямолінійних підходах багатоканальної мультикаст передачі.

УДК 621.391.1 (043.2)

О.Ю. Лавриненко
Національний авіаційний університет, м. Київ

АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ ПОБУДОВИ «РОЗУМНОГО» БУДИНКУ

Система «Розумний» будинок передбачає новий підхід в організації життєдіяльності в будинку, при якому, на основі комплексу високотехнологічного обладнання, створюється єдина автоматизована система управління, що дозволяє значно збільшити ефективність функціонування і надійність управління всіх систем життєзабезпечення.

Інтернет речей (IP, англ. - IoT) - це концепція простору, в якому все з аналогового і цифрового світів може бути поєднане. Крім цього це тісна інтеграція віртуального і реального світів, де відбувається "спілкування" між людьми і пристроями. Згідно з концепцією IP, речі, які оточують нас, зв'язуються між собою в єдину мережу, покликану забезпечити максимальний комфорт людині і економію енергоресурсів.

При аналізі були порівняні 3 найбільш популярні технології безпровідної передачі даних – ZigBee, Wi-Fi та Bluetooth.

Таблиця 1

Порівняння технологій передачі даних

Технологія передачі даних	**Zigbee (IEEE 802.15.4)**	**Wi-Fi (IEEE 802.1 1b)**	**Bluetooth (IEEE 802.15.1)**
Частотний діапазон	2,4-2,483 ГГц	2,4-2,483 ГГц	2,4-2,483 ГГц
Пропускна здатність, кбіт/с	250	11000	723,1
Розмір стеку протоколу, кбайт	32-64	Більше 1000	Більше 250
Час безперервної роботи від батареї, дні	100-1000	0,5-5	1-10
Максимальна кількість вузлів в мережі	65536	10	7
Діапазон дії	10-100	20-300	10-100
Галузь застосування	Дистанційний моніторинг та управління	Передача мультимедійної інформації	Заміна проводового з’єднання

З огляду на представлені дані порівняння основних параметрів бездротових технологій було визначено, що оптимальним стандартом для побудови розумного будинку є стандарт IEEE 802.15.4 також відомий як (ZigBee), тому що він використовується в разі, коли ставиться завдання встановлення зв'язку між автономними приладами та обладнанням, або збору інформації з території і централізації її на головному пристрої. Він визначає схему роботи на фізичному рівні (PHY), і на рівні управління доступом (MAC), і надає широкі можливості по підтримці різних топологій мереж. Збереження енергії забезпечується різними схемами мережевої маршрутизації, а наявність кількох маршрутів до координаторів мережі, забезпечує роботу мережі, навіть при виході одного з координаторів з ладу. Фізичний рівень ZigBee стежить за рівнем енергії в вузлах, а також проводить оцінку каналів, для більш достовірної і безперебійної комунікації. Рівень доступу до мережі відповідає за автоматичне підтвердження отримання пакетів, а також стежить за тим, щоб дані передавалися в певні часові інтервали. У MAC рівні ZigBee є можливість використовувати Wi-Fi або Bluetooth канали, якщо вони виявляться в межах досяжності.

Незважаючи на привабливі можливості технології ZigBee, необхідно ретельно врахувати кілька факторів, перш ніж зупинитися на її виборі. Основним фактором є можливість взаємодії, коли необхідно забезпечити зв'язок проектованого продукту з пристроями інших виробників. В іншому випадку в цілях економії можна реалізувати оригінальне рішення. Слід також мати на увазі, що координатор і маршрутизатори завжди повинні бути включені, настійно рекомендується підключити їх до енергомережі. Але велика перевагою цієї конфігурації полягає в можливості здійснювати обмін даними між точками за допомогою багатоінтервальних ліній зв'язку використовуючи коміркові топології.

В результаті було встановлено, що стандарт ZigBee являє собою дуже широкий інструмент для створення і обслуговування недорогих бездротових мереж з дуже низьким споживанням потужності і різноманітними функціями. Пристрої ZigBee мають дуже низьке енергоспоживання і невелику потужність, тому швидкість передачі даних невелика, але служать такі вузли досить довго і не вимагають постійного живлення від мережі.

УДК 621.39.005 (043.2)

М.В. Лихач, В.В. Антонов
Національний авіаційний університет, м. Київ

СИСТЕМА ЗВ'ЯЗКУ МІСТА НА ПЛАТФОРМІ SURPASS hiE9200

На сьогодні значна кількість операторів зв'язку має досить розвинену інфраструктуру для побудови становлення телекомунікаційної галузі. Інфраструктура включає в себе первинні мережі, в окремих випадках мережі доступу і транспортну інфраструктуру. Завдяки цим умовам традиційні послуги зв'язку, такі як доступ в Інтернет, телефонія і так далі, швидко втрачають прибутковість, в результаті чого розвивається конкурентна боротьба в усіх сегментах ринку і такій ситуації неминучого зниження тарифів. Для отримання доходів на ринку оператори зобов'язані вводити нові, високоприбуткові послуги зв'язку і, що не менш важливо, розділяти вже наявні послуги від аналогічних пропозицій конкурентів. Вирішення цього можливо шляхом удосконалення характеристик послуг користувачів, що надаються, додавання ефективних опцій і варіантів їх використання.

NGN (англ. Next Generation Network - мережі наступного покоління) - це мультисервісна мережа зв'язку, ядром якої є опорна IP-мережа (англ. Internet Protocol - міжмережевий протокол), що підтримує повну або часткову інтеграцію послуг передачі даних, мови і мультимедіа. Здійснює принцип конвергенції послуг зв'язку.

На сьогоднішній день, основним пристроєм для голосових послуг в мережах NGN є Softswitch - так називається програмний комутатор, який управляє VoIP (англ. Voice over IP; IP-телефонія - система зв'язку, що забезпечує передачу мовного сигналу по мережі Інтернет або по будь-яким іншим IP- мереж) сесіями. Також важливою функцією програмного комутатора є зв'язок мереж наступного покоління NGN з існуючими традиційними мережами ТМЗК, посредствам сигнального (SG) і медіа-шлюзів (MG), які можуть бути виконані в одному пристрої.

SURPASS hiE 9200 дозволяє об'єднати властивості мереж передачі мови, що підтримують широкий спектр послуг, з перевагами архітектури пакетно-орієнтованої мережі наступного покоління (NGN). У цій системі представлена унікальна комбінація новітніх комп'ютерних технологій, реалізованих на комерційній платформі з

високим потенціалом по продуктивності обробки, і всіх існуючих і майбутніх послуг.

Метою даного дипломного проекту є будівництво абонентських шлюзів типу DLU-IP фірми «Siemens» з перемиканням на них абонентів 25 вузлового району. Шлюз абонентських ліній DLU IP побудований на базі звичайного абонентського концентратора DLU з додаванням двох карт FPP на один статив DLU IP (4000 абонентських ліній). Одна плата FPP несе в собі чотири FP і забезпечує 16 E1 інтерфейсів з боку TDM частини. Пропонований тип плат дозволяє забезпечити 100% передачу голосу в кодеку G.711 без стиснення або для кожного мовного каналу може бути використаний будь-який кодек для стиснення. З іншого боку плати з'єднуються до вбудованого комутатора, через який забезпечується з'єднання в IP мережу.

Шлюз DLU IP підтримує інтерфейси FXS і ISDN BRI, ISDN PRI і V5.1 в сторону абонентських ліній. Всім абонентам DLU IP може бути надано набір послуг Class 5 в повному обсязі.Устаткування АШ буде розміщуватися в існуючих будівлях АТС.Будівництво цих об'єктів здійснюється на базі обладнання EWSD виробництва фірми «Siemens».

Для вирішення поставленого завдання був проведений аналіз структури існуючої міської телефонної мережі з виявленням особливості міжстанційних зв'язків проектованих абонентських шлюзів зі станціями мережі. Крім того, був проведений розрахунок капітальних витрат на комутаційне обладнання типу EWSD для абонентських шлюзів. Проведений аналіз дозволяє зробити висновок про доцільність застосування обладнання типу EWSD на міській телефонній мережі. Таким чином, поставлена в дипломному проекті завдання по заміні аналогового обладнання на цифрову систему комутації типу Surpass на міській телефонній мережі вирішена.

УДК 621.39.005 (043.2)

В.В. Сидорченко, В.Є. Курушкін
Національний авіаційний університет, м. Київ

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЛОГО ПІДПРИЄМСТВА

В результаті виконання роботи були розроблені необхідні організаційно-методичні документи і політика інформаційної безпеки.

Організовано процес реагування на інциденти за фактами порушень захисту інформації на підприємстві у вигляді Технічного регламенту.

Було проаналізовано всі інформаційні ресурси підприємства. В ході аналізу виявлено і класифіковано захищені інформаційні ресурси, класифіковані передбачувані порушники безпеки інформації, що циркулює на підприємстві, виявлені і класифіковані актуальні загрози безпеці ПДН в ІСПДн на основі базової моделі загроз безпеки ПДО при їх обробці в ІСПДн, для зменшення ризику реалізації загроз, були запропоновані і реалізовані заходи протидії.

Розроблено політику інформаційної безпеки та організаційно-розпорядчу документацію в області інформаційної безпеки для підприємства «Ukrainian TAX» України в м. Києві.

На закінчення, приведемо таблицю, як реалізуються різні механізми безпеки по рівнях запропонованої моделі.

Таблиця 1. Реалізація механізмів безпеки

Функція безпеки	Рівень моделі безпеки						
	1	2	3	4	5	6	7
Аутентифікація			+	+			+
Управління доступом		+	+	+	+	+	+
Конфіденційність з'єднання			+	+	+		+
Конфіденційність поза з'єднання				+			+
Виборча конфіденційність			+	+			+
Конфіденційність трафіку		+	+	+	+		+
Цілісність з відновленням				+			+
Цілісність без відновлення			+	+			+
Виборча цілісність			+	+			+

позначення: "+" - Даний рівень може надати функцію безпеки

Відзначимо особливо, що рівень 4 - «сервіси» надає всі функції безпеки. Не менш важливим є і рівень брандмауера (3), оскільки саме він забезпечує реалізацію функцій безпеки для зовнішніх мережевих з'єднань. Нарешті, останній рівень - 7 - "Політика безпеки". Знаки «+» у всіх рядках позначають, що в політиці безпеки можуть і повинні бути відображені всі аспекти забезпечення безпеки мережі.

Застосування запропонованої моделі на практиці, можливо, не відразу очевидно. Дійсно, адже сучасні мережі складаються з великої кількості робочих станцій, персональних комп'ютерів і серверів, а так само мережевого обладнання. Однак, як показала практика використання моделі, будь-яку мережу можна уявити в запропонованих термінах. Можливо, для цього її доведеться розбити на кілька підмереж з різними рівнями доступу, з'єднаних між собою брандмауерами. У цьому випадку, кожну таку підмережу слід розглянути окремо. З точки зору ж зовнішніх атак, можна розглядати всю мережу цілком. Такий підхід дозволить спростити практичну оцінку безпеки мереж і сервісів.

При розгляді моделі неможливо виділити більш-менш важливі рівні. Всі рівні важливі однаково для забезпечення безпеки. Разом з тим, можна відзначити особливу роль Політики безпеки, як основоположного документа.

Саме Політикою безпеки визначаються кроки і заходи, що вживаються на кожному рівні моделі. Саме Політика безпеки є тим стрижнем, навколо якого будується безпеку системи в цілому. Це важливо донести до розуміння як керівництва організації, так і рядових співробітників. Хоча, звичайно, дуже багато важить підтримка керівництва. Як уже згадувалося вище, Політика безпеки, яка не має активних прихильників в керівництві, приречена.

Словом, як ми бачимо, безпеку інформації в мережі підприємства або організації. Забезпечення безпеки включає в себе безліч аспектів як адміністративних, так і програмно-технічних. Причому заздалегідь складно сказати в якому разі які з них переважають і відіграють велику роль в загальній картині безпеки.

УДК 004 (043.2)

І.С. Сологуб, В.П. Климчук
Національний авіаційний університет, м. Київ

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

У рамках даної дипломної роботи було проведено дослідження становища вітчизняного нормативно-правового забезпечення в галузі безпеки інформації та розроблено підходи до створення та впровадження комплексної системи захисту інформації державного фінансового підприємства АКБ «Ощадбанк». Впровадження пропозицій і рекомендацій проведеного дослідження в державному банку дозволяє:

- суттєво підвищити якість моніторингу роботи систем захисту інформації (криптозахист, антивірусний захист, захист доступу до інформації, технічний захист обладнання мережі класу АС-3, програмний захист комп'ютерів мережі класу АС-3 від неліцензійного програмного забезпечення та технологічних збоїв т ін.) на базі комплексної системи захисту інформації в автоматизованих системах банку;
- підготувати банк до масового впровадження автоматів банківського самообслуговування та зменшити ризик несанкціонованого втручання в роботу систем обробки банківської інформації;
- побудувати систему ієрархічних резервних сховищ банківської інформації, які дозволяють на протязі 1-2 діб відновити роботу абиякого зруйнованого відділення банку без втрат клієнтської та банківської інформації;
- побудувати надійну спеціальну транспортну мережу на базі технології VPN між комп'ютерними мережами банку класу АС-3 та клієнтськими терміналами системи «Клієнт-банк» та «Інтернет-банкінг», які працюють через глобальну мережу Інтернет класу АС-3.

Для реалізації захищеного документообігу та забезпечення комплексного вирішення технічних питань організації захищеного юридично значущого електронного документообігу на корпоративному рівні фінансового підприємства запропоновано програмне рішення ТОВ «крипто-ПРО» «EToken КриптоАРМ».

УДК 621.391.7 (043.2)

О.О. Бережний
Національний авіаційний університет, м. Київ

ПРОГРАМНИЙ ЗАСІБ ШИФРУВАННЯ ЕЛЕКТРОННИХ ПОВІДОМЛЕНЬ

В сучасному світі в зв’язку з широким поширенням глобальної мережі Інтернет, значення електронного листування, як засобу швидкого пересилання повідомлень, складно переоцінити

Проблема шифрування електронних повідомлень полягає в вирішенні задачі перетворення повідомлення, використовуючи ключ, у такий вигляд з якого буде складно отримати повідомлення у початковому вигляді без наявності даного ключа. Ключ – це секретна інформація, яка використовується криптографічним алгоритмом при шифруванні/дешифруванні повідомлень.

Функцію шифрування електронних повідомлень реалізовано в поштових клієнтах, програмах миттєвого листування та окремих програмах шифрування файлів та рядків, зокрема в програмі PGP. Для цих програм властиво використання або асиметричного методу шифрування або гібридної криптосистеми.

В сучасних почтових клієнтах, таких як Microsoft Outlook та Mozilla Thunderbird використовуються асиметричні алгоритми шифрування, при чому користувачу необхідно попередньо зареєструвати ключ, оскільки за допомогою нього також здійснюється електронний підпис листа. Дані програми надають конфіденційність, цілісність та автентичність повідомленням, але не завжди є зручними для користувача.

В результаті аналізу засобів шифрування електронних повідомлень було встановлено, що використані в них алгоритми мають високу стійкість до криптоаналізу. Всі проаналізовані групи програм відрізняються:

а) в почтових клієнтах, окрім шифрування повідомлень, здійснюється цифровий підпис, що дозволяє захистити користувача від порушення цілісності та дозволяє однозначно ідентифікувати того, хто створив даний лист;

б) в програмах миттєвого листування ключі шифрування відомі лише на кінцевих пристроях (пристроях користувачів);

в) програма PGP є окремим програмним продуктом шифрування і підпису файлів і повідомлень, тому містить досить великий спектр налаштувань.

Характерними негативними рисами є або складний інтерфейс і складні налаштування для звичайного користувача або ж відсутність налаштувань безпеки взагалі, тому тема «Програмний засіб шифрування електронних повідомлень» є актуальною. Було розроблено програмний засіб, перевагами якого є:

а) використання web–інтерфейсу, що не вимагає від користувача встановлення окремої програми на свій комп'ютер;

б) наявність простих налаштувань безпеки;

в) простий інтерфейс користувача, що схожий на інтерфейси інших web–додатків.

Мною було проаналізовано технології для розробки програмного засобу, алгоритми шифрування, гешування та здійснено проектування основних модулів. Було проаналізовано симетричні алгоритми шифрування повідомлень, та встановлено, що алгоритмом з найкращими якісними показниками для розробленого додатку є AES. Для гешування паролів користувачів було вибрано алгоритм, що надає можливість багатоітераційного генерування хешу з використанням «солі», що має високий ступінь захисту від колізій – алгоритм PBKDF2WithHmacSHA512.

Було спроектовано діаграми класів для модулю генерації випадкового числа, модулю шифрування повідомлень та модулю взаємодії з базою даних. При цьому для модулів шифрування повідомлень та генерації випадкового числа було спроектовано множину класів, що реалізують різні алгоритми.

При розробці проекту була врахована необхідність застосування методів, що дозволяють покращити захист додатку і даних користувача та його гнучкість. Для захисту додатку було використано PreparedStatement для генерування запитів до бази даних та фільтер пакетів для захисту від міжсайтової підробки запиту.

Захист даних користувачів відбувається шляхом шифрування повідомлень та їх збереження у шифрованому вигляді та гешування паролів користувача. Гнучкість налаштувань забезпечується завдяки використання єдиного інтерфейсу для алгоритмів, що реалізують схожу функціональність. Таким чином було реалізовано вибір алгоритму шифрування повідомлень та гешування паролів.

УДК 004.75

В.Г. Корнішин
Національний авіаційний університет (м. Київ)

КОРПОРАТИВНА МЕРЕЖА ДЛЯ ПРОВЕДЕННЯ ВІДЕОКОНФЕРЕНЦІЙ

На сьогодні з розвитком технологій, також розвивається відеоконференцзв’язок. Одним з основних переваг, які дає нам відеоконференцзв'язок, є можливість перебувати одночасно в декількох місцях, віддалених на тисячі кілометрів, не залишаючи офісу. З кожним днем від компаній потрібна все більша ефективність для успішного ведення бізнесу. Інтернет і телекомунікації зробили величезний крок до прискорення всіх бізнес-процесів. Відеоконференцзв'язок відкриває нові кордони в цій гонці, роблячи прийняття важливих рішень, розвиток нових продуктів і послуг більш оперативним.

В ході відеоконференції Ви в реальному часі можете бачити вираз обличчя і мову жестів вашого співрозмовника. Ці речі є найважливішими аспектами спілкування, які губляться при звичайній телефонній розмові. Відеоконференція забезпечить більш ефективне спілкування персоналу компанії з клієнтами. Робота торгових представників може стати набагато продуктивніше, оскільки при візуальному спілкуванні можна краще оцінити перспективність клієнта для компанії. Все це, безсумнівно, поліпшить ваші ділові відносини з кращими клієнтами.

У роботі здійснено аналіз стану розробки та сфери використання відеоконференцзв’язку. На їхній основі, сформульовано вимоги до функцій і характеристик безпровідних вузлів та мереж. Виділено переваги й існуючі обмеження, які стримують широке використання відеоконференцзв’язоку. Використано класифікацію відеоконференцзв’язоку. Вказано перспективи використання і виділено існуючі проблеми при створенні корпоративної мережі для проведення відеоконференцій. Досліджено перспективні методи для вирішення питання стиснення відео та аудіо сигналів.

Було розглянуто існуючі види оптимізації відеосигналів, які використовуються в побудові мереж для проведення відеоконференцій.

Дані залежності досліджувалися при імітаційному моделюванні відеозв'язку. Використано методику розрахунку параметрів моделі, що враховує останні роботи по тематиці дослідження і особливості сучасних систем для проведення відеоконференцій.

Виявлено велику різноманітність підходів з визначення часу життя мережі. Запропоновано визначення, що враховує здатність корпоративної мережі до самовідновлення.

Доведено, що запропонована модель відрізняється від існуючих тим, що пропонує максимально економічну систему для проведення відеоконференцій, з підтримкою до 250 користувачів.

Підсумкове значення потужності, спожитої пристроєм при передачі даних, залежить від показників характеристики апаратних рішень; інтенсивності потоків даних; алгоритму доступу до середовища передачі.

Таким чином, на основі комплексного аналізу запроваджених даних топологій і алгоритмів стиснення відеосигналів, запропонована актуальна, мережа для проведення відеоконференцій

Висновки:

- Проведений аналіз показав, що системи для проведення відеоконференцій є перспективною технологією, що дозволяє зекономити кошти на відрядженнях.
- Ключовим показником, є можливість, стабільного, чіткого та візуального контакту з іншими учасниками переговорів в будь-якій точки світу.
- В ході дослідження було встановлено, що система TrueConf є максимально ефективною для малого та середнього бізнесу, так як вона підтримує протокол стиснення відеосигналу H264 та протоколу встановлення сесії SIP, та має конкуренто спроможною в співвідношенні ціна/якість.

УДК 621.39.005 (043.2)

А.С.Ткаченко
В.В.Антонов
Національний авіаційний університет, м. Київ

ПРОЕКТУВАННЯ МІСЬКОЇ МЕРЕЖІ ЗВ'ЯЗКУ НА БАЗІ ТЕХНОЛОГІЇ NGN

На сьогоднішній день перед керівництвом більшості операторів фіксованого зв'язку гостро стоїть питання оптимального вибору архітектурних шляхів реконструкції та розвитку своїх мереж. Пов'язано це, в першу чергу з тим, що відкритий конкурентний ринок телекомунікаційних послуг змушує операторів постійно розширювати номенклатуру послуг і, відповідно, модифікувати мережі.

Впровадження мережі послуг, відмінних від традиційної телефонії, призводить до розвитку сучасної мережевої інфраструктури. У телекомунікаціях активно позиціонується рішення з побудови мереж наступного покоління NGN(Next Generation Network), які не вписуються в раніше застосовувані підходи розвитку мереж зв'язку.

Найбільш важливим і витратним станом переходу до мереж NGN для всіх операторів зв'язку є процес інтеграції «старої» гетерогенної мережі, побудованої за принципами комутації каналів, з «новою» NGN-мережею. Причому під інтеграцією розуміється не тільки забезпечення технічного шлюзування трафіку між «старою» і «новою» мережею, але і спадкоємність відносно раніше створених послуг.

У даній роботі розроблена структура мережі з пакетною комутацією на прикладі міської телефонної мережі. Визначено склад апаратури, досліджені використовувані технології, розглянута економічна доцільність переходу з мережі з комутацією каналів на мережу з комутацією пакетів.

У ході виконання даної роботи були отримані наступні основні результати:

Розглянуто приклад побудови мережі на базі технологій NGN. На сьогоднішній день практично значущим є сценарій розвитку NGN на базі існуючої мережі ТМЗК. Основним елементом мережі є транспортна магістральна мережа, заснована на технологіях SDH, Ethernet, CWDM, DWDM.

Проаналізовано основні моделі NGN. Таким чином, в базовій функціональної моделі NGN виділяють два основних шари: транспортний і сервісний.

Виявлено недоліки мереж наступного покоління та визначено перешкоди на шляху до повсюдного впровадження NGN.

Зроблено аналіз принципів побудови мереж доступу. Був проведений розрахунок обладнання.

Представлені концептуальні підходи до мереж нового покоління, зокрема модернізація мережі, перспективи застосування технологій для побудови мультисервісної мережі.

При виборі технологій і концепцій перспективного розвитку та модернізації мережі підприємства зв'язку необхідно керуватися економічними мотивами. У разі мереж наступного покоління основними комерційними цілями є:

Збільшення доходів від впровадження широкого переліку послуг з доданою вартістю операторського класу, включаючи послуги інтелектуальної мережі(FPH, VOT, PCC, ACC, PRM);

Скорочення інвестицій на модернізацію та розвиток мережі телекомунікацій за рахунок оптимізації схеми передачі транзитного трафіку;

Скорочення витрат на експлуатацію мережі телекомунікацій;

Перехід від традиційних послуг приєднання сторонніх операторів до надання послуг з доданою вартістю, таких як Voice VPN, Hosted PBX, IP-телефонія, Teleworking та ін.;

Поділ бізнесу з надання послуг з доданою вартістю на операторський і провайдерський.

УДК 621.39.005 (043.2)

З.Н. Кудиненко
Національний авіаційний університет, м. Київ

БІЛІНГ-СИСТЕМА ІНТЕРНЕТ ПРОВАЙДЕРА

На сьогоднішній день невід'ємною складовою життя кожної людини є її швидка комунікація із навколишнім світом. Усе це загалом здійснюється за допомогою функціональних можливостей телефона та інтернету. За доступ окремого користувача до всесвітньої мережі інтернет, можливість здійснювати дзвінки, надсилати повідомлення та інші можливості відповідає провайдер, а за плату та виставлення рахунків за ці надані користувачам послуги відповідає спеціальна система, котра називається білінговою системою інтернет провайдера (БС).

Як відомо, кожен постачальник послуг прагне найкращого та найшвидшого обслуговування. Тому мета кожного провайдера забезпечити безперервне функціонування такої БС, що буде швидко та справно працювати. З цього виходить, що білінгова система повинна завжди коректно підраховувати всі використання користувача, тобто їх трафік, а також забезпечувати наглядне представлення, для того, щоб клієнт завжди бачив, за які саме послуги він сплачує кошти.

Термін «білінгова система» означає комплекс процесів, які відповідають за збір інформації про використання телекомунікаційних послуг, їх тарифікацію, виставлення рахунків абонентам та обробку платежів.

Кожна БС повинна мати в основі підсистеми для обслуговування клієнтів, такі як підсистема попередньої обробки даних, оперативного управління білінгом та підсистема оповіщення клієнтів. Ключовими моментами створення таких підсистем та самої БС є час обслуговування абонентів та збереження даних, необхідних для виставлення рахунку за надані послуги.

У наш час ця тема є дуже актуальною, бо наразі справу з провайдерами інтернету має кожен, а тому і з БС також. Це спонукає на створення нових БС із кращими характеристиками швидкості та правильності.

Широкого використання у рішеннях БС отримала препейд-система оплати послуг Післясплата з'явилася раніше, але передплата виявилася зручнішою саме для клієнтів, бо коли трохи щось йде не

так, то одразу відбувається відключення послуги, а не виставляється великий рахунок у кінці. Тобто гроші заносяться системою заздалегідь, у якості авансу.

У сучасному світі вже майже всі провайдери та мобільні оператори використовують конвергентні БС, що можуть одразу працювати як система передплати так і післясплати, а також надавати безліч інших переваг.

У роботі розглянуто роботу білінгових систем в залежності від виду, здійснено огляд та аналіз існуючих БС, якими користуються мобільні оператори України, їх характеристики, архітектура, функціональні рішення та переваги.

З розглянутих даних можна зробити висновок, що функціонал обраної БС перш за все залежить від запитів мобільного оператора або провайдера, тобто від того, на скільки якісно, швидко та вчасно вони прагнуть постачати послуги своїм абонентам.

Наразі зростає конкуренція між провайдерами та мобільними операторами, бо кожен прагне постачати послуги якнайкраще заради забезпечення лояльності своїх клієнтів.

У роботі розроблена структура мережі провайдера і білінової системи, також запропоновано такий алгоритм роботи БС, який містить швидкий та надійний механізм підрахунку плати за використанні послуги абонентами.

Отримані результати роботи дозволять використовувати БС із збільшеною ефективністю роботи та покращеним наглядним представленням використаних послуг абонентам та відповідної вартості на них.

УДК 621.391.7 (043.2)

Д.П. Микитьон
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА ПЕРВИННОГО РЕГІОНАЛЬНОГО ПРОВАЙДЕРА

Комп'ютерні мережі - як провідні, так і бездротові - стрімко приходять в повсякденне життя. Індивідуальні користувачі і організації в рівній мірі залежать від надійної роботи комп'ютерів і мереж в таких завданнях, як електронна пошта, облік, організаційне управління та робота з файлами. Несанкціоноване вторгнення в мережу може призвести до надзвичайно витратним перебоїв і втрати цінних результатів роботи. Атака на мережу може мати руйнівні наслідки з втратою часу і грошей в результаті пошкодження або розкрадання важливої інформації і ресурсів.

Зловмисники можуть отримати доступ в мережу, експлуатуючи уразливості в ПЗ, атакуючи обладнання або навіть використовуючи такі витончені прийоми, як вгадування чужого імені користувача та пароля. Зловмисники, які отримують доступ, змінюючи програмне забезпечення або експлуатуючи уразливості в програмному забезпеченні, часто іменуються хакерами.

Хакер, який отримав доступ в мережу, відразу стає джерелом чотирьох видів загроз:

розкрадання інформації;

розкрадання персональних даних;

втрата даних і маніпуляції з даними;

припинення обслуговування.

Загроза вторгнення в мережу виходить від зловмисників, розташованих як всередині, так і за межами організації.

Зовнішні загрози походять від осіб, які перебувають за межами організації і не володіють санкціонованим доступом до комп'ютерних систем і мереж. Зловмисники проникають в мережу ззовні, головним чином - з Інтернету, по бездротових каналах і через сервери комутованого доступу.

Внутрішні загрози походять від користувачів, що мають офіційно дозволений доступ в мережу з обліковим записом або фізичний доступ до мережного обладнання. Зловмисники, атакуючі

мережу зсередини, знайомі з внутрішньою політикою і персоналом. Крім того, вони зазвичай знають, яка інформація представляє цінність і найбільш вразлива, а також - як отримати до неї доступ.

Однак не всі внутрішні атаки є навмисними. У деяких випадках, внутрішня загроза виходить від сумлінного працівника, який, перебуваючи за межами компанії, став жертвою вірусу або порушення безпеки і, згодом, неусвідомлено приніс цю загрозу у внутрішню мережу.

Основним показником DDoS-атаки в мережі провайдера буде використання 100% використання центрального процесору на маршрутизаторі або взагалі відсутність зв'язку з ним. Якщо атака відбувається у клієнта можна побачити падіння BGP- сесій з ним та збільшення трафіку в каналі. Частіше всього великі провайдери використовують метод захисту від DDoS- атак засобами динамічної маршрутизації: - метод Blackhole («чорної діри») та аналізатори трафіку по IP-адресі, такі як sFlow та Kibana.

Blackhole дозволяє управляти трафіком на рівні провайдера, до попадання в нашу AS. Він ефективний для боротьби з великими атаками на пропускну здатність каналу. У магістральних провайдерів маршрути до приватних мереж, здебільшого, мають бути спрямовані в Null0 (Cisco термінологія, в Juniper - discard) пакети з адресою призначення цієї мережі буду автоматично відкидатися - потрапляти в «чорну діру» ще в мережі провайдера.

УДК 621.391 (043.2)

А. О. Павленко
Національний авіаційний університет, м. Київ

ЗАХИЩЕНА КОРПОРАТИВНА МЕРЕЖА ПІДПРИЄМСТВА З РОЗПОДІЛЕНОЮ СТРУКТУРОЮ

Останнім часом в світі телекомунікацій спостерігається підвищення інтерес до віртуальних приватних мереж. Це обумовлено необхідністю зниження витрат на утримання корпоративних мереж за рахунок більш дешевого підключення віддалених офісів і віддалених користувачів через мережу Інтернет. Однак необхідно відзначити, що при об'єднанні мереж через Інтернет, відразу ж виникає питання про безпеку передачі даних, тому необхідне створення механізмів, що дозволяють забезпечити конфіденційність і цілісність переданої інформації. Мережі, побудовані на базі таких механізмів називаються VPN.

У роботі було проведено розгляд загроз інформаційної безпеки з метою визначення набору вимог до розроблювальної системи захисту, а також створено захищену корпоративну мережу.

Слід зауважити, що відомо про великий перелік загроз інформаційної безпеки АС.

Тому необхідно класифікувати загрози інформаційної безпеки АС, це обумовлено тим, що збережена і оброблювана інформація в сучасних АС піддається впливу надзвичайно великому числу факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тож для захисту системи зазвичай визначають не повний

перелік загроз, а перелік класів загроз. Перелік класів загроз являє собою базові ознаки, тобто, природа виникнення, ступені та методи проявів загроз.

Більшість проблем з потенційними загрозами відкритого інтернету може вирішити VPN.

Нерідко людям потрібен доступ до своєї інформації, що зберігається на їх домашньому комп'ютері, або на комп'ютері фірми. VPN — технологія яка дозволяє забезпечити одне або декілька мережевих з’єднань (логічну мережу) поверх іншої мережі(наприклад Інтернет). Мета VPN технології полягає в максимальному ступені відокремлення потоків даних одного підприємства від потоків даних всіх інших користувачів мережі загального користування. Відособленість повинна бути забезпечена відносно параметрів пропускної здатності потоків, які гарантують конфіденційність. Отже, завданнями технологій VPN — є забезпечення в мережах загального користування гарантованої якості обслуговування для потоків даних, а також захист їх від можливого несанкціонованого доступу.

Підсумовуючи, хочу сказати, що технологія VPN має перспективу на широке поширення по всьому світу, не лише для приватних офісних мереж але, й для персональних.

УДК 621.39.005 (043.2)

А.П. Совгиря
Національний авіаційний університет, м. Київ

Радіомережа системи стільникового зв'язку

На сьогоднішній день по всій Україні успішно функціонує друге покоління мобільного зв'язку GSM (2G). Послуги, що можуть надаватися мережами GSM:

- Передавання голосової інформації.
- Послуга передавання даних (синхронний та асинхронний обмін даними, в тому числі пакетна передача даних — GPRS).
- Передавання коротких повідомлень (SMS).
- Передавання мультимедійних повідомлень (MMS).
- Передавання текстових інформаційних повідомлень (Cell Broadcast)
- Передавання факсів.

Процес вибору стільника.

Після вмикання живлення МС виконує пошук широкомовних каналів.

Кожна БС передає ці канали з постійною потужністю на частоті, такі частоти різні в кластері.

В процесі пошуку, МС:

- Сканує піддіапазон частот прямих каналів.
- Вимірює середню потужність радіосигналу на кожній частоті.
- Запам'ятовує частоти f з постійною потужністю сигналів.
- Обирає частоту на якій потужність максимальна.
- Перевіряє передачу каналу FCCH.

Мобільна станція може не сформувати такі біти, в цьому випадку мобільна станція переналаштовує синтезатор на іншу частоту з меншою потужністю сигналу, та знову перевіряє передачу каналу FCCH.

Процес розрахунку бюджету потужності.

Підготовка хендовера.

Контролер приймає рішення про необхідність хендовера у двох випадках:

- Відстань L> 35 км., при цьому порушується синхронізація МС та БС навіть при сильному сигналі і малому відсотку помилок.

- Будь-який усереднений параметр N разів підряд виходить за межі допуску (N=1…31). Значення N і всі допуски встановлюються в процесі налаштування системи БС індивідуально для кожної зони LA.

Складання списку БС кандидатів на хендовер, на основі вихідних даних.

Для БС виконується нерівність.

$$P_{\text{прм,i}} > P_{\text{прм},min,\text{i}} + max\left[0; P_{\text{прд,дозв,i}} - P_{\text{прд},max}\right]$$

Формула розрахунку бюджета потужності:

$$B_i = \left[\min\left(P_{\text{прд,дозв,0}}; P_{\text{прд},max}\right) P_{\text{прм,0}} - \Delta P\right] - \left[\min\left(P_{\text{прд,дозв,i}}; P_{\text{прд,max}}\right) - P_{\text{прм,i}}\right]$$

$P_{\text{прм,0}}$ — рівень FCCH сервісної БС на вході приймача МС;

$P_{\text{прм},i}$ — рівні прийнятих сигналів FCCH сусідніх БС. i = 1…n;

$P_{\text{прм},min,i}$ — мінімальний допустимий рівень прийнятого сигналу сусідньої БС;

$P_{\text{прд},max}$ — максимальна потужність передавача МС;

$P_{\text{прд,дозв,0}}$ — дозволена потужність МС в стільнику сервісної БС;

$P_{\text{прд,дозв,i}}$ — дозволена потужність МС в сусідніх стільниках;

$\Delta P = P_{\text{прд},,max} - P_{\text{прд,факт}}$ — резерв потужності передавача сервісної БС;

Приймальний сигнал БС1 менший ніж БС2, БС1<БС2 (-60<-58), однак в стільнику БС2 МС має дефіцит потужності передавача (30<33), тому обирає для хендовера першу БС.

Після цього виконується мережева операція в результаті якої, канал трафіка перемикається на обрану БС. Умова B_i≥B_min може не виконуватися для всіх сусідніх БС. В цьому випадку вираховування їхніх бюджетів продовжується і всі вони є кандидатами на хендовер.

УДК 621.39 (043.2)

В.О. Харь, В.В. Антонов
Національний авіаційний університет, м. Київ

ЦИФРОВА СИСТЕМА КОМУТАЦІЇ SI 2000 V. 5

На сьогоднішній день зв'язок відіграє першорядну роль у всіх сферах людської діяльності: в економіці й промисловості, науці й техніці, культурі, державному керівництві.

Мережі зв'язку – це головні комунікаційні лінії, по яким передається інформація, і які внаслідок цього надто розширились по своїм масштабам і функціональним можливостям.

Розвиток електрозв'язку в нашій країні, на жаль, йде з деяким відставанням від розвинених закордонних країн. Незважаючи на це, в Україні можна побачити значний прогрес – це пов'язано з появою нових операторів зв'язку.

Для задоволення сучасних вимог в області електрозв'язку й повноцінного входження у світове телекомунікаційне співтовариство необхідний перехід до цифрової комутації. Значним кроком у розвитку телекомунікацій стала побудова цифрових систем комутації. На мережах України впроваджено досить багато типів ЦСК переважно зарубіжної розробки. Цифрова система комутації SI2000, розроблена словенською фірмою ISKRATEL, виробляється в кількох країнах, в тому числі і в Україні, спільне українсько-словенське підприємство "Моніс" (м. Харків) на мережах країни впроваджує цифрове телекомунікаційне обладнання сімейства SI2000. Достатньо велика кількість абонентів станції SI2000 можуть з честю оцінити якість зв'язку та широкий спектр додаткових послуг.

ЦСК SI2000 має гнучку модульну архітектуру обладнання і ПЗ, комутацію і керування, централізовані експлуатацію і технічне обслуговування, інтегровану систему електроживлення. Ця цифрова система економічна, її можна легко пристосовувати до обслуговування територій з малою щільністю населення.

Дана комутаційна система невибаглива до умов використання на мережі та до умов довкілля. ЦСК SI2000 має широкі можливості використання на всіх ієрархічних рівнях міських та сільських телекомунікаційних мережах загального користування і в корпоративних мережах.

В ході виконання роботи були проведені розрахунки навантаження цифрової станції та кількості з'єднувальних ліній, що дозволяють підключитись Оператору до ТфМЗК, розраховано сигнальне навантаження, яке передбачається маршрутувати між комутаційними станціями операторів.

В даній роботі розраховано кількість обладнання станції, склад обладнання цифрової комутаційної станції SI-2000. Дані результати можуть бути використані на практиці.

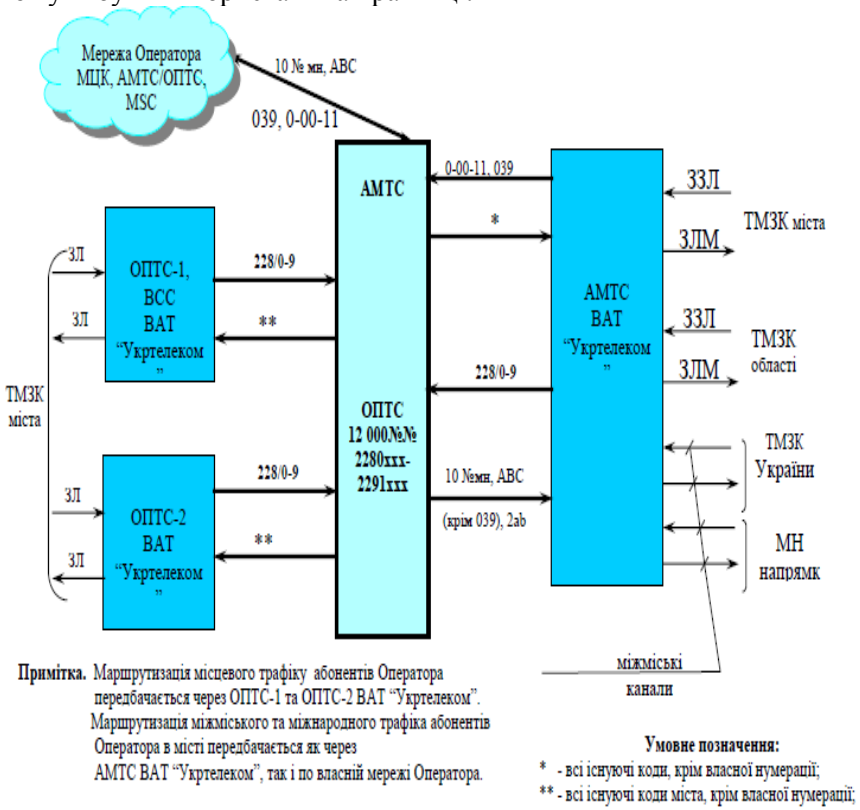


Рис.1. Схема маршрутизації трафіку від/до АМТС/ОПТС Оператора

УДК 004.75

Квашенко І.В.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ

АНАЛІЗ ВИКОРИСТАННЯ МОДЕЛІ ПУБЛІЧНОЇ ХМАРИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

На даний час розглядається можливість розгортання п’яти моделей для послуг хмарних обчислень: приватна хмара, громадська хмара, публічна хмара, гібридна хмара та віртуальна приватна хмара. Розглянемо більш детально одну з напоширініших моделей – комерційну хмару, що являється різновидом моделі публічних хмар. Перевагою цієї технології є економічна ефективність та масштабованість, однак ця технологія стикається з цілою низкою труднощів і проблем, зокрема проблеми безпеки та доступності.

Проблеми безпеки в хмарних обчисленнях зазвичай пов’язані з основними технологічними компонентами, на які покладаються хмарні обчислення. Цими компонентами є веб-додатки, віртуалізація і криптографічні методи. Основною загрозою для веб-складової хмарних обчислень є атаки сеансового рівня моделі OSI та ін’єкційні атаки на веб-додатки, а віртуалізаційний бар’єр може бути прорваний хакерами, що призводить до часткового чи навіть повного доступу до даних.

До сторонніх проблем безпеки можна віднести проблему встановлених програм в хмарному середовищі, що можуть містити вразливості, які дозволяють потрапити всередину інфраструктури. Також існує проблема відновлення даних минулих користувачів сервісів новими користувачами через використання одних і тих самих апаратних ресурсів.

Аналіз публікацій в даній предметній області показує, що на даний час проблема безпеки хмарних сервісів торкається навіть лідерів ринку хмарних послуг, таких як Amazon, Google, Microsoft, що створює необхідність створення нових способів захисту даних на різних рівнях взаємодії клієнта та сервера. Для вирішення даної проблеми необхідно проводити перевірку цілісності даних та аутентифікацію користувача.

Перевірка цілісності даних у хмарі є необхідною умовою для розгортання додатків, тому для реалізації дистанційної перевірки цілісності даних шляхом об'єднання коду виправлення помилок і перевірки точок запропоновано використання теоретичної основу «Докази відновлення» (“Proofs of Retrievability”). Розглянемо основні механізми доступу, перевірки та зберігання даних:

Система HAIL, що використовує POR механізм для перевірки зберігання даних в різних хмарах, яка може забезпечити надмірність різних копій та реалізувати наявність і перевірку цілісності.

Віддалена перевірка надійного модуля платформи (TPM) для віддаленої перевірки цілісності даних.

Механізми шифрування для надійного доступу до персональних даних у хмарі, що використовують такі алгоритми як RSA, 3DES (рис. 1). Якщо RSA використовується для створення захищенного зв’язку між аутентифікованим користувачем та сервером хмари, то 3DES– для шифрування блоків даних.

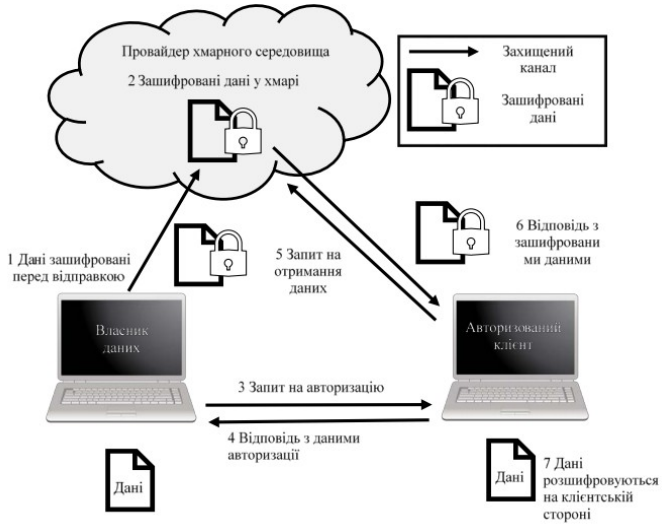


Рис. 1. Варіант механізму шифрування для надійного доступу до персональних даних у хмарі

Отже, аналіз даної публікації показує важливість перевірки цілісності даних та аутентифікації користувача. Розвиток механізмів

УДК 621.39.005 (043.2)

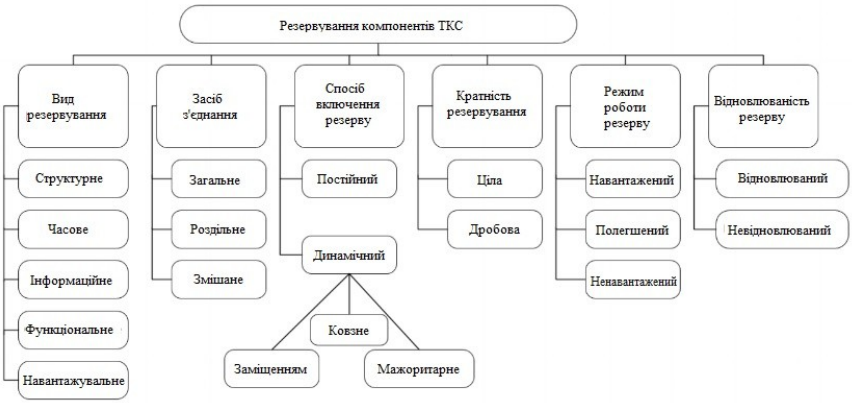
Шихов М.С.
Національний технічний університет України "Київський політехнічний інститут" імені Ігоря Сікорського, м. Київ

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Інформаційно-комунікаційні мережі є невід'ємною частиною сучасної інфраструктури і слугують для забезпечення безперебійного зв'язку та передачі даних на великі відстані без втрати чи спотворення цих даних. Однією з ключових характеристик інформаційно-комунікаційних мереж, що розглядається при їх проектуванні, є їхня надійність. В свою чергу надійність є комплексним терміном, що описує сукупність багатьох властивостей інформаційно-комунікаційних мереж, а саме безвідмовність, ремонтопридатність, довговічність, збережуваність та комплексна властивість надійності. Для розрахунку значень, що відповідають цим властивостям використовуються наступні кількісні показники надійності: ймовірність безвідмовної роботи, густина розподілу наробітку до відмови, середній наробіток до відмови, інтенсивність відмов, параметр потоку відмов, середній наробіток на відмову, ймовірність відновлення в заданий час, густина розподілу часу відновлення, середній час відновлення, інтенсивність відновлення, ймовірність відновлення в заданий час, густина розподілу часу відновлення, середній час відновлення, інтенсивність відновлення, гама-відсотковий термін збереження, середній термін збереження, коефіцієнт готовності, коефіцієнт технічного використання, коефіцієнт оперативної готовності та коефіцієнт збереження ефективності.

Важливою концепцією в сучасних інформаційно-комунікаційних мережах є концепція програмно-конфігурованих мереж, в яких рівень керування мережею відділений від пристроїв передачі даних і реалізується програмно. В таких мережах під надійністю в першу чергу розуміють відмовостійкість системи та здатність до швидкого відновлення. Існує 2 окремих механізми забезпечення відмовостійкості в мережі: резервування (захисне перемикання) та перемаршрутизація (відновлення). Ці методи мають свої недоліки та переваги, тому вибір робиться в залежності від функціональних вимог до конкретної мережі, а бізнес-сегменті

частіше використовуються обидва методи. Резервування потребує заздалегідь підготованого додаткового (резервного) шляху, по якому буде направлений весь трафік. Нижче наведена класифікація резервування компонентів телекомунікаційних систем:



В свою чергу перемаршрутизація виконується за рахунок пошуку нового шляху після відновлення зв’язку. Основними вимогами до методів забезпечення надійності є економія пропускної здатності, обмеження комп’ютерних ресурсів, здатність до масштабування, швидкість заміщення та складність методу.

Таким чином, залежно від призначення і розв'язуваних завдань інформаційно-комунікаційні та радіотехнічні системи мають різний склад, різні концепції реалізації, технічні характеристики й розташовуються найчастіше в різних пунктах. У зв'язку із цим доцільно розглядати експлуатаційні процеси стосовно до радіоелектронного пристрою й лише в окремих випадках - до системи у цілому.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 ЧЕРВНЯ 2019 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР КОНАХОВИЧ Г.Ф.

КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.

КОНТАКТНИЙ E-MAIL: conference.tks@i.ua

ВІДПОВІДАЛЬНІСТЬ
ЗА ЗМІСТ ТА ФОРМУ ВИКЛАДЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ
НЕСУТЬ АВТОРИ МАТЕРІАЛІВ ТЕЗ.

ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ КОНФЕРЕНЦІЇ ЗРОБЛЕНА СПЕЦІАЛЬНО ДЛЯ РОЗМІЩЕННЯ НА САЙТІ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ
http://tks.nau.edu.ua