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

Т Е З И

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

3 – 6 ЧЕРВНЯ 2013 Р.

М. КИЇВ

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

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

3 – 6 ЧЕРВНЯ 2013 Р.

М. КИЇВ

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

Кулик М.С. — д.т.н., професор, ректор Національного авіаційного університету, заслужений діяч науки і техніки України, лауреат Державної премії України.

Члени оргкомітету:

Харченко В.П. — д.т.н., професор, проректор Національного авіаційного університету з наукової роботи, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, заступник голови конференції;

Конахович Г.Ф. — д.т.н., професор, завідувач кафедри телекомунікаційних систем Національного авіаційного університету, заслужений працівник транспорту України, заступник голови конференції, відповідальний редактор збірника тез конференції;

Корнейко О.В. — к.т.н., доцент, заступник Голови Державної служби спеціального зв'язку та захисту інформації України, заступник голови конференції;

Лінник О.О. — голова технічного департаменту ТОВ «ТІПІ-ЛІНК ЮКРЕЙН», заступник голови конференції;

Корченко О.Г. — д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету;

Юдін О.К. — д.т.н., професор, директор Інституту комп'ютерних інформаційних технологій Національного авіаційного університету, член-кореспондент Академії зв'язку України, лауреат Державної премії України в галузі науки і техніки;

Швець В.А. — к.т.н., доцент, завідувач кафедри засобів захисту інформації Національного авіаційного університету.

Секретар:

Голубничий О.Г. — к.т.н., доцент, докторант Національного авіаційного університету.

УДК 004.71 (043.2)

А.Д. Сорокун
Національний авіаційний університет, м. Київ

МЕРЕЖЕВІ ТЕХНОЛОГІЇ PLC В ТЕЛЕКОМУНІКАЦІЯХ

Актуальність питань дослідження існуючих мережевих технологій та виведення альтернативних стає все більш значною по мірі збільшення кількості пристроїв, які люди використовують у повсякденному житті та які мають різноманітні варіанти підключення один до одного.

Проводяться інтенсивні дослідження за кордоном, і виводяться в промисловість кінцеві розробки, що потрапляють і на наш ринок.

Інтерес до нової технології PLC виявили вже давно, а тепер вона стає все більш доступною і в Україні.

Дослідження цієї технології в Україні поки що не проводились.

PLC (Power Line Communication) розшифровується як «зв'язок за допомогою ліній електропередач». По цій лінії і передається мережевий сигнал. Схожі системи стали застосовуватися ще більше століття назад. Тоді по кабелям між підстанціями передавався телеграфний сигнал. Зі збільшенням числа високовольтних ліній електропередач, впроваджувалися системи високочастотного зв'язку для телефонії та телеметрії. Принцип роботи PLC в тому, що різні типи даних (тональні сигнали, голос, мережевий трафік) передаються по кабельному з'єднанню, але на різних частотах. Кожен пристрій (телефон, модем, адаптер) фільтрує «чужі» частоти і отримує тільки те, що здатен обробити. Головною перевагою PLC є відсутність необхідності в прокладанні додаткових кабелів для створення ще однієї мережевої інфраструктури, а також відносна простота використання і більш надійний зв'язок, ніж при організації бездротового доступу.

Стандарт HomePlug AV, є різновидом технології PLC. Він був представлений влітку 2005 року. Згідно з цим стандартом, швидкість мережевого з'єднання може досягати 200 Мбіт/с, якої повинно вистачати для передачі потокового відео і голосу. При цьому швидкість автоматично регулюється залежно від якості

зв'язку. З'єднання має шифруватися за допомогою 128-бітного ключа AES, а також підтримувати правила QoS (Quality of Service).

В ході досліджень були зроблені такі висновки:

- в цілому PLC технологія забезпечує дуже непогану швидкість з'єднання;
- для якісного зв'язку необхідно хороше провідне з'єднання – без скруток, врізок кабелю різного типу, пошкодженої ізоляції;
- використовувати PLC має сенс тільки у разі недоцільності або неможливості прокласти кабель Ethernet до певної віддаленої точки чи невеликого сегменту мережі, або організувати бездротове з'єднання;
- при ідеальному варіанті підключення PLC взагалі практично аналогічний стомегабітному каналу Ethernet.

УДК 621.396.49 (043.2)

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

ПОБУДОВА МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ LTE У СОЛОМ'ЯНСЬКОМУ РАЙОНІ м. КИЄВА

Розвиток бездротового зв'язку супроводжується безперервною зміною технологій, в основі яких лежать стандарти стільникового зв'язку GSM і CDMA, а також стандарти систем передачі даних IEEE 802. Історично технології бездротового зв'язку розвивалися по двох незалежних напрямках – системи телефонного зв'язку (мобільний зв'язок) та системи передачі даних (Wi-Fi, WiMAX). Сьогодні дві групи технологій явно націлені на надання універсальних послуг зв'язку. Це WiMAX (як розвиток лінії IEEE 802) і технології стільникового зв'язку поколінь 3GPP LTE. Основною перевагою мереж побудованих на технології 3GPP LTE є передача інформації зі значно більшими (на порядок) швидкостями.

Технологія LTE є черговим етапом еволюції мереж бездротового мобільного зв'язку після GSM та UMTS. Ця технологія дозволяє підвищити ефективність передачі

інформації, знизити питомі витрати на побудову мереж, розширити і удосконалювати послуги, що вже надаються. Мережі на основі стандарту LTE здатні працювати практично по всій ширині спектра частот від 700 МГц до 3,8 ГГц. Швидкість закачування за стандартом 3GPP LTE в теорії досягає 326,4 Мбіт/с (download), і 172,8 Мбіт/с на віддачу (upload). Практично забезпечує швидкість передачі даних від базової станції до пристрою абонента до 100 Мбіт/с і швидкість від абонента до базової станції – до 50 Мбіт/с. LTE-мережа дозволяє користуватися такими послугами як «відео на вимогу», забезпечуючи потокову передачу без затримок відео в HD-роздільності. Операторам впровадження технології LTE дозволить зменшити капітальні та операційні витрати, знизити сукупну вартість володіння мережею, розширити свої можливості в області конвергенції послуг і технологій, підвищити доходи від надання послуг передачі даних. Враховуючи перспективність та сучасність цієї технології, як природного чергового етапу еволюції мереж мобільного зв'язку, розроблено концепцію побудови мережі на основі LTE технології в Солом'янському районі м. Києва. Також проаналізовано структури мереж на базі технологій: GSM, UMTS, LTE, та основні переваги і недоліки кожної технології мобільного зв'язку для організації мереж зв'язку і надано порівняльні характеристики технологій бездротового мобільного зв'язку.

Враховуючи характеристики радіо інтерфейсу LTE, структуру мережі, принципи прийому та передачі інформації, принципи організації інформаційних потоків, диспетчеризації, переваги технології в частині частотного плану для базових станцій та основні характеристики місцевості і кількості населення, що можуть стати потенційними клієнтами послуг мобільного зв`язку стандарту LTE, обрано оптимальне місце їх встановлення. Також стисло розглянуто необхідне обладнання, для побудови мережі на базі обладнання LTE компанії Alcatel-Lucent.

УДК 621.39:376.71 (043.2)

І.В. Василюк
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА БАНКІВСЬКОЇ УСТАНОВИ. РОЗРОБКА, ПРОЕКТУВАННЯ, РОЗРАХУНОК ПАРАМЕТРІВ. ПРОПОЗИЦІЇ ЩОДО МОДЕРНІЗАЦІЇ МЕРЕЖІ

В роботі розглянуто типові принципи побудови локальної мережі для організації даного типу. Досліджено вимоги щодо проектування, вибору та налаштування обладнання. Дана банківська установа займає одне з провідних місць на ринку фінансових послуг. Тому комп'ютерна мережа має бути спроектована відповідно до усіх існуючих нормативно-правових актів, має бути виконана з використанням найсучаснішого передового телекомунікаційного обладнання та володіти високим рівнем захищеності від несанкціонованого доступу до банківських даних.

За відомою мені схемою змодельовано комп'ютерну мережу з базовим телефонним каналом зв'язку, що з'єднує відділення банку (точка обслуговування клієнта) з регіональним управлінням банку (точка зосередження централізованих баз даних, серверів управління та доступу, та ін.).

При виборі пасивного обладнання увага зверталась на відомі компанії, що позитивно зарекомендували себе на ринку телекомунікаційних послуг. Враховуючи серйозність даної мережі, перевагу віддано продукції фірми-виробника Panduit (США). Виробник дає гарантію 25 років на побудовані сертифікованими спеціалістами кабельні мережі з використанням його продукції. Розроблена типова мережа, окрім пасивного обладнання, включає наявність сплітера (мікрофільтра), adsl-модему, маршрутизатора Cisco та комутатора на 8 портів. Враховуючи тенденції розвитку сучасного ринку телекомунікаційного обладнання, запропоновано замінити в перспективі adsl-модем та маршрутизатор пристроєм «2 в 1». До переваг запропонованого пристрою можна віднести наявність безпровідного зв'язку стандарту 802.11a/b/g/n та можливість керування пристроєм та користувачами мережі, використовуючи смартфон на базі iOS/Android. Проте запропонована ідея буде вимагати підвищенної уваги до

безпеки та захисту від несанкціонованого доступу до ресурсів мережі. Проведено співставлення протоколів та методів захисту даних використовуваного маршрутизатора Cisco 871 та запропонованого adsl-маршрутизатора Linksys X-1000. Для того, щоб підтвердити проект наявної мережі чи довести можливість її модернізації, було прийнято рішення проаналізувати можливість використання програмних та апаратних засобів маршрутизаторів Cisco 871 та Linksys X-1000. Порівняння проводилось на основі методу аналізу ієрархій (MAI).

Згідно з отриманими результатами виявилось, що незважаючи на наявні переваги у використанні та додаткові функції, а також нижчу вартість у маршрутизатора Linksys X-1000, цілісність даних у комп'ютерній мережі відділення банку не може бути гарантована через відсутність протоколів, що відповідають за захист інформації. Зважаючи на те, що в банківській мережі відбувається обмін даними про клієнтів та обіг грошових одиниць, вирішено використовувати мережу з маршрутизатором Cisco 871, спираючись на наявні в нього засоби захисту інформації.

УДК 004.056.53:004.451.622 (043.2)

И.В. Кохан, А.Б. Кочубей
Национальный авиационный университет, г. Киев

МЕТОДЫ СКРЫТОГО ПОДСОЕДИНЕНИЯ К ОПТОВОЛОКНУ

Количество информации передаваемой по оптоволоконным линиям связи постоянно растет, что в свою очередь порождает вопросы о возможности несанкционированного снятия информации и ее защиты.

Подключение к оптоволокну (fiber tapping) – процесс, при котором безопасность оптического канала компрометируется вставкой или извлечением световой информации. Различают два метода подключения: интрузивный или неинтрузивный, при первом требуется перерезать волокно и подсоединить его к промежуточному устройству, при использовании второго подклю-

чение выполняется без нарушения потока данных и перерыва сервиса.

Рассмотрим основные методы подсоединения к волокну:

1. *Сгибание волокна* – кабель разбирается до волокна, которое затем сгибается таким образом, чтобы угол отражения стал меньше чем критический угол полного внутреннего отражения, и свет стал проникать через оболочку. Существует два типа сгибов: микроскгиб и макросгиб.

2. *Оптическое расщепление* – оптоволкно вставляется в сплиттер, который отводит часть оптического сигнала, этот метод является интрузивным, т.е. может вызвать срабатывание тревоги, но необнаруженное подключение может работать годами.

3. *V-образный вырез* – это специальная выемка в оболочке близкая к ядру, сделанная таким образом, чтоб угол между светом, распространяющимся в волокне и проекцией V-выреза больше, чем критический, это вызывает полное внутреннее отражение, при котором часть света будет уходить из основного волокна через оболочку и V-образный вырез в ней.

4. *Использование неоднородных волн* – данный способ используется для перехвата сигнала от волокна-источника в волокно-приемник, путем полировки оболочек до поверхности ядра и затем их совмещения. Что позволяет некоторой части сигнала проникать во второе волокно. Данный метод трудновыполним в полевых условиях.

Защита от несанкционированных подключений включает три категории методов предотвращающих или снижающих до минимума влияние таковых.

1. Наблюдение за кабелем и мониторинг – включает мониторинг мощности мод в многомодовых волокнах, внедрение дополнительных волокон или проводников для срабатывания тревоги при попытке согнуть кабель или нарушении целостности его оболочки, и другие методы.

2. Использование сильногнущегося волокна с низкими потерями и сильным радиусом изгиба, что позволяет защитить сеть передачи данных, ограничивая высокие потери при прокалывании или сгибании волокна.

3. Шифрование – никак не препятствует подключению к волокну, но делает снятую информацию малополезной для злоумышленников.

Стоит отметить, что помимо снятия информации существует ряд методик по внедрению ее в передаваемый поток, что может привести к нарушению целостности передаваемой полезной информации.

УДК 004.056.53 (043.2)

Д.Б. Бур'янцев
Національний авіаційний університет, м. Київ

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ДАНИХ У ХМАРНИХ СЕРВІСАХ

На даний момент хмарні сервіси дуже стрімко розвиваються, і питання про безпеку їх використання стоїть дуже гостро. Як прості так і корпоративні користувачі хочуть бути впевненими, що їх інформація буде в повній безпеці, як на віртуальному так і на фізичному рівнях.

Зараз багато великих компаній мають свої хмарні сервіси, серед них можна назвати такі: iCloud від компанії Apple, Google Drive, Dropbox, нещодавно з'явився copy.com який робить акцент на високу безпеку і чималий обсяг безкоштовного сховища.

Хмарні сервіси дають можливість не маючи великого обсягу фізичної пам'яті в ПК, розширювати її за допомогою віртуальної яку надають сервіси такого роду, а також за допомогою "хмари" можна виробляти різного роду обчислювальні процеси не маючи при цьому потужного заліза, і при всьому цьому мати доступ до всього в будь-якій точці світу, при наявності Інтернету.

Звичайно при виборі сховища своїх даних варто відштовхуватися і від того, чим компанія, що надає послуги займалася або займається ще. Наприклад copy.com, творці якого, як вже було вище сказано, акцентують увагу на безпеці свого дітища. А якщо копнути глибше можна зрозуміти, що copy.com створено

компанією Barracuda Networks основна діяльність якої – захист даних.

Але є сервіси серйозніше, там і захист, і надійність в рази вище, але звичайні користувачі швидше за все не будуть використовувати їх з причини високої вартості і спрямованості цих компаній на корпоративних клієнтів.

Компанії, що пропонують різне програмне забезпечення для інформаційної безпеки, створили багато систем шифрування і міжмережевих екранів для захисту хмарних послуг. Наприклад CloudProtect CloudSpan від компанії Layer 7 та JaxView for Cloud Management від компанії Managed Methods. Такі компанії, як Catbird Networks, Altor Networks і Reflex Systems, також адаптували свої продукти для безпеки центрів обробки даних до роботи в хмарному середовищі [1].

Список літератури

1. Безопасность в облаке. [Електронний ресурс] – Режим доступу: http://www.cisco.com/web/UA/about/news/2011/11152011b.html – Загол. з екрану.

УДК 621.3.029.64 (043.2)

Ю.В. Романюк
Національний авіаційний університет, м. Київ

БЕЗДРОТОВИЙ СЕГМЕНТ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Тенденція розвитку сучасних засобів зв’язку така, що основоположними критеріями прогресу є швидкість передачі даних, якість переданої інформації та збільшення її об’єму, а також зручність доступу до неї. Так, сьогодні вже не є фантастикою безпроводові засоби зв’язку і робота над їхнім вдосконаленням не стоїть на місці.

Сучасні технології безпроводової передачі даних активно впроваджуються й широко використовуються як у виробничій діяльності більшості компаній, так і для побудови комп’ютерних мереж для домашнього використання. Нові апаратні рішення в області безпроводової передачі даних дозволя-

ють створювати й комп'ютерні мережі в межах одного будинку, і розподілені мережі в масштабах цілого міста.

На сучасному етапі розвитку мережних технологій, безпроводова технологія Wi-Fi є найбільш зручною в умовах потребуючих мобільність, простоту розгортання та використання.

Безпека корпоративних мереж відіграє дуже важливу роль. У міру розвитку технологій електронних платежів, "безпаперового" документообігу серйозний збій локальних мереж може паралізувати роботу цілих корпорацій і банків, що призводить до відчутних матеріальних втрат. Слід також зазначити, що окремі сфери діяльності (банківські та фінансові інститути, інформаційні мережі, системи державного управління, оборонні та спеціальні структури) вимагають спеціальних заходів безпеки даних і пред'являють підвищені вимоги до надійності функціонування інформаційних систем, відповідно до характеру і важливості вирішуваних ними завдань.

Метою роботи є оцінка існуючих систем захисту корпоративної мережі на основі безпроводової технології Wi-Fi, економічна оцінка доцільності застосування даних систем в корпоративних мережах, розробка рекомендацій побудови захищеної Wi-Fi мережі офісу на основі вихідних даних проведених оцінок.

Для досягнення поставленої мети вирішуються такі основні задачі:

– дослідження побудови та функціонування безпроводових мереж Wi-Fi;

– аналіз систем захисту Wi-Fi мереж та їх вразливостей;

– математичний розрахунок оцінки доцільності застосування систем захисту в корпоративних безпроводових мережах;

– розробка рекомендацій щодо побудови захищеної Wi-Fi мережі офісу.

УДК 621.3.029.64 (043.2)

Ю.В. Ступаков
Національний авіаційний університет, м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ПРИМІЩЕННЯ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

Одним з найпоширеніших технічних засобів, які використовуються для несанкціонованого отримання інформації, є різні електронні пристрої перехоплення інформації або так звані радіозакладні пристрої, які використовують радіоканал як середовище передачі небезпечних сигналів. Основне місце їх використання внутрішні приміщення об'єктів і будівель як державного призначення, так і комерційних структур.

Найпоширенішими засобами є так звані акустичні заставні пристрої з передачею інформації по радіоканалу. Вони займають лідируюче місце серед засобів технічного шпигунства. Радіозакладні пристрої використовуються для негласного добування інформації як із статичних об'єктів, так і динамічних.

Останніми роками розвиток систем знімання інформації (радіозакладних пристроїв) йде у напрямі підвищення передачі отриманої інформації шляхом використання в радіозакладних пристроях спеціальних сигнально-кодових конструкцій і зменшення часу, необхідного для передачі інформації.

В даний час, самими досконалими і ефективними в маскуванні факту роботи є два типи радіозакладних пристроїв: які використовують шумоподібний сигнал і сигнал надкороткої передачі.

При цьому слід врахувати, що сучасні РЗП в більшості випадків використовуються в межах промислово розвинених індустріальних центрів. Це призводить до того, що пошукові бригади здійснюють пошук і виявлення небезпечних сигналів радіозакладок в неоптимальних, умовах, що обумовлене відсутністю апріорних відомостей про самий небезпечний сигнал і місце його появи, нестаціонарністю шумової обстановки в умовах міста і екрануванням небезпечних сигналів несучими конструкціями будівель і міжповерхових перекриттів.

Слід зазначити, що якщо задача виявлення для типових радіозакладок, що використовують прості види модуляції (АМ,

ЧМ, ФМ) вже знайшла достатньо точне і ефективне рішення, то для радіозакладних пристроїв які використовують різного роду складні або шумоподібні сигнали, а також сигнали надкоротких передач ще не розроблені ефективні методи локалізації і виявлення.

В даній роботі розглянуто особливості технічної побудови заставних пристроїв і їх характеристики, які можуть зробити істотний вплив на процедуру пошуку і виявлення. Розглянутий радіоканал як середовище розповсюдження небезпечного сигналу. Розглянуті основні існуючі методи і способи технічною аналізу сигналів для встановлення їх приналежності до заставних пристроїв.

УДК 004.7 (043.2)

Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

ЗАХИЩЕНА КОРПОРАТИВНА МЕРЕЖА АВІАПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ D-LINK

Метою проекту є набуття практичних навиків в проектуванні захищених корпоративних мереж масштабу крупного підприємства, закріплення теоретичних знань по дисциплінах підготовки спеціальності «Телекомунікаційні системи та мережі».

Виходячи з мети роботи, завданням проекту є розробка захищеної корпоративної мережі на базі доступного по вартості, надійного та гнучкого в налаштуванні обладнання телекомунікаційної компанії D-Link.

На першому етапі проектування я дослідив переваги корпоративних мереж та способи їх побудови. Далі було обрано оптимальній спосіб побудови корпоративної мережі для конкретного авіапідприємства.

На другому етапі проектування було досліджено комплексні системи захисту корпоративних інформаційних систем та обрано реалізацію системи захисту мережі авіапідприємства з використанням демілітаризованої зони, двох міжмережних екранів, другого Mail та Web серверів.

На третьому етапі проектування були вирішені наступні завдання:

1. Розподілення всіх комп'ютерів центрального офісу авіакомпанії.

2. Розробити схему IP-адресації мережі.

3. Обрання ОС на хостах мережі, мережевої ОС, СУБД, та іншого програмного забезпечення.

4. Визначення числа і типів серверів, що використовуються в мережі.

5. Обрання та обґрунтування типів каналів зв'язку та активного комунікаційного обладнання згідно обраної технології передачі даних.

6. Розробка структурної схеми мережі авіакомпанії.

На четвертому етапі проектування було розроблено систему захисту ІТС, яка включає в себе:

1. Рольову структуру ІТС та категорії користувачів згідно з правами доступу центрального офісу авіапідприємства.

2. Опис потенційних загроз для інформації в мережі.

3. Розробку системи захисту поштового серверу Windows Exchange Server 2010, налаштування безпеки в Windows та захист від DOS-Атак.

4. Вибір антивірусного захисту серверів та робочих станцій авіакомпанії

5. Приклад налаштування міжмережних екранів D-Link серії DFL-1600.

В результаті проведених досліджень було розроблено корпоративну мережу авіапідприємства з використанням технології VPN на базі місцевого провайдера зв'язку для зручності обміну інформацією з віддаленими співробітниками та філіями. Для фізичного захисту мережі був використаний метод на базі двох міжмережних екранів та використання другого Mail та Web серверів, які будуть знаходитись у демілітаризованій зоні. Для програмного захисту було використано розмежування доступу особового складу авіапідприємства до окремих ресурсів мережі та встановлено антивірусний захист серверного та комп'ютерного устаткування авіакомпанії.

УДК 004.258 (043.2)

А.Ю. Черкай
Національний авіаційний університет, м. Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПАКЕТНИМ ТРАФІКОМ

Перед будь-якою сучасною телекомунікаційною мережею, яка обслуговує пакетний трафік, постає проблема раціонального управління ресурсами: забезпечення максимально можливого коефіцієнта завантаженості комутаційного обладнання при збереженні заданого рівня якості обслуговування потоків інформації. Вона виникає через непередбачуваний пульсуючий характер інформаційного трафіка, який ускладнює забезпечення необхідної якості надання послуг при суттєвому навантаженні на мережеві комутаційні пристрої. Через це показник коефіцієнта використання обладнання будь-якої мережі не перевищує 0,4. Для його підвищення використовуються механізми інженерії пакетного трафіка, які дозволяють збільшити рівень інформаційного завантаження мережевого устаткування в середньому лише до величини 0,5 – 0,55.

Поставлена задача підвищення ефективності керування пульсуючими потоками протокольних блоків даних вирішується за допомогою адаптивного методу управління смугами пропускання портів пакетного комутатора. Суть технічного рішення полягає у включенні до підсистеми розподілу пропускної спроможності комутаційного пристрою певного адаптивного механізму керування, який у реальному часі забезпечує динамічні зміни пропускних спроможностей портів синхронно із поточними змінами інтенсивності потоків даних. В даному випадку це означає виділення більшої частки від загальної пропускної спроможності комутатора для того порту, на вводі якого збільшилася інтенсивність потоку протокольних блоків даних, за рахунок частки пропускної спроможності порту, на якому в цей час спостерігається її зменшення або незмінність. На кожному з портів комутатора параметри інтенсивності увідних потоків вимірюються за допомогою вимірювального блоку. Результати подаються на вхід регулятора, який зіставляє їх з існуючими в цей момент часу розмірами смуг пропускання та визначає вели-

чину та напрямок необхідних змін. Таким чином виконується динамічний перерозподіл пропускної спроможності мережевого пакетного комутатора між його портами відповідно до пульсацій потоків протокольних блоків даних, що ними просуваються. В наслідок цього мінімізується кількість проміжків часу, на яких інтенсивність трафіка більша за смуги пропускання портів і перевантаження обладнання виникає рідше.

За допомогою комп'ютерного моделювання виконано експериментальні дослідження, які підтвердили ефективність використання адаптивного методу управління смугами пропускання портів пакетного комутатора. Аргументована можливість істотного підвищення коефіцієнта використання комутаційного пристрою (до величин порядку 0,65 – 0,75) без істотного зменшення якості обробки інформаційного трафіка. Отже, застосування дослідженого методу в телекомунікаційних мережах дозволяє досягти суттєвого підвищення інформаційного навантаження.

УДК 004.258 (043.2)

О.І. Василенко
Національний авіаційний університет, м. Київ

ФОРМУВАННЯ ПАКЕТНОГО ТРАФІКА ДЛЯ ЗАБЕЗПЕЧЕННЯ РОБОТИ ЗАСОБІВ АДАПТИВНОГО УПРАВЛІННЯ

Адаптивне управління розподілом ресурсів пакетних мереж – вид динамічного управління, що здійснюється в реальному часі. Дана технологія дозволяє виділяти більшу частку ресурсів для тих елементів мережі, навантаження котрих наближається до критичної межі, за рахунок зменшення частки ресурсів виділеної недовантаженим елементам. Сумарна продуктивність вузлового обладнання (ВО) при цьому не змінюється.

Технологія адаптивного управління дозволяє завантажити комутуюче обладнання мережі на 65-70%. Однак досягнення такого результату на практиці не можливе внаслідок недостатньої швидкодії системи, що призводить до появи системних помилок управління; недостатньої прогнозованості та високої динамічно-

сті пакетного трафіка, що призводить до непередбачуваних втрат пакетів.

Для боротьби з переліченими недоліками та підвищення якості адаптивного управління в умовах значних пульсацій трафіку пропонується вдосконалити відому систему адаптивного управління за рахунок застосування у схемі блоків формування потоків пакетів (БФП) та блоку прогнозування (БПР). Введення таких елементів дозволяє якісно підвищити завантаженість мережевого обладнання, а також зменшити кількість системних помилок управління.

Встановлення БПР дозволяє використовувати в процесі управління раніш виміряну (апостеріорну) інформацію, що дає можливість системі прогнозувати можливу поведінку потоків трендів на наступних кроках управління. Однак для ефективної роботи передбачувача, необхідно аби трафік, що надходить до ВО, відносився до асимптотично самоподібних процесів. На практиці ж маємо справу з мало прогнозованими пульсаціями нестаціонарних потоків пакетів. Тобто просте включення БПР у контур адаптивного управління не вирішує проблеми прийняття помилкових рішень. Для ефективної роботи технології необхідно застосування методів формування пакетного трафіку, що досягається введенням БФП.

Формування пакетного трафіку відбувається в декілька етапів: спершу проводиться процедура усереднення потоків пакетів, далі – формування трендів цих потоків. Останнє дозволяє забезпечувати узгодженість роботи системи адаптивного управління.

Введені вдосконалення (механізми прогнозування та формування пакетного трафіку) забезпечують ефективну роботу засобів адаптивного управління розподілом ресурсів пакетних мереж. Процедура усереднення потоків пакетів дозволяє певною мірою згладжувати пульсації трендів, що сприяє якості прогнозування трафіку, а встановлення БПР – зменшувати кількість втрачених через системні помилки управління пакетів. Загалом маємо можливість значною мірою підвищити завантаженість ВО.

УДК 004.042 (043.2)

Є.В. Сказатня
Національний авіаційний університет, м. Київ

ДОСЛІДЖЕННЯ ВПЛИВУ ПАРАМЕТРІВ НАДІЙНОСТІ ТА ЗАВАДОСТІЙКОСТІ КАНАЛУ НА ЕФЕКТИВНУ ШВИДКІСТЬ ПЕРЕДАЧІ ДАНИХ

Мова являє собою потік інтервалів активності та пауз, що чергуються. Аналоговий за своєю природою, мовний сигнал може передаватися цифровим способом після дискретизації, квантування і кодування. У мережах з комутацією пакетів повідомлення розбивається на частини стандартної довжини, що забезпечуються службовою інформацією та передаються по мережі як єдине ціле. Кожен пакет може передаватися незалежно від інших, що суттєво знижує затримку яка відносно рівномірно розподіляється між усіма активними абонентами або ж з урахуванням інших переданих пакетів.

Причин виникнення відмови у системах передачі даних доцільно поділити на дві основні групи:

1) Стійкі відмови елементів обладнання, які зумовлені кінцевою апаратурною надійністю. Вони можуть мати місце навіть при відсутності завад у каналі зв'язку. Розподіл проявів таких відмов зазвичай моделюють за допомогою закону Пуасона.

2) Відмови, що за певних умов можуть самоусуватися (такі відмови називають збоями). Вони проявляються в межах одного чи декількох тактів роботи СПД і зумовлені, головним чином, дією завад, що виникають у каналах зв'язку.

У реальних умовах експлуатації мережного обладнання мають місце обидва види відмов.

Швидкість передачі даних визначиться як:

$$R_{\text{E}} = f\left(R_0, \rho_{\text{K}}, n_{\text{П}}, t_{\text{A}}, \varepsilon, \omega, T_{\text{B}}, p_{\text{E}}, s\right),$$

де R_0 – швидкість передачі сигналів даних; ρ_{K} – кодова швидкість; $n_{\text{П}}$ – довжина пакету даних; t_{A} – час розповсюдження сигналів через канал зв'язку, а також аналізу та підтвердження (або перепитування) прийому пакету; ε – показник групування помилок внаслідок завад; ω – інтенсивність апаратурних від-

мов; $T_{\text{В}}$ – середній час відновлення після відмови; s –кількість перепитувань; p_{E} – ймовірність збою одиничного елементу сигналу даних.

Величина R_{E} визначає реальну пропускну здатність каналу зв'язку і, таким чином, з одного боку, визначає час передачі пакету, а з іншого боку, вплив завад та надійності обладнання на системні характеристики системи обслуговування. Тим самим, параметр R_{E} можна вважати одним із основних чинників, що безпосередньо пов'язує параметр навантаження Y з показниками якості обслуговування QoS.

УДК 004.7 (043.2)

Ю.В. Чуприна
Національний авіаційний університет, м. Київ

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ РЕЗЕРВУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Глобальність масштабів застосування телекомунікаційного обладнання (ТКО), величезні розміри абонентських баз користувачів їхніх ресурсів, надзвичайна різноманітність та важливість багатьох вирішуваних на їхній основі завдань обумовлюють жорсткі вимоги щодо забезпечення норм на показники надійності функціонування обладнання. Зокрема, коефіцієнт готовності ТКО (інтегральний показник надійності) у сучасних умовах його використання має бути не гіршим, ніж 0,9999, а в деяких особливо відповідальних випадках має наближатися до 0,99999. Зрозуміло, що без застосування методів експлуатаційного резервування ТКО, у т.ч. його програмного забезпечення, здійснити дотримання названої норми не уявляється можливим. Тому у даній роботі поставлено за мету розробити методи та схеми експлуатаційного резервування елементів ТКО, що забезпечують мінімізацію капіталовкладень та експлуатаційних витрат за умов необхідності задоволення жорстких вимог щодо показників надійності функціонування обладнання.

З метою отримання конкретних результатів удосконалення існуючих технологій експлуатаційного резервування сфера да-

ного дослідження обмежена однією конкретно визначеною функціональною групою об'єктів ТКО - обладнанням систем управління елементами мережі абонентського радіодоступу до опорної мережі 3G WCDMA стандарту UMTS/WCDMA, а у рамках визначеної групи – двома конкретно визначеними рівнями агрегації обладнання – рівнем макроелементів мережі абонентського радіодоступу (базові станції, контролер базових стацій, канали передачі даних в межах домену підсистеми радіодоступу тощо) та рівнем функціональних модулів (конструктивно оформлених у вигляді типових елементів заміни – ТЕЗів), що реалізовані у складі цих макроелементів.

У даній роботі виконано узагальнене представлення структури середовища експлуатаційного резервування ТКО і на цій основі визначено відповідні методи та схеми резервування цього обладнання. Зокрема, надане оригінальне представлення структури взаємодії макроелементів, функціональних та конструктивних модулів обладнання підсистеми абонентського радіо доступу стільникової мережі 3G, яке дозволило забезпечити досягнення максимального значення коефіцієнту готовності обладнання при заданих капіталовкладеннях та експлуатаційних витратах.

Отриманий результат може слугувати формальною основою для розробки нового комбінованого методу та відповідних процедур оптимального резервування елементів обладнання 3G WCDMA, впровадження котрих в експлуатаційний процес дозволяє забезпечити підтримку високих показників надійності функціонування обладнання.

УДК 004.032.2 (043.2)

М.М. Солнцева
Національний авіаційний університет, м. Київ

АБОНЕНТСЬКИЙ ТЕРМІНАЛ GSM

Перші системи наземного мобільного зв'язку з автоматичною комутацією та маршрутизацією з'єднань були розроблені і запроваджені у 60-х роках XX сторіччя. Глобальна система мобільного зв'язку – міжнародний стандарт для мобільного циф-

рового стільникового зв'язку з розділенням каналу за принципом TDMA та високим рівнем безпеки за рахунок шифрування з відкритим ключем. Стандарт був розроблений під патронатом Європейського інституту стандартизації електрозв'язку (ETSI) наприкінці 1980-х років. Більшість мереж GSM працюють у діапазоні 900 МГц або 1800 МГц. Деякі країни Америки використовують діапазони 850 МГц та 1900 МГц, оскільки стандартні діапазони 900 та 1800 МГц зайняті іншими системами. Діапазони 400 та 450 МГц використовуються у деяких країнах (включаючи країни Скандинавії та деякі острівні країни). Послуги, що можуть надаватися мережами GSM:

– передача голосової інформації;
– послуга передачі даних (синхронний та ансинхронний обмін даними, в тому числі пакетна передача даних – GPRS);
– передача коротких повідомлень (SMS);
– передача мультімедійних повідомлень (MMS);
– передача текстових інформаційних повідомлень (Cell Broadcast);
– передача факсів.

В роботі розраховувалася мережа стільникового мобільного рухомого зв'язку. Були визначені такі параметри: загальна кількість частотних каналів МРЗ, розмірність кластеру, кількість секторів обслуговування в одному стільнику, кількість абонентів, що обслуговуються однією базовою станцією, кількість базових станцій, які потрібно встановити для обслуговування заданої території, радіус одного стільника , необхідна чутливість радіоприймача мобільної станції (МС).

Частотно-територіальне планування мережі радіозв'язку передбачає вибір структури мережі, місця встановлення базової станції, вибір типу, висоти та орієнтації антен, розподіл частот між базовими станціями. Проаналізувавши отримані розрахунки, можна зробити висновок, що кількість базових станцій від кількості абонентів залежить прямо пропорційно. Для обслуговування менше 40 тис. абонентів потрібна одна базова станція, а для обслуговування від 40 до 80 тис. абонентів буде достатньо дві базові станції.

Стрімкий розвиток мережі мобільного зв'язку спостерігається в усьому світі. Активне використання такого виду зв'язку робить актуальною задачу ефективного використання радіочастотного спектру, який дозволяє оптимально планувати мережі радіозв'язку. Слід відзначити, що на протязі всього життєвого циклу мобільного зв'язку кількість її абонентів, об'єм трафіку та його розподіл по території обслуговування постійно змінюється. Окрім цього, існують сезонні зміни об'єму трафіку і його територіального розподілення. Конфігурація стільникової мережі повинна адаптуватись до змін.

УДК 621.396.49 (043.2)

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

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ ПСЕВДОВИПАДКОВИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ В ШИРОКОСМУГОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Об'єктом дослідження даної роботи є коди Голда.

Метою роботи є моделювання кодових послідовностей Голда і дослідження кореляційних властивостей їх усічених реалізацій.

В ході роботи були вивчені алгоритми моделювання М-послідовностей та кодів Голда. Отримані 32 коди довжиною 1023 біти. На їх основі були досліджені усічені послідовності. Вивчались два варіанти усікання: з початку і з кінця комбінації.

Актуальність роботи полягає саме у застосуванні усічених ортогональних кодів. Використання даного способу дає змогу розробникам систем із кодовим розділенням каналів не обмежувати довжину кодових послідовностей довжинами 2^N–1 для кодів Голда, чи 2^N для функцій Уолша.

Усікання кодових послідовностей негативним чином впливає на їх кореляційні властивості. Чим сильніше усікаються кодові комбінації в системі з кодовим розділенням каналів, тим сильніше дані канали впливають одне на одного, підвищуючи взаємні завади сигналів. Зі збільшенням видалених елементів послідовностей все більше порушується ортогональність кодів.

В роботі досліджені залежності ступеня зменшення ортогональності кодів та інших їх властивостей від кількості елементів, що усікаються. А також розглянуті два варіанти локації видалення елементів із кодових послідовностей: з початку із кінця послідовності.

Отримані результати дають нам змогу говорити про перспективи використання усічених кодових послідовностей Голда в системах із кодовим розділенням каналів, в яких розробники не мають можливості використовувати відомі нам ортогональні коди Голда стандартної довжини. Наприклад: у таких системах GPS, де використовуються коди Голда, в яких обмежена смуга частот, в межах якої вони повинні експлуатуватися. Системи із кодовим розділенням каналів потребують доволі широкої смуги частот, адже кодові послідовності, що використовуються значно довші за інформаційний сигнал. Саме в такій ситуації роль усічених ПВП важко переоцінити. Адже у наш час найціннішим ресурсом у сфері телекомунікації, що бурхливо розвивається, є радіочастотний. З кожним роком кількість систем, які потребують певного радіочастотного ресурсу, стає все більше і питання економного їх використання вже давно стало гострим.

УДК 621.396 (043.2)

А.Ф. Шатирко
Національний авіаційний університет, м. Київ

ВСТАНОВЛЕННЯ NGN В МІСТІ КИЄВІ. РОЗРОБКА, ПРОЕКТУВАННЯ, РОЗРАХУНОК ПАРАМЕТРІВ

В роботі розглянуто принцип побудови мережі нового покоління NGN для району міста Києва.

Досліджено основні вимоги щодо проектування, вибору та налаштування обладнання. Проведено вибір і обґрунтування апаратури мережі, вирішені питання вимірювання основних параметрів мережі, проведені необхідні розрахунки, прорахована вартість реалізації проекту.

У техніко-економічній та теоретичній частинах проекту я обґрунтував актуальність введення нової мережі NGN та її реалізація, додаткові послуги, які вдасться реалізувати при її ввe-

денні. Також описувалися питання побудови мереж NGN, розглянуті протоколи, топології та архітектури мереж, управління мережею, функціонування та обслуговування мереж. Основними елементами мережі NGN є SoftSwitch, що є мережевою архітектурою; сигнальний шлюз; транспортний шлюз; шлюз доступу; медіасервер; цифрова телевізійна станція; STB.

У технічній частині проекту обрано технології доступу, розподілу, взаємодія мережевих елементів, і відповідні їм обладнання. В даний час волоконно-оптичні лінії зв'язку (ВОЛЗ) найбільш перспективні для побудови різних мереж зв'язку. Розроблено загальна структурна схема мережі, розроблена методика проектування даної мережі. Місто в побудові проекту NGN ми розбиваємо на райони, кожен з яких обслуговується одним OLT. Райони підключаються до центральної станції по топології кільце. Даний спосіб збільшує надійність мережі.

У структурній схемі центрального вузла зв'язку та для побудови мережі доступу ми використовуємо обладнання: Концентратор GPON (OLT) SURPASS hiX 5750 підтримує до 56 інтерфейсів GPON; 5 абонентських терміналів; Обладнання цифрового телебачення і відео за запитом; Приймач-декодер Codico CID-3100; Шлюз DVB IP IVG-7100; Відеосервер VOD MediaBase XMP; STB приймачі; Мережеве обладнання; Модульний комутатор DES 6500 фірми D-Link. Має 8 слотів розширення для модулів.

В експериментальній частині проекту зроблено розрахунок мережі NGN одного мікрорайону міста Києва. Приведено основне вимірювальне обладнання, контрольні точки вимірювань і основні параметри мережі. Ми розрахували кількість абонентів, схему траси прокладки кабелю вибраної ділянки. Розрахували бюджет лінії, розробили загальну схему відгалужень і відзначимо на ній втрати в лінії.

Зробивши економічний аналіз, ми наводимо стрічковий графік, складаємо кошторис витрат на розробку вироби, проводимо розрахунок собівартості дослідного зразка. Загальна сума витрат на виконання робіт з проектування лінії зв'язку включає в себе: Матеріальні витрати; Витрати на оплату праці; Відрахування на соціальні потреби; Амортизація основних фондів; Інші витрати.

У проекті також розглянуті питання забезпечення безпеки життєдіяльності та екологічності проекту, організація праці інженера-розробника.

NGN визначається як концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями щодо їх управління, персоналізації та створенню нових послуг.

УДК 621.396.2 (043.2)

К.В. Севрюгіна
Національний авіаційний університет, м. Київ

УПРАВЛІННЯ ДОСТУПОМ ДО РЕСУРСІВ МЕРЕЖІ LTE

У мережах мобільного зв'язку 4-го покоління LTE для диференціювання послуг, що надаються користувачам, використовується система класів (QoS Class Identifier, QCI), які визначаються на рівні логічного з'єднання (Evolved Packet System Bearer, EPS Bearer). EPS з'єднання являє собою потік IP пакетів, який передається між мережевим шлюзом і терміналом користувача з певними параметрами якості обслуговування. Послуги різних класів відрізняються один від одного наявністю або відсутністю гарантованої швидкості передачі (Guaranteed Bit Rate, GBR), наприклад, голосові послуги і передача даних відповідно, пріоритетами в обслуговуванні (Allocation and Retention Priority, ARP). Відео послуги можуть бути реалізовані на базі кодеків, що дозволяють, при наявності ресурсів передавати інформацію не тільки на гарантованій, але і на максимальній швидкості (Maximum Bit Rate, MBR).

Однією з ключових особливостей мереж зв'язку нового покоління є можливість одночасної підтримки додатків з різними вимогами QoS [1]. Таким чином, для диференціювання послуг, надаваних користувачам мережею LTE, з урахуванням різних пріоритетів і типів логічних з'єднань виділяють 9 QCI класів [2].

Для того, щоб забезпечити дотримання вимог QoS для різних послуг, надаваних користувачу, виникає завдання розрахунку основних показників якості обслуговування, таких як ймовірності блокування, коефіцієнт використання ресурсів мережі, а

також середнє число обслуговуваних користувачів. Окрім дослідження схем управління доступом до радіоресурсів мережі LTE виникають завдання оптимізації потужності або завдання максимізації швидкості передачі, які мають на увазі оптимізацію деякої функції корисності.

Найбільш простим варіантом для дослідження є модель з двома послугами типу GBR – послугою голосової телефонії (QCI = 1, пріоритет 2) і послугою відео телефонії (QCI = 2, пріоритет 4). Голосова телефонія має зарезервований ресурс мережі і у випадку потреби за допомогою витіснення, за рахунок більшого пріоритету (параметр ARP), може використовувати ресурси, призначені для надання відео телефонії.

Схема управління доступом для всіх перелічених в таблиці класів послуг [2] на сьогодні не описана в рекомендаціях консорціуму 3GPP. Тому, є актуальною задача розробки оптимальної схеми управління доступом до радіоресурсів мережі LTE з дев'ятьма класами послуг за критерієм максимізації числа одночасно обслуговуваних користувачів в стільнику і в обмеженнях на значення ймовірностей блокування запитів користувачів на надання тієї чи іншої послуги.

Список літератури

1. *Тихвинский В.О.*, *Терентьев С.В.*, *Юрчук А.Б.* Сети мобильной связи LTE. Технологии и архитектура. – М.: Эко-Трендз, 2010. – 284 с.

2. 3GPP TS 23.203: Policy and charging control architecture: V. 11.4.0. – 2011. – 167 p.

УДК 004.932.72 (043.2)

Т.А. Грищенко
ПАО «КП ВТИ», г. Киев

ВОПРОСЫ ИНТЕГРАЦИИ РАСПРЕДЕЛЕННЫХ БИОМЕТРИЧЕСКИХ СИСТЕМ В ОБЩЕГОСУДАРСТВЕННЫЕ БАЗЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Системы защиты информации, использующие биометрические технологии и алгоритмы сегодня находятся в стадии ин-

тенсивного развития. Диапазон их применения широк. Это разнообразные устройства контроля доступа, учета рабочего времени, банковские системы, Match–on–Card, АДИС, электронные документы и прочее. Учитывая степень востребованности пользователями сервисных функций, предоставляемых такими системами, можно в перспективе прогнозировать дальнейшее расширение спектра их применения.

Постановка задачи

В настоящее время сохранение конфиденциальности информации, хранящейся в базах данных, достигается несколькими основными способами. Ниже они расставлены в порядке убывания эффективности.

1. Изоляция внутренней вычислительной системы от любых электронных каналов передачи данных, выходящих за пределы контролируемой территории, а также теоретически доступных сред передачи данных по ПЭМИН.

2. Создание для обмена данными собственных закрытых сетей, не использующих общедоступные каналы.

3. Применение различных программно-аппаратных средств защиты (шлюзы, брандмауэры, и.т.д.) в комплексе с шифрованием трафика.

Очевидно, что способ (1) дает наивысшую степень защиты, но в современных условиях, требующих распределенного сетевого взаимодействия он неприменим. Для работы в таких условиях может быть использован способ (2) или (3). В реальности можно ориентироваться лишь на использование способа (3), учитывая крайне высокую стоимость, проблемное масштабирование, а также сложность интеграции способа (2) в существующие системы обмена данными.

В недалеком будущем, в связи с внедрением в государственные базы данных биометрической информации, вопросы защиты этих систем будет стоять достаточно остро. Специфика биометрических систем заключается в невозможности замены скомпрометированных данных, вследствие чего степень их защиты вероятно должна соответствовать способу (1). Однако такой способ хранения информации неприменим для биометрического распознавания, которое требует оперативной работы с удаленными интерфейсами. Иными словами, системы биомет-

рической безопасности сами нуждаются в весьма эффективной защите, ввиду крайне высокой ценности информации, хранящейся в них.

В классическом понимании, информационная безопасность – это вопрос баланса. Слишком низкий ее уровень делает информацию уязвимой, но излишний упор на безопасность приводит к снижению скорости обработки информации. Задача, как правило, состоит в нахождении равновесия между защищённостью и эффективностью. Однако в биометрических системах такой подход не приводит к правильному решению. Именно по этой причине в системах электронных документов наблюдается парадокс, когда биометрический загранпаспорт полноценно работает только на территории страны его выпустившей, поскольку международный обмен ключами доступа к защищенной части документа практически отсутствует.

Можно предположить, что существующие в настоящее время системы безопасности не обеспечивают эффективной защиты баз данных, хранящих персональную информацию при работе в распределенных вычислительных средах. С другой стороны возможность интеграции распределенных биометрических интерфейсов может быть существенно ограничена требованиями безопасности этих баз.

Для решения проблемы требуется создание специфических систем безопасности, учитывающих и использующих особенности передачи и обработки биометрической информации для реализации наиболее эффективной ее защиты.

Результаты исследований

В настоящее время автором проводится работа по изучению существующих систем обработки и хранения биометрической информации, а также поиск эффективных методов защиты их уязвимостей. Промежуточные результаты, имеющиеся на сегодняшний день, позволяют сделать вывод о возможности создания комплексной системы безопасности для государственных баз данных с персональной биометрической информацией. Создана концепция для отдельных элементов защиты, позволяющих безопасно работать с удаленными биометрическими интерфейсами по электронным каналам связи.

Автор изначально ставит под сомнение утверждение, что невзламываемых систем информационной безопасности не существует. Примером может служить принцип шифрования Вернама, абсолютная криптографическая стойкость которого до сих пор не опровергнута.

Выводы

Резюмируя суть изложенного выше материала, приходим к выводу, что биометрические технологии – весьма сложный и тонкий инструмент. Потери, обусловленные неправомерным применением или физической опасностью для владельцев защищенных данных, подчас могут быть очень высоки. Компрометация биометрических данных необратима, однако специализированные комплексные способы их защиты до сих пор отсутствуют.

Целью исследований является создание новых методик и подходов к проектированию биометрических систем, в результате применения которых степень безопасности данных, обрабатываемых в этих системах, будет стремиться к абсолютным значениям.

УДК 621.391.31 (043.2)

Є.О. Сокирка
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ ІКМ ПІДПРИЄМСТВА З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ

Будь-яке підприємство, тим паче якщо воно успішно працює і розвивається, має тенденцію до розширення своєї інформаційно-комунікаційної мережі, а саме створення нових робочих місць і як наслідок збільшення навантаження на вже існуючу мережу. Балансування навантаження в мережі є сигналізатором того, що мережа спланована ретельно і її розширення відбувається контрольовано.

Балансування навантаження в мережі здійснюється введенням в мережу між мережним обладнанням та серверами, апаратного розподілювача навантаження (Hardware Load Balancer). Всі запити користувачів, адресовані на певний URL проходять через

розподілювач. До нього підключається група Web-серверів, які ведуть себе, як один сервер. Ця конфігурація називається кластером (cluster). Для всього зовнішнього світу весь кластер серверів має одну IP-адресу. При отриманні TCP/IP пакетів призначених для кластера, розподілювач робить наступне:

- Приймає рішення, якому з серверів кластера слід направити наступний запит.
- Опитує всі сервери і додатки (тобто певний TCP/IP порт) – чи доступні вони.
- Переробляє IP-заголовок пакета так, щоб він пішов певному серверу. Ця переробка називається “перетворенням мережевої адреси” (network address translation).
- Відправляє пакет на сервер.
- Коли сервер відповідає клієнту, розподілювач справляє таке ж перетворення всіх пакетів і повертає їх клієнту. У результаті цього другого перетворення клієнт отримує TCP/IP-пакети в такому вигляді, так якби вони були отримані від певної IP-адреси, яка закріплена за кластером.

Розподілювач навантаження збирає величезну кількість інформації про активність в мережі. У тому числі обсяг трафіку, що йде до сервера або від нього, швидкість, з якою відповідає сервер на TCP/IP запити, кількість з’єднань, яке підтримує в даний момент часу кожен сервер, історія відповідей на попередні запити. У розподілювача навантаження закладено кілька алгоритмів, з яких адміністратор системи може вибирати будь-який. Алгоритми включають в себе і кругове перемикання адрес і пропорційний перебір (круговий перебір адрес з коефіцієнтами). Завдяки цим алгоритмам розподілювач може прийняти “розумне” і ефективне рішення з розподілу навантаження.

УДК 621.3.029.64 (043.2)

Я.О. Козак
Національний авіаційний університет, м. Київ

МЕРЕЖА ПІДПРИЄМСТВА НА БАЗІ СУЧАСНИХ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

Основним напрямком цієї роботи являється розробка бездротової локальної мережі на основі технологій Wi-Fi, ZigBee, Bluetooth.

Однією з найактуальніших послуг для підприємств є корпоративні мережі передачі даних для компаній, що мають розгалужену регіональну мережу офісів. Адже без надійної і швидкої передачі даних між офісами дуже важко налагодити роботу.

Тенденція розвитку сучасних засобів зв'язку така, що основоположними критеріями прогресу є швидкість передачі даних, якість переданої інформації та збільшення її об'єму, а також зручність доступу до неї. Так, сьогодні вже не є фантастикою бездротові засоби зв'язку і робота над їхнім вдосконаленням не стоїть на місці. Сучасні технології бездротової передачі даних активно впроваджуються й широко використовуються як у виробничій діяльності більшості компаній, так і для побудови комп'ютерних мереж для домашнього використання. Нові апаратні рішення в області бездротової передачі даних дозволяють створювати й комп'ютерні мережі в межах одного будинку, і розподілені мережі в масштабах цілого міста.

На сучасному етапі розвитку мережних технологій, безпроводові технології Wi-Fi, ZigBee та Bluetooth є найбільш зручними в умовах потребуючих мобільність, простоту розгортання та використання.

Користувачі в Wi-Fi-, ZigBee-, Bluetooth-мережі, в яких є ноутбук, оснащений вбудованим модулем безпроводового зв'язку, сьогодні вже не прив'язані до проводової локальної обчислювальної мережі, а можуть вільно ходити по кімнатах або переміщатися в сусідній будинок, залишаючись при цьому постійно підключеними до мережі.

Використання роумінгу дозволяє користувачам підтримувати постійне підключення до мережі, перебуваючи в межах зони покриття бездротової мережі. Корпоративні співробітники, які по службовій необхідності роблять регулярні ділові поїздки, розглядають бездротові технології як необхідну складову бізнесу. Бездротові комп'ютерні мережі активно розгортаються в таких громадських місцях, як готелі, транспортні термінали, ресторани, кафе, надаючи відвідувачам доступ до Інтернету. Сумісність бездротової комп'ютерної мережі із проводовою інфраструктурою взагалі не є проблемою, оскільки більшість систем бездротового доступу відповідає галузевим стандартам з'єднання з мережами Ethernet. Низька вартість, швидке розгортання, широкі функціональні можливості по передачі трафіка даних, IP-телефонії, відео – все це робить бездротову технологію одним із найперспективніших телекомунікаційних напрямків.

Метою даної роботи є оцінка існуючих систем бездротових технологій Wi-Fi, ZigBee, Bluetooth, їх захист, економічна оцінка доцільності застосування даних систем в корпоративних мережах.

УДК 004.733 (043.2)

Д.М. Несімока
Національний авіаційний університет, м. Київ

ОПОРНИЙ СЕГМЕНТ МЕРЕЖ WiMAX ДЛЯ МІСЬКИХ УМОВ

В роботі розглянута мережа зв'язку наступного покоління (NGN) – концепція побудови мережі зв'язку, що забезпечує 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 з розподіленою комутацією, винесення функцій надання послуг та інтеграцію з традиційними мережами зв'язку.

В результаті аналізу моделі та загальної архітектури мережі NGN, особливістю якої є те, що передача та маршрутизація па-

кетів і елементи устаткування передачі фізично і логічно відокремлені від пристроїв та логіки керування викликами й послугами, була розглянута архітектура мережевих елементів на базі обладнання компанії «Іскрател Україна» SI3000, яка включає в себе інтегрований сервер обробки викликів (SI3000 iCS), мультисервісний вузол абонентський (SI3000 MSAN) з аналоговими, ADSL2+, VDSL2, WIMAX, Ethernet і оптичними інтерфейсами. Представлені продукти сімейства SI3000 OSAP, які розроблені так, що можуть задовольнити потреби як великих телекомунікаційних операторів, так і операторів невеликих мереж, провайдерів послуг, за допомогою додатків нового покоління. Розглянуто програмний комутатор SI3000 CS, який забезпечує широку пропозицію будь-яких послуг, в основі яких лежить IP-протокол.

Наступним етапом було проведено модернізацію фрагменту міської телефонної мережі при використанні обладнання SI3000, яка включає в себе аналіз вже існуючої телефонної мережі міста. Також було розроблено схему фрагмента міської телефонної мережі на основі технології NGN, і організовано підключення кінцевих користувачів телефонної мережі загального користування за допомогою технології NGN. Був здійснений розрахунок інтенсивності навантаження та ємності пучків з'єднувальних ліній мережі, навантаження від абонентів стільникового рухомого зв'язку та виникаючого місцевого і міжміського навантаження.

В даній роботі спроектована модернізація міської телефонної мережі до мультисервісної мережі на базі обладнання SI3000 з використанням комутації пакетів. Системи управління мультисервісними мережами повинні будуватися за такими ж основними принципами, що і самі мережі, тобто мати модульну архітектуру з використанням відкритих інтерфейсів між модулями.

Важливу роль має організація взаємодії різних операторів постачальників послуг та їх якість, а також можливість взаємодії користувачів із системою управління. В наш час споживач потребує велику кількість послуг, до яких входять телефонія, телебачення, доступ до локальної мережі, доступ до відео зв'язку та таке інше, і щоб користуватися цими видами інформації була створена мережа NGN.

УДК 004.716 (043.2)

Ю.В. Васюков
Національний авіаційний університет, м. Київ

СИСТЕМИ ЗВ'ЯЗКУ З РОЗШИРЕНИМ СПЕКТРОМ СИГНАЛІВ

У теперішній час рівень розвитку мікроелектроніки дозволяє випускати масові дешеві засоби безпровідного зв'язку. Бум стільникового зв'язку, який можна порівняти з зростанням рівня виробництва комп'ютерів, не уповільнюється вже чверть століття. На сьогодні ноутбук, нетбук – звичайні аксесуари великої кількості людей, особливо молоді. А таким персональним засобам необхідна мультимедійна інформація завжди і всюди. Тому зараз поширені стільникові мережі третього покоління 3G, які певною мірою забезпечують роботу комп'ютерів в стільникових мережах. Поширюється впровадження мереж четвертого покоління 4G, які працюють з значно більшими швидкостями і тому розширюють можливості та покращують якість обробки мультимедійної інформації. Системи з розширеним спектром широко застосовуються при побудові систем стільникового зв'язку покоління 3G і 4G.

Мета роботи складається в розробці моделей і алгоритмів оптимального діагностування й оцінювання надійності функціонально-надлишкових систем зв'язку з розширеним спектром сигналів (Bluetooth 3+3).

Об'єктом дослідження є процеси самодіагностування, адаптивної реконфігурації й оцінювання надійності функціонально-надлишкових систем зв'язку з розширеним спектром сигналів (Bluetooth 3+3).

Предметом дослідження обрані моделі й алгоритми оптимального самодіагностування, адаптивної реконфігурації й оцінювання надійності функціонально-надлишкових систем зв'язку з розширеним спектром сигналів (Bluetooth 3+3).

Розроблено програмну модель функціонально-надлишкових систем зв'язку з розширеним спектром (ФНСЗРС-вв-n/m) роботи ФНСЗРС у режимі виявлення несанкціонованих впливів у системі MathCAD. Досліджено працездатність алгоритмів виявлення несанкціонованих впливів на функціонально-надлишкові

системи зв'язку з розширеним спектром для двох сингулярних випадків. У першому сингулярному випадку перевірена працездатність алгоритму при відсутності несанкціонованих впливів. У другому сингулярному випадку виконана перевірка працездатності алгоритму при наявності одного впливу – відмові третього каналу. Розроблено програмну модель ФНСЗРС-ар-n/m роботи системи в режимі самодіагностування й адаптивної реконфігурації в системі MathCAD. Використання цієї моделі дозволило розробити методику експериментів й узагальнені алгоритми самодіагностування, адаптивної реконфігурації, самокорекції перекручених сигналів, автоматичного самовідновлення працездатності уражених впливами функціональних підсистем ФНСЗРС.

УДК 004.735.5 (043.2)

Т.Є. Тимошевська
Національний авіаційний університет, м. Київ

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ НА АВІАПІДПРИЄМСТВІ

В наш час технології хмарних обчислень стають дедалі популярнішими, а концепція хмарних обчислень є однією із самих актуальних тенденцій розвитку інформаційних технологій. Суть концепції хмарних обчислень полягає в наданні кінцевим користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів та програм (враховуючи операційні системи та інфраструктуру) через Інтернет. Багато організацій в наш час реалізовують цю нову технологію, намагаючись зменшити витрати за рахунок віртуалізації машин, меншого часу на адміністрування та зниження витрат на інфраструктуру.

В ході роботи вивчалися поняття «хмарні обчислення» і походження технології, на основі цього визначені всі переваги та недоліки хмарних обчислень, розглянуто структуру та принципи роботи основних моделей надання хмарних послуг, а саме програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS); також були розглянуті такі моделі розгортування як публічна, приватна, гібридна та суспільна хмари; важливим моментом є аспекти безпеки хма-

рних технологій (збереження даних, їх захист при передачі, аутентифікація, ізоляція користувачів, надійне шифрування даних, винайдення способів зниження ризику тощо).

Телекомунікаційні мережі авіапідприємства досить складні і включають в себе багато різноманітних служб та розвинену інфраструктуру мереж. Всі вони мають свої особливості, протоколи передачі і вимоги до якості обслуговування. Тому для того, щоб удосконалити та скоординувати роботу на авіапідприємстві, буде досить доречно використовувати саме хмарні обчислення, враховуючи їх численні переваги: доступність – хмарні обчислення можуть проводитись в будь-якому місці, де є персональний комп'ютер і доступ до інтернету; мобільність – співробітники підприємства мають можливість отримати доступ до робочого місця з будь-якої точки планети; їх відносно низька вартість; надійність, яку забезпечують хмарні обчислення, суттєво вища надійності локальних обчислювальних ресурсів; і одна з найважливіших переваг – велика обчислювальна здатність, що дозволяє зберігати, аналізувати та обробляти величезні об'єми даних.

В результаті було виявлено, що хмарні обчислення характеризуються новими можливостями, такими як самообслуговування, автоматичне масштабування, тим самим базуючись на таких технологіях, як розподілені обчислення, віртуалізація, розподілені сервіси і широкомасштабна автоматизація систем управління. Хмарні обчислення пропонують переваги з боку швидкості і затрат, але викликають багато питань з приводу безпеки, внутрішнього контролю, якості обслуговування тощо. Не дивлячись на все, на даному етапі розвитку хмарні технології активно використовуються для вирішення різних задач у багатьох сферах діяльності.

УДК 004.032.2 (043.2)

А.Ю. Павловський
Національний авіаційний університет, м. Київ

РАДІОПІДСИСТЕМА МОБІЛЬНОЇ МЕРЕЖІ LTE

Найбільш технічно розвинуті країни зараз активно переходять на використання систем 3-го покоління, та в багатьох мережах вже використовуються технології, котрі отримали назву 3,5G. В комерційній експлуатації вже більше 90 відповідних мереж. На думку аналітиків телекомунікаційної індустрії, ряд країн, в котрих нещодавно виникла необхідність впровадження мереж 3-го покоління, сьогодні обирають «стрибок» на покоління уперед, починаючи часткову експлуатацію 4G

Мета роботи: аналіз системи 4-го покоління LTE (Long Term Evolution) як безпосереднього рішення міської безпроводової мережі передачі даних.

Для досягнення мети дослідження були поставлені та вирішені такі основні задачі:

– Аналіз розвитку систем широкосмугового мобільного звяку, причин виникнення систем 4-го покоління та огляд технологій, котрі задовольняють вимогам систем 4-ї генерації зв'язку.

– Обґрунтування основних концепцій технології LTE.

– Аналіз технічних характеристик та методів досягнення цільових показників технології LTE.

– Порівняльний аналіз основних технічних характеристик з вже існуючими стандартами.

Існуючі системи 3GPP (GSM и UMTS/HSPA) та 3GPP2 (CDMA2000 1xRTT, EV-DO) інтегруються в LTE за рахунок використання стандартизованих інтерфейсів, з'єднуючих вузол SGSN (обслуговуючий вузол підтримки GPRS) і удосконалену опорну мережу. Сюди входять інтерфейси з MME для передачі контексту та установки каналів у разі переміщення між технологіями доступу, а також зі шлюзом для встановлення IP-з'єднання з термінальним обладнанням. Таким чином, для терміналів GSM та UMTS/HSPA вузол шлюзу функціонує в якості GGSN (вузла підтримки GPRS). Для систем 3GPP це значить наявність сигнального інтерфейсу між CDMA RAN та новою опо-

рною мережею. Така інтеграція також повинна забезпечити, як дуальний, так і одиночний хендовер викликів, що забезпечить плавну міграцію з мереж CDMA в LTE.

Пропорційно потребам абонентів збагачується різноманітність послуг мобільного широкосмугового зв'язку, що вимагає покращення характеристик існуючого покоління зв'язку в особливості широкої смуги пропускання. Не очікується, що користувач погодиться жертвувати можливостями за додану вартість мобільності – головним чином, навряд буде використовувати стаціонарне обладнання телезв'язку. Тому безпровідна система повинна бути прозорою для користувача і конвергентною із стаціонарною мережею. Персональні безпровідні термінали повинні бути малогабаритними і споживати мінімум енергії.

УДК 004.056.53 (043.2)

А.В. Новікова
Національний авіаційний університет, м. Київ

РЕАЛІЗАЦІЯ ОСНОВНИХ ТИПІВ ФАЙЕРВОЛІВ РІЗНИХ РІВНІВ МОДЕЛІ OSI

Міжмережевий екран або мережевий екран – комплекс апаратних чи програмних засобів, який здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, відповідно до заданих правил.

Однією з прийнятих класифікацій мережевих екранів є поділ їх на типи в залежності від рівня моделі OSI, на якому вони працюють.

Мережеві екрани мережевого рівня, звані також екранами з фільтрацією пакетів (packet filtering firewall), вирішують завдання фільтрації пакетів за IP-адресами і портам додатків на підставі списків доступу. Перевагами брандмауерів мережевого рівня є простота, невисока вартість і мінімальний вплив на продуктивність мережі.

Мережеві екрани сеансового рівня відстежують стан з'єднань. Вони фіксують підозрілу активність, спрямовану на сканування портів і збір іншої інформації про мережу.

Відстеження станів сполук полягає в тому, що мережевий екран перевіряє, наскільки відповідає послідовність обміну повідомленнями контрольованому протоколом. Брандмауери мережевого рівня можуть захищати сервери внутрішньої мережі від різних видів атак, що використовують уразливості протоколів, зокрема від DoS-атак.

Мережеві екрани прикладного рівня здатні інтерпретувати, аналізувати і контролювати вміст повідомлень, якими обмінюються програми. До цього рівню відносять проксі-сервери, які перехоплюють запити клієнтів до зовнішніх серверів з тим, щоб потім відправити їх від свого імені. Цей тип мережевих екранів забезпечує найвищий рівень захисту, хоча і вимагає великих обчислювальних витрат.

Використовувані в мережах протоколи не завжди однозначно відповідають моделі OSI, і тому зазначені екрани можуть відображати і сусідні рівні еталонної моделі, наприклад, шлюз прикладного рівня може зашифровувати повідомлення при їх передачі і розшифровувати прийняті дані. Тоді він функціонує на рівнях представлення даних і прикладному.

Реалізація мережевого екрану так само різноманітна, як і його функціональність. В якості апаратної складової мережевого екрану може виступати маршрутизатор або комбінація маршрутизаторів, комп'ютер або комбінація комп'ютерів і т.д. Такою ж різноманітністю відрізняється і програмна складова мережевого екрану, що має гнучку структуру і включає в себе різні модулі, функції яких можуть широко варіюватися.

Міжмережеві екрани кожного з типів мають свої переваги і недоліки, але надійний захист забезпечують тільки комплексні системи, які об'єднують всі види екранування.

Тільки у випадку якісного налаштування апаратури і програмних модулів мережевий екран дійсно може стати ефективним засобом системи захисту мережі підприємства.

УДК 004.057.4 (043.2)

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

ПРОТОКОЛИ ЗАХИЩЕНОГО КАНАЛУ

Захист даних в мережах доволі важке завдання. Мережі сприйнятливі до великого числа загроз, наприклад, отримання доступу обманним шляхом, втрата секретності, втрата цілісності даних, контроль з'єднання і відмова від обслуговування.

Для забезпечення безпеки даних при їх передачі по публічних мережах використовуються різні технології захищеного каналу. Технологія захищеного каналу забезпечує захист трафіку між двома точками у відкритій транспортній мережі, наприклад в Інтернеті. Захищений канал має на увазі виконання трьох основних функцій:

1) взаємна аутентифікація абонентів при встановленні з'єднання, яка може бути виконана, наприклад, шляхом обміну паролями;

2) захист переданих по каналу повідомлень від несанкціонованого доступу, наприклад, шляхом шифрування;

3) підтвердження цілісності надходять по каналу повідомлень, наприклад, шляхом передачі одночасно з повідомленням його дайджесту.

Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі OSI:

Прикладний	HTTP/S, S/MIME, PGP, SSH
Представлення даних	SSL
Сеансовий	SOCKS
Транспортний	
Мережевий	IPSec, SKIP
Канальний	PPTP, L2TP
Фізичний	

Якщо захист даних здійснюється засобами верхніх рівнів (прикладного, рівня відображення або сеансового), то такий

спосіб захисту не залежить від технологій транспортування даних (IP чи IPX, Ethernet або ATM), що можна вважати безсумнівним достоїнством. У той же час програми при цьому стають залежними від конкретного протоколу захищеного каналу, так як в них повинні бути вбудовані явні виклики функцій захисту протоколу.

Працюючий на мережевому рівні протокол IPSec є компромісним варіантом. З одного боку, він прозорий для додатків, з іншого – може працювати практично у всіх мережах, оскільки заснований на широко розповсюдженому протоколі IP і використовує будь-яку технологію канального рівня.

УДК 654.025 (043.2)

Г.О. Морозова
Національний авіаційний університет, м. Київ

ВІДОМЧА СИСТЕМА ЗВ'ЯЗКУ НА БАЗІ ОБЛАДНАННЯ GOODWIN SPREE

Сучасні тенденції розвитку засобів телекомунікацій характеризуються все більш зростаючим використанням мобільних телефонів в різних сферах діяльності. Аналіз тенденцій розвитку мобільних систем зв'язку показує, що існуючі системи мобільного зв'язку у великих містах вже не справляються з навантаженням. Дуже часто присутній дефіцит частотного і просторового ресурсу. Крім того, розподіл трафіку в містах, як правило, нерівномірний. Є місця великого скупчення людей, такі як ринки, стадіони, великі підприємства, організації, в яких потреба в телефонному зв'язку дуже велика. Для організації зв'язку в місцях з підвищеним трафіком все частіше використовують системи мінісотового зв'язку. Серед усіх відомих систем мінісотового зв'язку найбільшого поширення набула система стандарту DECT. В основному система стандарту DECT аналогічна системі мобільного телефонного зв'язку, відрізняючись лише набагато меншим розміром сот (пікосоти), що дозволяє працювати при набагато більш високій щільності користувачів, ніж у мобільних системах.

В даній роботі було запропоновано застосування системи Goodwin SPREE в аеропорті. Впровадив дану систему ми змогли встановити голосовий зв'язок через дротові і бездротові телефони, гучномовно оповіщувати через гучномовці та бездротові телефони, змогли використовувати попереджувальну сигналізацію і дані про місцеположення через бездротові телефони і індивідуальні мітки, а також мати можливість отримувати дані телеметрії через бездротові модулі, які підключені до датчиків, що вимірює концентрацію газу, тиск та температуру.

Саме за допомогою системи Goodwin SPREE ми отримали можливість застосування систем зв'язку у підземних і наземних транспортних спорудах як на етапі будівництва, так і в період експлуатації аеропорта, маємо оперативність прийняття рішень і мобільність співробітників, безпеку, надійність і стійкість зв'язку при максимальній зручності користування. Система, що ми впровадили також виконує специфічні вимоги з боку систем диспетчерського зв'язку. Система Goodwin SPREE при провадженні в аеропорті оптимізує фінансові затрати невисокою вартість базового та абонентського обладнання, скорочення витрат на прокладку і вміст лінійно-кабельних споруд; надійністю обладнання, високою керованістю і можливістю віддаленого технічного обслуговування системи через мережу передачі даних: безкоштовним внутрішнім зв'язком без виходу на міську лінію, можливістю обмеження доступу співробітників до міських телефонних ліній.

Goodwin SPREE – це більше, ніж просто телефонна система, що одночасно є і цифровою, і сумісною з аналоговими мережами системою, вона дозволяє ефективно вирішувати усі питання, що виникають при організації раціональної комунікації на малих та середніх підприємствах. Система може легко, майже непомітно нарощуватися до 14/96 точок підключення, і побудована таким чином, що з безлічі можливостей що представляються для обробки мовного сигналу, зображення, текстової інформації і даних завжди можна вибрати оптимальний варіант для даного робочого місця. При цьому одна телефонна система забезпечує необхідні конфігурації "шеф-секретар", режим опитування викликів, індивідуальну роботу та в групі – Team, а також мобільні робочі місця.

УДК 621.3.029.64 (043.2)

Д.М. Москвич
Національний авіаційний університет, м. Київ

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА ЧЕТВЕРТОГО ПОКОЛІННЯ ІЗ ЗАДАНИМ РІВНЕМ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ

Сучасні тенденції розвитку телекомунікацій пов'язані з появою нових послуг та сервісів, що є більш вимогливими до існуючих мереж. З кожним днем ці послуги стають більш актуальними серед користувачів. Таким чином побудова, сучасної мультисервісної бездротової мережі є дуже вигідним рішенням для існуючих провайдерів, як результат – залучення ще більшої кількості абонентів, а значить й збільшення прибутків. За останні роки розвиток мережних технологій привів до значного розширення списку й можливих способів об'єднання персональних комп'ютерів у мережі, і видів підключень до глобальної мережі Інтернет. Технології WI-MAX (англ. Worldwide Interoperability for Microwave Access) та LTE, які будуть далі розглядатися детальніше в роботі, належать до найсучасніших розробок в області телекомунікацій останнього на даних момент покоління технологій мобільного зв'язку 4G.

Об'єктом дослідження даної роботи є процес надання послуг в мережах четвертого покоління.

Предметом дослідження є якість обслуговування абонентів мереж четвертого покоління.

Можна виділити основні особливості передачі даних по мережі зв'язку і вони полягають у наступному:

• потрібна висока вірогідність передачі, не допускаються вставки і випадання окремих порцій інформації. Необхідно застосовувати надійні способи виявлення помилок і повторної передачі відповідних блоків даних;

• відсутні жорсткі вимоги до величини постійної затримки інформації в мережі і до її дисперсії, хоча для деяких інтерактивних програм можуть існувати обмеження на транзитну затримку, обумовлені вимогами часу відгуку;

• допускається довільні і незалежні темпи передачі і прийому даних в мережі;

• потрібна організація багаторежимного обміну даними (діалогова передача, передача файлів тощо) і розгалужена система пріоритетів;

• канали зв'язку використовуються, як правило, високої якості з ймовірністю помилки не нижче 10^{-4};

• вимоги до ширини смуги пропускання лежать в широких діапазонах: від десятків кбіт/с для низькошвидкісних інтерактивних додатків до тисяч Мбіт/с для додатків, орієнтованих на роботу з графічними даними.

Розглянуті технології четвертого покоління поки що не в змозі задовольнити всіх вищенаведених вимог, тому необхідною є побудова такої мережі, де якість обслуговування абонентів буде на досить високому рівні. Це і пропонується зробити в рамках даної роботи.

УДК 004.715 (043.2)

С.Г. Синьогуб
Національний авіаційний університет, м. Київ

СТВОРЕННЯ МЕХАНІЗМІВ НАЛАШТУВАННЯ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ МАРШРУТИЗАТОРІВ CISCO

В роботі досліджено основні механізми налаштування протоколів динамічної маршрутизації на маршрутизаторах компанії CISCO. Це один із лідерів на ринку телекомунікаційного обладнання, яке має високу надійність і функціональність. Обладнання працює на власній операційній системі IOS (Internetwork Operating System – Міжмережева Операційна Система), яка постійно оновлюється із додаванням нових можливостей для обладнання. Комп'ютерна мережа, спроектована з використанням обладнання CISCO, володіє високим рівнем надійності і захищеності від несанкціонованого доступу з метою порушення роботи мережі та викрадення даних.

За основу було взято дві спроектовані мережі з довільними топологіями та адресами. У першій мережі за замовчуванням на всіх маршрутизаторах налаштовано протокол маршрутизації RIP (використовується для автоматичного обміну маршрутами між

маршрутизаторами невеликих мереж до 15 вузлів), а у іншій – OSPF (використовується для обміну маршрутною інформацією між маршрутизаторами у великих мережах без обмеження кількості вузлів).

У зв'язку із відсутністю доступу до необхідного обладнання для відображення процесу конфігурації використовувалася програма Cisco Packet Tracer (симулятор для повноцінного проектування та налаштування комп'ютерних мереж на базі обладнання CISCO у віртуальному середовищі).

У кожній мережі було обрано маршрутизатори, які найкраще підходили для ілюстрації особливостей процесу налаштування протоколів маршрутизації. Конфігурування здійснюється за допомогою команд, що вводяться у інтерфейсі командної строки (CLI – Command line interface). У зв'язку з цим було проведено аналіз особливостей налаштування пристроїв CISCO. Коротко розглянуто механізми функціонування протоколів, на роботу з якими налаштовуються маршрутизатори. Розглянуто особливості підготовки обладнання та необхідних даних для правильного налаштування маршрутизаторів. Створена покрокова методика налаштування протоколів маршрутизації RIP та OSPF. Приведені приклади із розгорнутими поясненнями команд, які виконуються на маршрутизаторах, та їх графічним зображенням у інтерфейсі командної строки маршрутизатора.

У результаті дослідження основних механізмів, принципів та особливостей конфігурації телекомунікаційного обладнання CISCO, була створена спрощена методика налаштування протоколів динамічної маршрутизації RIP та OSPF. Керуючись цією методикою, користувач, із певними навичками роботи із комп'ютерним та телекомунікаційним обладнанням і розумінням технологій комп'ютерних мереж та протоколів, зможе здійснити налаштування будь-якого маршрутизатора компанії CISCO.

УДК 004.056.53 (043.2)

Є.О. Шовковий
Національний авіаційний університет, м. Київ

СИСТЕМИ ЗАХИСТУ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Стрімкий розвиток у галузі бездротового зв'язку призвів до ситуації, коли тотальна більшість сеансів обміну інформацією відбувається саме за допомогою засобів стільникового зв'язку. За допомогою мобільного телефону ми обговорюємо як звичайні побутові питання, так і певні конфіденційні дані, які можуть становити неабиякий інтерес зі сторони різного роду зловмисників (конкурентів, шпигунів і т.д.). Тому не дивно, що увага до питання конфіденційності зв'язку невпинно зростає. На сьогоднішній день існує декілька стандартів мобільного зв'язку, які по-різному вирішують задачу захисту даних абонента.

Мета роботи полягає в розробці ефективної системи захисту мобільного зв'язку від несанкціонованого доступу.

Об'єктом дослідження є процеси ідентифікації та аутентифікації абонента, а також механізми шифрування мовного сигналу.

Предметом дослідження обрані моделі й алгоритми шифрування мовного сигналу, механізми ідентифікації та аутентифікації абонента.

Досліджено процес ідентифікації та аутентифікації абонента, процедура шифрування даних абонента в стандарті GSM, для забезпечення надійної системи захисту мобільної мережі зв'язку від несанкціонованого доступу. Досліджено варіанти алгоритму шифрування А5 (А5/1, А5/2, А5/3). Детально досліджений алгоритм шифрування А5/3, який використовуються в стандарті GSM.

УДК 621.396.2 (043.2)

А.И. Антух
Национальный авиационный университет, г. Киев

МЕТОДИКА ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОЙ ТОПОЛОГИИ СЕТИ GSM ДЛЯ ГОРОДСКОГО МИКРОРАЙОНА

При проектировании мобильных систем связи необходимо решать задачу оптимизации положения базовых станций в зоне обслуживания. Оптимальным считается такое положение, при котором заданный уровень качества сигнала обеспечивается в любой точке зоны обслуживания при минимальном числе базовых станций В условиях урбанистической застройки задача определения сигнала в точке приема существенно усложняется, поскольку приходится учитывать дополнительные сигналы, переотраженные от объектов застройки.

Целью данной работы является создание алгоритма оптимального размещения базовых станций сети мобильной связи стандарта GSM. Положение базовых станций определяется исходя из условия обеспечения заданного уровня сигнала в каждой точке зоны обслуживания.

Первым шагом в алгоритме является анализ существующих моделей распространения радиоволн и выбор наиболее оптимальной (подходящей) модели для заданной территории. По результатам анализа была выбрана модель Уолфиша-Икегами, которая хорошо подходит для густонаселенной урбанистической местности и учитывает направления прихода радиоволн. Модель Уолфиша-Икегами, в отличие от остальных, учитывает возможность прихода волны в точку приема несколькими маршрутами с последующим сложением. Однако, данная модель требует большего количества информации, по сравнению с другими существующими моделями, такими как модели Окумура и Хата.

При расчете покрытия сети GSM для городского микрорайона необходимо учитывать ограничения, которые влияют на радиус покрытия. Для линии “downlink” главным ограничением является мощность передатчика базовой станции, иногда значительно уменьшаемая за счет потерь в антенно-фидерном устрой-

стве (АФУ). На линии “uplink” ограничением для увеличения радиуса соты является недостаточная чувствительность приемника. Следовательно, искомое решение должно учитывать сбалансированность мощности на линии “uplink” и “downlink”.

Вторым шагом в алгоритме будет расчет баланса мощностей линии “downlink” и линии “uplink”.

Третий шаг алгоритма – расчет радиуса соты.

На четвертом этапе выбирается оборудование, которое обеспечивает максимальный радиус соты. Здесь же и рассчитывается предварительное количество базовых станций, необходимое для покрытия района.

На пятом этапе определяется такое положение базовых станций в зоне обслуживания, при котором площадь теневых зон оказывается минимальной.

Таким образом, после проведения расчетов и получения результатов по приведенному алгоритму можно предложить рекомендации для получения оптимального покрытия городского микрорайона областного центра Украины, которые будут включать топологию размещения базовых станций в микрорайоне, обеспечивающих заданный уровень качества сигнала в любой точке зоны обслуживания, а также параметры оборудования базовых станций.

УДК 621.396.49 (043.2)

П.О. Рибак
Національний авіаційний університет, м. Київ

ОЦІНКА ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ СУПУТНИКОВИХ МЕРЕЖ ЗВ’ЯЗКУ

Супутниковий зв’язок широко поширений у світі і використовується для створення міжнародних і національних мереж зв’язку. Супутниковий зв’язок – економічно доцільний вид міжконтинентального зв’язку та зв’язку з віддаленими регіонами. Сучасні технології супутникових телекомунікацій забезпечують велику гнучкість при створенні мереж відомчого та ділового зв’язку в інтересах державних та комерційних структур, при організації некомутованих каналів для побудови комп’ютерних

мереж на великих територіях (технології VSAT), забезпечують можливість надавати водночас кілька видів послуг за допомогою однієї станції супутникового зв'язку (передавання даних, двосторонній телефонний, відеоконференцзв'язок тощо).

На теперішній час у космосі розгорнута велика кількість систем зв'язку з штучними супутниками Землі (ШСЗ), які мають глобальну, регіональну або національні зони обслуговування. При цьому для надання різних телекомунікаційних послуг використовуються певні орбіти та діапазони частот.

При зв'язку з мобільними абонентами дуже ускладнюються процеси відслідковування ретранслятора, електромагнітна сумісність станцій з іншими наземними радіослужбами, виникає можливість блокування радіотрас місцевими предметами і перерви в радіозв'язку. У таких умовах динамічною зміни електромагнітної обстановки необхідні спеціальні заходи для забезпечення завадостійкості. Це говорить про те, що технологія мобільних систем зв'язку (МСЗ) є однією з найбільш складних серед інших супутникових служб.

Зазвичай, до складу супутникової системи зв'язку (ССЗ) входять:

- Космічний сегмент, до якого належать декілька штучних супутників ретрансляторів (ШСР);
- Наземний сегмент, до якого входять центр керування системою (ЦКС), центр запуску ШСЗ, командно-вимірювальні станції, центр керування зв'язком та шлюзові наземні земні станції (GES – Ground Earth System);
- Абонентський сегмент (сегмент користувача), до якого в AMSS входять авіаційні (бортові) земні станції (AES – Airborne Earth Station);
- Наземні мережі зв'язку, які базуються на відомчих каналах або каналах загального користування і до яких через відповідні інтерфейси підключаються GES.

Всі види послуг ССЗ можна узагальнити в три супутникові служби за типом земної станції. Це такі супутникові служби: фіксовані (FSS – Fixed Satellite Services), рухомі (MSS – Mobile Satellite Services), радіомовні (BSS – Broadcast Satellite Services).

УДК 004.451.9 (043.2)

А.К. Суман
Национальный авиационный университет, г. Киев

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ДОСТУПА К СЕРВЕРУ НА БАЗЕ ОС MICROSOFT WINDOWS SERVER 2008

В современном мире приходиться регулярно сталкиваться с проблемами растущих потребностей бизнеса. Организации требуется круглосуточная работоспособность, возможность удаленного доступа к серверам, при этом необходим высокий уровень безопасности. Каждый день рекламодатели пытаются проникнуть в сети, чтобы взломать сервера, инфицировать их вирусами или изъять информацию о клиентах и служащих. Угроза поступает как от служащих, находящихся внутри сети и посещающих Веб-сайты, инфицированные вредоносными программами, внешних подключений пользователей через виртуальные частные сети (virtual private networks, VPNs), подключений сети филиала к серверам предприятия, так и от прямых нападок на уязвимые компьютеры или серверы сети. Windows Server 2008 с самого начала разрабатывалась с учетом вопросов безопасности и предлагает целый ряд новых и улучшенных технологий и компонентов, которые обеспечивают надежную базу для ведения и построения бизнеса.

Новые возможности, такие как технология PatchGuard, позволяют уменьшить контактную зону ядра и повысить безопасность и стабильность серверной среды. Ограниченный режим служб Windows предотвращает нарушение работы критически важных серверных служб аномальной активностью в файловой системе, реестре или сети, и способствует обеспечению стабильной работы систем. Такие технологии, как защита доступа к сети(NAP), которая позволяет с помощью правил предоставлять вход только тем клиентам, которые отвечают предварительно заданным критериям безопасности, а в случае отрицательного ответа сервер VPN отказывает в соединении (эту функцию поддерживают серверы DHCP, коммутаторы и терминальные серверы); контроллер домена только для чтения (RODC); улучшения в инфраструктуре открытого ключа (PKI); ограниченный

режим работы служб Windows; поддержка криптографии нового поколения, также усиливают защищенность операционной системы Windows Server 2008. Новый брандмауэр Windows контролирует не только входящий, но и исходящий сетевой трафик. Сетевой администратор может настроить исключения, блокирующие все пакеты, отправляемые на определенные порты. По умолчанию брандмауэр Windows Server 2008 ограничивает любой входящий сетевой трафик, кроме случаев, когда он вызван запросами или для него настроено исключение. Большинство серверных ролей автоматически вносят свои исключения.

Рекомендации на счет использования ОС Windows Server 2008 для предприятия помогут в организации защищенного доступа к серверу и его безопасного эксплуатирования. Помогут в настройке служб сертификации Active Directory и Web Server, служб Политики сети и доступа, создания и настройки сервера Аутентификации сертификатов, настройка Network Policy Server (NPS). Результаты работы помогут в выборе сервера, количестве и пропускной способности каналов, дадут возможность расчитать возможное время задержки, коефициент использования канала и его пропускной способности между сервером и пользователем для операционной системы Windows Server 2008.

УДК 004.724.4 (043.2)

Н.О. Зінченко
Національний авіаційний університет, м. Київ

ПРОЕКТУВАННЯ ОБЛАДНАННЯ ДЛЯ ПЕРЕДАВАННЯ МОВНОГО ТРАФІКУ КАНАЛАМИ ПАКЕТНОЇ МЕРЕЖІ

У роботі досліджено обладнання IP-телефонії, яке використовується для передавання мовного трафіку і забезпечує реалізацію IP послуг каналами пакетної мережі. IP-телефонія (або VoIP – Voice over Internet protocol) – технологія, яка використовує мережу з пакетною комутацією повідомлень на базі протоколу IP для передачі голосу в режимі реального часу.

В такій мережі увесь трафік передається у вигляді пакетів змінної довжини, які містять заголовок та інформаційну части-

ну. У заголовку кожного пакета міститься вся інформація, яка необхідна для маршрутизації пакета по мережі, причому для передачі не потрібно встановлювати ніякого мережного з'єднання між задіяними в комунікації кінцевими пунктами.

За встановленими характеристиками обладнання було здійснено вибір параметрів для пакетної мережі, що будуть гарантувати передавання мовного трафіку за визначеними показниками якості, таких як затримка, показник розбірливості мови та певного рівня гучності та якості сигналізації, включаючи можливості встановлення виклику, завершення виклику, функції DTMF (Dual-Tone Multi-Frequency – двотональний багаточастотний аналоговий сигнал). За методику дослідження була обрана теорія інженерії трафіка.

Пакетна мережа включає в себе обладнання у складі маршрутизаторів та каналів транспортування даних, що реалізує стек протоколів TCP/IP у режимі із встановленням з'єднань. IP-телефонія реалізується за протоколом SIP.

Протокол ініціювання сеансів (Session Initiation Protocol – SIP) є протоколом прикладного рівня і призначений для організації, модифікації й завершення сеансів зв'язку (наприклад, мультимедійних конференцій, телефонних з'єднань). Користувачі можуть брати участь в існуючих сеансах зв'язку, запрошувати інших користувачів і бути запрошеними ними до нового сеансу зв'язку. Протокол SIP розроблений групою MMUSIC комітету IETF, а специфікації протоколу представлені в документі RFC 2543.

Далі здійснюється проектування показників обладнання, що впливають на якість транспортування мовного трафіку каналами пакетної мережі. А саме вибір показників функціональності QoS (Quality of Service – Якість послуги) та NP (Network Performance – Досконаліть мережі), нормативи якості передавання мовного трафіку, обгрунтування обраних значень показників якості передавання голосового трафіка та умови і порядок вимірювань показників якості транспортування мовного трафіку.

У результаті виконаного дослідження характеристик мережі з пакетною комутацією IP, визначення її можливостей був складений проект обладнання для передавання мовного трафіку. Та-

ке обладнання разом з мережею задовольняє усім технічним вимогам, що забезпечують його використання в режимі надання послуг IP-телефонії.

УДК 00.004.735 (043.2)

Д.А. Кононенко
Національний авіаційний університет, м. Київ

РОЗРОБКА ЛАБОРАТОРНИХ РОБІТ З ДИСЦИПЛІНИ «ВОЛОКОННО-ОПТИЧНІ СИСТЕМИ ПЕРЕДАЧІ»

Починаючи від часу становлення волоконної оптики основною областю її застосування є системи оптичного зв'язку. Перші комерційні волоконно-оптичні телефонні системи були встановлені у квітні 1977 року компаніями AT&T і GTE (General Telephone and Electronics). Перевершивши за своїми характеристиками всі існуючі на той час стандарти, вони дуже швидко набули широкого використання. Більше мільйона телефонних розмов сьогодні можна одночасно передавати через одне оптичне волокно. Поява всесвітньої мережі "Інтернет" та постійно зростаюча потреба в інформаційній пропускній здатності каналів зв'язку посприяли ще більшому розвитку і використанню волоконної оптики в системах передачі даних.

Волоконно-оптичні системи передачі на сьогоднішній день утримують першість в побудові високошвидкісних магістральних ліній зв'язку. Це пояснюється беззаперечними перевагами оптичного кабелю над давно застарілим мідним. Науково-методичних робіт, присвячених цьому питанню на сьогодні є багато, як зарубіжних, так і вітчизняних. Але лабораторних робіт на українській мові, які можна було б застосувати в навчальному процесі ВНЗ – на жаль, недостатньо. Тому, я вважаю, що це питання є актуальним, а отже заслуговує достатньої уваги. З допомогою дипломного керівника були розроблені лабораторні роботи для дисципліни «Волоконно-оптичні системи передачі» за наступними темами:

1. «Оптичне волокно та його характеристики»
2. «Параметри ВОСП»

3. «Методи вимірювання параметрів волоконно-оптичного кабелю»

4. «QoS для волоконно-оптичних систем передачі».

Також, в роботі були досліджені технології передачі даних, які працюють з оптичними волокнами (ATM, SONET/SDH, PDH, WDM). Викладені основні методи мультиплексування/демультиплексування даних, структура мереж, побудованих за даними технологіями, формати кадрів (комірок, потоків, фреймів), ієрархія швидкостей, інтерфейси та ін. Були розглянуті міжмодова, хроматична, поляризаційна дисперсії притаманні волоконно-оптичним лініям зв'язку, та методи їх подолання. Багато уваги приділено найпрогресивнішій, на мою думку, технології ущільнення за довжинами хвиль – WDM, та зокрема підвиду цієї технології – DWDM. За допомогою цієї технології можна ущільнити до сорока каналів, з пропускною здатністю кожного до 10 Гбіт/с. В роботі розглянуто пасивне і активне оптичне обладнання найвідоміших компаній-виробників, таких як Lucent Technologies, AT&T, Alcatel та ін.

Задача передачі інформації на великі відстані виникла дуже давно. В кожен період часу вона вирішувалась по різному. Але спільною тенденцією стало збільшення об'ємів передаваних даних. Збільшення пропускної здатності і швидкості передачі даних відбуваються завдяки постійному вдосконалюванню елементної бази компонентів волоконно-оптичних систем зв'язку. Сучасний спеціаліст з телекомунікацій, для того, щоб створювати реальну конкуренцію на ринку праці, має чітко орієнтуватися в нових технологіях волоконно-оптичних систем передачі, знати основні принципи та постулати. Я надіюсь, що моя робота допоможе майбутнім спеціалістам у цьому.

УДК 004.051 (043.2)

К.В. Величко
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ СТРУКТУРИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

По мірі розвитку компанії у керівництва обов'язково виникають питання: створення максимально гнучкої та ефективної системи управління підприємством, офісними майданчиками, створення єдиної системи документообігу, оперативного збору інформації та звітів зі складів і виробничих майданчиків, централізація інформаційно-фінансових потоків. Правильне вирішення цих питань дозволяє успішно керувати компанією в цілому, робить її гнучкою і забезпечує динамічний розвиток. Світовий досвід великих компаній і корпорацій говорить про те, що таким рішенням є створення корпоративної мережі передачі даних. Корпоративна мережа є складною системою, яка включає тисячі різноманітних компонентів: комп'ютери різних типів від настільних до мейнфреймів, системне та прикладне програмне забезпечення, мережні адаптери, концентратори, комутатори та маршрутизатори, кабельну систему. Працівники підприємства одночасно здійснюють дзвінки, відео конференції, користуються електронною поштою та базами даних.

Головним питанням залишається які все ж таки технології вибрати при проектуванні своєї мережі, яким виробникам програмного та апаратного забезпечення довірити передачу даних, та послугами яких провайдерів скористатись, адже правильно спроектована структура корпоративної мережі веде до досягнення максимальної ефективності роботи кожного з працівників та підприємства в цілому.

В залежності від поставленого завдання і цілі, методи створення локальної мережі підприємства (корпоративної мережі) можуть бути різними. Найчастіше саме комбінація різних технологічних рішень дозволяє досягти оптимального рішення. У кожного із методів є свої переваги і недоліки.

Завданням мого дослідження було дослідити існуючі технології корпоративних мереж, переваги та недоліки кожної з них, та визначити альтернативне рішення опираючись на потре-

би конкретного підприємства. В роботі наведені порівняльні характеристики технологій віртуальних мереж, передачі даних, виробників програмно-апаратного забезпечення, з допомогою яких було прийняте оптимальне рішення для проектування мережі.

Після проведення досліджень, розрахунків та порівняння існуючих технологій було досягнуто висновку, що оптимізація структури підприємства полягатиме у переході на систему уніфікованих комунікацій, що значним чином покращить ефективність роботи, знизить вартість обслуговування мережі. Дане рішення об'єднало телефонію, електронну пошту, аудіо конференцзв'язок, обмін повідомленнями та даними, голосові повідомлення та веб-співробітництво в єдину комунікаційну платформу, що дало змогу досягти бажаного результату в оптимізації роботи підприємства.

УДК 621.395.4 (043.2)

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

РАЙОНОВАНА МІСЬКА ТЕЛЕФОННА МЕРЕЖА В м. ПИРЯТИН

Місцеві телефонні мережі як елемент найближчими роками розвиватимуться на базі цифрового устаткування комутації і цифрових систем передачі, що забезпечують роботу всіх видів зв'язку.

Нові можливості цифрових комутаторів і технічних засобів транспортного середовища пред'являють нові вимоги до планування і проектування сільської телефонної мережі. Одним з складних завдань є забезпечення в перехідний період спільної роботи на СТМ аналогового і цифрового устаткування. Сучасні мережі повинні бути цифровими, мати гнучку, легко керовану структуру. Електронні системи комутації володіють значними перевагами і новими можливостями в порівнянні з електромеханічними:

– велика ємність станцій;
– мала займана площа;

– висока надійність;

– можливість аналізу будь-якого числа цифр номера;

– можливість централізованого управління і інше.

У даному проекті було розглянуто питання побудови сільської телефонної мережі на базі автоматичної телефонної станції AXE-10. Було зроблено проект станційних споруджень центральної станції сільської телефонної мережі (СТМ) AXE-10.

Для цього потрібно знати принципи побудови СТМ; способи передачі сигналів управління; типи систем передачі використаних на сільських мережах; технічну характеристику системи AXE-10 в цілому і окремих її модулів; методи розрахунків інтенсивності телефонного навантаження на станції і на мережі; методи розрахунків станційного і лінійного обладнання АТС.

Було розглянуто принципи побудови телефонної мережі в сільській місцевості, оскільки на сьогоднішній день в сільській місцевості рівень телефонізації в декілька раз нижчий, ніж в місті. В першу чергу це пояснюється збитковістю сільського телефонного зв'язку (СТС), основними причинами якого є: віддаленість частини абонентів від АТС, внаслідок чого витрати на її експлуатацію і розвиток в три і сім разів перевищують середньорічні доходи; нечисленність абонентських груп; складність прогнозування зростання ємкості в населених пунктах, а також інші чинники, не сприяючі зацікавленості операторів зв'язку в розвитку СТС.

Для проектування даної мережі було вибрано АТС AXE-10. Будучи встановленими в 86 країнах загальним обсягом більше 55 мільйонів ліній, АТС AXE-10 продемонстрували свою пристосованість до різного оточення, починаючи із густонаселених міських районів, що вимагають використання АТС великої ємності, і закінчуючи віддаленими районами з малою щільністю населення, в яких АТС малої ємності поєднуються із віддаленими абонентськими концентраторами, реалізовуючи недорогу цифрову мережу. AXE-10 заснована на відкритій модульній розподіленій архітектурі, що забезпечує підвищену гнучкість і що допускає ефективну реалізацію сучасних технологічних рішень в області компонентів і програмного забезпечення.

Також було розглянуто надійність та експлуатацію даної системи.

УДК 621.396.93 (043.2)

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

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ МЕРЕЖ LTE

На сьогоднішній день Україна має у своєму розпорядженні зовнішні канали зв'язку з достатньою пропускною здатністю, практично в кожному населеному пункті є провайдери послуг доступу в зовнішню мережу, проте, з'єднання між ними і кінцевим споживачем дотепер здійснюється переважно або по комутованих або по виділених лініях. Як результат – низька швидкість обміну інформацією, ненадійність з'єднання, обмежені можливості підключення. Важливою проблемою є прокладка кабельних ліній, іноді вона неможлива, незручна й економічно недоцільна, особливо у великих містах. Актуальністю даної теми є пошук рішень щодо впровадження нових технологій в сучасні телекомунікаційні мережі.

Об'єктом дослідження даної роботи є сегмент мережі LTE в Печерському районі міста Київ.

Предметом дослідження є розробка та побудова мережі LTE в Печерському районі міста Київ . Основною вимогою для проектування такої мережі є вибір найбільш вигідною і якісної технології передачі даних. Останнім часом у сфері телекомунікації все більше уваги стали приділяти технологіям 4 покоління, які мають кращі, в порівнянні з попередніми поколіннями, характеристики якості, швидкості передачі даних і більший спектр послуг. Однією з таких технологій є технологія LTE.

Таким чином , можна сформулювати мету даної роботи, яка полягає в створенні мобільної мережі з надійним радіопокриттям, якісно новими послугами, низькими затримками і високою пропускною здатністю, обґрунтування необхідності впровадження технології LTE, пошуку економічно обґрунтованого рішення для впровадження технології LTE

В результаті проведених досліджень був спроектуваний сегмент мережі LTE, за рахунок введення його в експлуатацію ми збільшимо дохід компанії стільникового зв'язку в кілька разів. Рівень прибутку стільникових компаній від передачі голосу

практично досяг своєї межі і необхідні нові шляхи збільшення прибутку. Тим самим збільшивши швидкості передачі даних через мережу і число надаваних послуг, і зменшивши вартість на їх використання хоча б на 5% ми збільшимо частку прибутку від передачі трафіку в 3 рази мінімум. Тому, розвиток в напрямку переходу до нових швидкісних технологій передачі даних є найбільш ефективним способом приросту прибутку стільникових операторів зв'язку. Ми використали вкрай гнучке устаткування, яке дозволить забезпечити подальшу еволюцію бездротових мереж передачі даних. Тим самим впровадження мереж четвертого покоління в значній мірі збільшить швидкості передачі даних, що відкриє користувачам такі можливості як: надання послуг мультимедіа в рамках глобальної інформаційної інфраструктури; передачу даних по радіоканалу і по мережах фіксованого зв'язку з однаковою швидкістю передачі в каналі до 150 Мбіт/с; підтримку асиметричності трафіку по каналах; реалізація послуг Інтернет в повному обсязі.

УДК 621.395.4 (043.2)

Р.С. Сачук
Національний авіаційний університет, м. Київ

ТЕЛЕФОННА МЕРЕЖА м. БІЛА ЦЕРКВА

Робота присвячена проектуванню міської телефонної мережі м. Біла Церква, на базі цифрової системи комутації «DX-200». Засоби зв'язку відіграють важливу роль в задоволенні зростаючих проблем населення. Мережа електрозв'язку являє собою складний комплекс пристроїв, які забезпечують передачу та розподілення між споживачами різного виду інформації: телефонних переговорів, телеграм, передача даних для ЕОМ, передача програм радіомовлення та телебачення. Збільшення об'єму інформації, яка передається, і появлення її нових видів потребує підвищення технічного рівня засобів електрозв'язку шляхом впровадження нових досягнень науки і техніки, а також об'єднання всіх засобів електрозв'язку з метою підвищення її використання, організаційно і технічно об'єднуючи в єдиний комплекс.

У ході роботи було розглянуто телефонні мережі та їх класифікацію, проаналізовані технічні характеристики обладнання цифрової системи комутації «DX-200». Розглянута структура апаратних коштів та програмного забезпечення, описані основні блоки та структурні одиниці, а саме: загальна кількість абонентських ліній, які включаються в АТС – 100000, загальна кількість з'єднувальних ліній, які включаються в АТС – 57000, загальна пропускна здатність – 22800 Ерл, потужність ліній, що споживається – 1 Вт, апаратні відмови/рік/10000 ліній – 50. Також розглянули структуру організації міського телефонного зв'язку м. Біла Церква, зобразили спосіб зв'язку «DX-200» з іншими діючими АТС міста. Встановлені та проаналізовані технічні характеристики встаткування «DX-200», структура апаратних засобів, описані основні блоки та структурні одиниці, розглянутий алгоритм встановлення внутрішньостанційного з'єднання на ЕАТС «DX-200». Зроблений розрахунок абонентського навантаження та розподіл навантажень в усіх напрямках. За результатами розрахунків був зроблений розрахунок устаткування на даній АТС. Також були розглянуті питання, пов'язані з експлуатацією і технічним обслуговуванням даного об'єкта. Були враховані наступні позитивні якості, властиві АТС даного типу: висока сумісність із різними типами існуючих станцій; висока надійність та ремонтопридатність; наявність відпрацьованого програмного забезпечення; прийнятна вартість, порівняна з вартістю станцій інших типів.

Цифрова комутаційна система ЕАТС DX-200 розроблена фахівцями фірми «Теленокія» (Фінляндія). Перші АТС цієї системи були введені в лад в 1985 р. До складу системи ЕАТС DX-200 входять чотири функціональні блоки: абонентська підсистема; підсистема обробки викликів; підсистема технічної експлуатації; підсистема підключення з'єднувальних ліній. До складу системи ЕАТС DX-200 входять два типи АТС: ЕАТС DX-210 і ЕАТС DX-220.Станція ЕАТС DX-210 найкращим чином пристосована для роботи в якості АТС малої ємності, однак при необхідності вона може бути використана в якості транзитної.

УДК 621.396.49 (043.2)

В.Т. Кривоус
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ АРХІТЕКТУРИ СИСТЕМ УПРАВЛІННЯ МЕРЕЖ 3G

В даній роботі приділяється увага дослідженню систем, протоколів управління сучасних комплексів управління мереж стільникового мобільного зв'язку третього покоління – 3G.

Основною метою виконання роботи є дослідження різноманітних протоколів, систем, що використовуються для адміністрування мереж стільникового мобільного зв'язку третього покоління, а також вирішення проблеми оптимального та раціонального вибору з наявних апаратних та програмних засобів. В ході виконання роботи були взяті до уваги ключові особливості функціонування, експлуатування та можливого масштабування телекомунікаційного обладнання, що входить до складу мереж GSM. Акцент було зроблено на класичних рекомендаціях request for comments UMTS для мереж третього покоління та на вже успішно інтегрованих рішеннях від виробників телекомунікаційного обладнання.

UMTS ставить перед виробниками і операторами мобільного зв'язку проблеми, зв'язані зі складністю технічної реалізації та великими затратами на інфраструктуру. Уніфікація протоколів та методів доступу до обладнання є необхідною умовою стандартизації у рамках UMTS. Типові задачі управління, адміністрування, експлуатації в залежності від суб'єктивних факторів отримання та видачі необхідної інформації можуть бути однаково успішно виконанні за допомогою наступних технологій: web-протоколу http, протоколу secure shell (ssh), незахищеного протоколу TErminaL NETwork (telnet), а також спеціальних систем керування телекомунікаційним обладнанням на основі протоколу Simple Network Message Protocol (SNMP), а також використання інших протоколів, що опосередковано можуть впливати на вищезгадані процеси.

Результати, отримані внаслідок дослідження та визначення оптимальних шляхів управління мережами 3G мають практичних характер. В разі впровадження визначеного підходу на етапі

розгортання, або інтегрування у вже існуючий операторський комплекс, очікується гарантований приріст ефективності управління. До факторів, що призводять до цього явища можна віднести: зменшення закладеного бюджету на використання ліцензованого ПО на кількість співробітників, скорочення часу на виконання нетипових операцій конфігурування, можливість дублювання засобів доступу безпосередньо до обладнання. Враховуючи концептуальну близькість мереж UMTS та мереж 3G, широку розповсюдженість останніх, можна стверджувати, що дана робота зачіпає велике коло систем.

УДК 004.772(043.2)

І.О. Кукулевський
Національний авіаційний університет, м. Київ

ПІДВИЩЕННЯ ГАРАНТОВАНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ДО РІВНЯ Г3

На сьогоднішній день кожне сучасне підприємство має корпоративну мережу. Тому виникає потреба в оцінці захищеності телекомунікаційної системи (ТЛК-системи) від несанкціонованого доступу (НСД). Бувають різні обставини за яких оцінюють корпоративну мережу. По-перше, коли оцінка проходить вперше для підприємства, по-друге, коли підприємство хоче покращити рівень захищеності корпоративної мережі, і по-третє, коли проходить планова перевірка дійсності рівня захищеності мережі підприємства. В усіх вищеперерахованих випадках оцінки захищеності ТЛК-системи від НСД розглядають дотримування вимог двох видів:

– вимоги до функцій (послуг) забезпечення безпеки;

– вимоги до рівня гарантій.

Виконання вимог першого виду забезпечується Розробником системи захисту в процесі її проектування (розробки) і перевіряється Експертною комісією в процесі оцінки її якості. Виконання вимог другого виду забезпечується, як діями Розробника, проте вже на всіх стадіях життєвого циклу ТЛК-системи, так і спільними діями Розробника і Експертної комісії в процесі

оцінки. Критерії гарантії вимоги регламентують передусім дії Розробника. Дії Експертної комісії регламентуються іншими документами. Більшість з вимог критеріїв гарантій являють собою конкретизацію положень стандартів серії ДСТУ ISO 9000 щодо створення КЗЗ у ТЛК-системах і для їх викладення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95).

В даному випадку є корпоративна мережа, яка має рівень гарантованості Г2. Тому виникла проблема, яким чином отримати рівень Г3. Так як рівень Г2 відноситься до низьких рівнів забезпечення гарантій коректності архітектури КЗЗ, тому від Розробника вимагається лише описати складові компоненти КЗЗ та їх призначення. А ось рівень Г3 відноситься вже до більш високих (проміжних) рівнів забезпечення гарантій, тому вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, що є критичними з точки зору забезпечення безпеки. Також всі внутрішні деталі і дані, що використовуються всередині кожного модуля, повинні бути приховані від усіх зовнішніх об’єктів., а послуги КЗЗ повинні бути доступні тільки через зовнішній документований інтерфейс.

Отже, після дотримання всіх вимог для підвищення гарантованості захисту інформації в корпоративних мережах до рівня Г3, мною був розроблений комплекс апаратно-технічних заходів по вдосконаленню ТКС-системи.

УДК 621.391.63 (043.2)

О.В. Антонюк
Національний авіаційний університет, м. Київ

ВОЛОКОННО-ОПТИЧНА ЛІНІЯ ЗВ’ЯЗКУ

Телекомунікаційні системи України відіграють визначну роль в забезпеченні всіх видів і форм діяльності держави. Одним з важних показників забезпечуючих надійне функціонування цих систем, являється рівень їх безпеки в умовах впливу технологічних факторів та можливих несанкціонованих дій.

В проекті розробляється телекомунікаційна волоконно-оптична лінія з організацією технічних мір по забезпеченню безпеки вузлів зв'язку які не охороняються.

Необхідний рівень захищеності об'єктів зв'язку, які не охороняються, може бути досягнутий тільки створенням розгалуженої системи безпеки. В роботі розглядаються організаційно-технічні аспекти і обґрунтовуються принципи побудови систем захисту таких об'єктів. Під системою захисту об'єкта мається на увазі сукупність технічних засобів безпеки: датчиків, пристроїв спостереження та реєстрації.

Для досягнення гарантованого рівня безпеки віддалених об'єктів насамперед необхідно забезпечити практично миттєве оповіщення служби фізичної охорони з необхідною вірогідністю. Це завдання вирішується за допомогою датчиків охоронно-пожежної сигналізації (ОПС), зовнішніх (периметрів) систем виявлення, зовнішніх і внутрішніх систем телеспостереження.

Тому в рішенні проблеми захисту вилучених віддалених об'єктів чільну роль грають як повнота й вірогідність інформації про характер події, так і рівень активного й пасивного захисту. Під активним захистом розуміють фізичне й у якісь мірі, психологічний вплив на зловмисника: сліпучі джерела світла, джерела звуку що оглушають, пристрої розбризкування незмивної фарби (для полегшення подальшого розшуку зловмисника), пристрої розпилення штучних мрячних утворень, сльозоточивих речовин, імітатори підривних пристроїв (петарди, хлопавки). Обов'язковою умовою застосування засобів активного захисту є мінімальна шкода здоров'ю й гарантія відсутності загрози життю зловмисника.

Не менш важливою є вимога оперативності надходження й повноти інформації про стан об'єкта. Виконання цієї умови необхідно для мінімізації як рівня фіктивних тривог, так і рівня пропусків погроз. Об'єкт повинен бути обладнаний відповідною системою датчиків і пов'язаний із центром прийому й обробки інформації високонадійною системою передачі.

Розробка структурної схеми ВОЛЗ між містами Київ та Вінниця є важливою умовою створення високошвидкісної магістральної лінії зв'язку, що буде сполучати між собою столицю та обласний центр. Побудова волоконно-оптичної магістралі на-

дає багато перспектив для розвитку бізнесу, взаємодії, високошвидкісного та надійного зв'язку між кінцевими пунктами.

УДК 621.396.67 (043.2)

А.В. Ткач
Національний авіаційний університет, м. Київ

ОЦІНКА ЗАВАДОСТІЙКОСТІ ТА ШВИДКОСТІ ПЕРЕДАВАННЯ АНТЕННИХ СИСТЕМ MIMO

У наш час відбувається інтенсивний розвиток цифрових систем бездротового зв'язку, і одним з найбільш пріоритетних напрямків досліджень у цій області є підвищення ефективності такого роду систем, пов'язаної, в першу чергу, з підвищенням швидкості передачі інформації при збереженні високої якості обслуговування абонентів (низькій ймовірності помилки при передачі інформації). Основними перешкодами для досягнення цієї мети є складні умови багатопроменевого розповсюдження сигналів у випадково розсіювальному середовищі, яке викликає глибокі завмирання. Рішенням цих проблем є використання технології MIMO (Multiple Input – Multiple Output), яка, в загальному випадку, означає, що кожний радіотехнічний пристрій, який бере участь в обміні даними, буде мати декілька антен.

Одним із завдань роботи було дослідження пропускної здатності, а особливо знаходження точного виразу для її розрахунку, адже в цілому вона є випадковою величиною (канальна матриця H є матрицею випадкових чисел). Також у даній роботі було досліджено статистичні характеристики власних чисел канальної матриці в MIMO-системі з конфігураціями (Mx2) та (2xN), де M – число передаючих антен, N – число приймальних антен. Було розглянуто поведінку ймовірності бітової помилки (BER – Bit Error Rate) в MIMO-системах в залежності від відношення сигнал-шум. Показано, що вона повністю визначається статистичними властивостями власних чисел канальної матриці. Були отримані вирази для BER у сильному па слабкому підканалах системи для сигналів різних видів модуляції (QPSK, BPSK, 16-QAM, 64-QAM).

Нижче на рис. 1 наведені графіки для M = 2 і M = 4 ілюструють, що доцільніше використовувати більше число передавальних антен, оскільки при однаковій величині ВСШ значення ймовірності бітової помилки є набагато меншою при M = 4, що також вказує на кращу роботу системи.

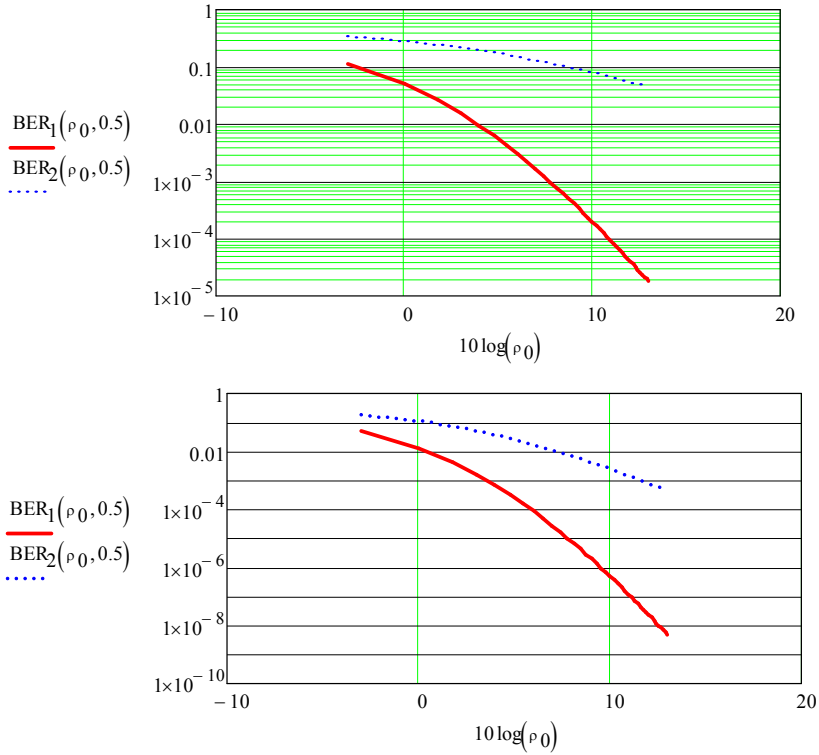

Рис. 1

Дана робота є актуальною у наш час, коли впроваджуються нові технології зв’язку, а користувачі бездротових мереж прагнуть мати більші швидкості передачі даних.

УДК 681.3.06 (043.2)

А.І. Хромов
Національний авіаційний університет, м. Київ

ВИЯВЛЕННЯ ЗАГРОЗ ЗА ДОПОМОГОЮ МЕТОДУ ІЄРАРХІЙ

З кожним днем, разом зі стрімким розвитком науки та техніки, все актуальніше стає питання захисту інформації. Стрімкий розвиток мереж, дротових так і мобільних, разом із стрімким розвитком обчислювальних ресурсів та прощенням доступу до них користувачів (наприклад до хмарних технологій) надає широкі можливості до здійснення різного типу атак. Тому необхідність у розробці комплексних систем захисту інформації стає з кожним днем все актуальніше.

Створення комплексної системи захисту інформації потребує чималих витрат на всіх стадіях: обстеженні, розробки, впровадження СЗІ. В залежності від вартості інформації що передбачається, та послуг які буде надавати таке підприємство проводиться різна глибина аналізу інформаційної системи (далі ІТС) та її системи захисту.

Метою роботи було визначити можливість використання методу експертних оцінок для виявлення ризиків та формування моделі загроз для подальшого створення комплексної системи захисту інформації.

Для аналізу ризиків існує декілька підходів серед них анкетування, що проводиться серед співробітників організації, методи експертних оцінок, що дозволяють визначати множини ризиків, як одному так і декільком експертам за допомогою застосування математичного апарату. Серед останніх є такі методи відносних цінностей, на базі теорії нечітких множин, метод аналізу ієрархій та ін.

У цій роботі було запропоновано застосовувати метод аналізу ієрархій, як найбільш гнучкий і як метод, що може ефективно застосовуватись одним експертом

Для дослідження, наведена спрощена структура системи. Деякі компоненти були об’єднані у більш глобальні вузли. Основними компонентами, які досліджувались при аналізі й оцінці ризиків були наступними: сервер білінгу, WWW-сервер, робочі

місця адміністраторів, між мережевий екран, комутаційне обладнання. Інформаційні об'єкти, що бралися для аналізу були: інформація о стану рахунку клієнта, запит на зміну стану рахунку, відповідь на запит на зміну стану рахунку.

У результаті проведеної роботи було визначено перелік найбільш актуальних загроз для досліджуваної мережі, сформована модель загроз, за допомогою методу експертних оцінок, та надані рекомендації щодо їх усунення. Визначено мінімальний профіль безпеки, відповідно до українського законодавства.

УДК 621.395.74 (043.2)

А.Є. Вовченко
Національний авіаційний університет, м. Київ

МІСЬКА ТЕЛЕФОННА МЕРЕЖА З СЕГМЕНТОМ МЕРЕЖІ NGN

В роботі розглянута мережа зв'язку наступного покоління (NGN) – концепція побудови мережі зв'язку, що забезпечує 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 з розподіленою комутацією, винесення функцій надання послуг та інтеграцію з традиційними мережами зв'язку.

В результаті аналізу моделі та загальної архітектури мережі NGN, особливістю якої є те, що передача та маршрутизація пакетів і елементи устаткування передачі, фізично і логічно відокремлені від пристроїв та логіки керування викликами й послугами, була розглянута архітектура мережевих елементів на базі обладнання компанії «Іскрател Україна» SI3000, яка включає в себе інтегрований сервер обробки викликів (SI3000 iCS), мультисервісний вузол абонентський (SI3000 MSAN) з аналоговими, ADSL2+, VDSL2, WIMAX, Ethernet і оптичними інтерфейсами. Представлені продукти сімейства SI3000 OSAP, які розроблені так, що можуть задовольнити потреби як великих телекомунікаційних операторів, так і операторів невеликих мереж, провайдерів послуг, за допомогою додатків нового

покоління. Розглянуто програмний комутатор SI3000 CS, який забезпечує широку пропозицію будь-яких послуг, в основі яких лежить IP-протокол.

Наступним етапом було проведено модернізацію фрагменту міської телефонної мережі при використанні обладнання SI3000, яка включає в себе аналіз вже існуючої телефонної мережі міста. Також було розроблено схему фрагмента міської телефонної мережі на основі технології NGN, і організовано підключення кінцевих користувачів телефонної мережі загального користування за допомогою технології NGN. Був здійснений розрахунок інтенсивності навантаження та ємності пучків з'єднувальних ліній мережі, навантаження від абонентів стільникового рухомого зв'язку та виникаючого місцевого і міжміського навантаження.

В даній роботі спроектована модернізація міської телефонної мережі до мультисервісної мережі на базі обладнання SI3000 з використанням комутації пакетів. Системи управління мультисервісними мережами повинні будуватися за такими ж основними принципами, що і самі мережі, тобто мати модульну архітектуру з використанням відкритих інтерфейсів між модулями.

Важливу роль має організація взаємодії різних операторів постачальників послуг та їх якість, а також можливість взаємодії користувачів із системою управління. В наш час споживач потребує велику кількість послуг, до яких входять телефонія, телебачення, доступ до локальної мережі, доступ до відео зв'язку та таке інше, і щоб користуватися цими видами інформації була створена мережа NGN.

УДК 621.396.21(043.2)

Є.М. Бабенко
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ ЗАТУХАНЬ В КАНАЛАХ ЗВ'ЯЗКУ WiMAX

У зв'язку із широким розвитком бездротових систем зв'язку, актуальним стало питання про вплив умов поширення радіо-

хвиль на роботу мобільних абонентів. Проблема ця важлива й багатогранна, тому детальне вивчення цієї теми дозволить більш успішно будувати різноманітні мобільні мережі передачі даних. При цьому виникає ряд проблем, пов'язаних з моделюванням перешкод на шляху поширення сигналів, а також у зв'язку з багатопроменевим поширенням сигналів і великою кількістю перевідбиттів.

Під час проведення дослідження було помічено, що розраховані значення затухання потужності сигналу сильно відрізняються від реальних, виміряних за допомогою приладів. Тому було запропоновано створити математичний апарат який зумів би максимально наближено видавати дані.

На основі отриманих даних було створено методику визначення загасання сигналу від відстані.

Представлена методика є повною і дійсною для наших умов, але вона може мати розбіжності з дійсними значеннями, це пов'язано з тим, що не було змоги використати більш точне обладнання. І теоретично, прилад з якого знімали параметри міг прийняти інший сигнал в цьому діапазоні.

Також, в даній роботі представлено один з найважливіших показників для розрахунку цифрової системи радіозв'язку та її практичне використання і порівняння отриманих параметрів з експериментальними даними.

Рівень сигналу на вході приймача визначається за наступною формулою:

$$P_{\text{ПР}} = P_{\text{ПД}} + G_1 + G_2 - L_0 - L_{\text{Ф1}} - L_{\text{Ф2}} - L_{\text{Г}} - L_{\text{РФ}} - L_{\text{ДОП}}.$$

Для розрахунку L_0 скористаємось виразом який ми отримали в результаті математичного моделювання:

$$L_0 = \begin{cases} -1{,}667 \cdot 10^{-4} R^3 + 0{,}02 R^2 - 1{,}183 R - 46 \\ -1{,}768 \cdot 10^{-5} R^3 + 2{,}619 \cdot 10^{-3} R^2 - 0{,}477 R - 54{,}976 \\ 1{,}101 \cdot 10^{-5} R^3 - 1{,}001 \cdot 10^{-3} R^2 - 0{,}352 R - 54{,}094 \\ -1{,}121 \cdot 10^{-6} R^3 + 1{,}564 \cdot 10^{-3} R^2 - 0{,}509 R - 53{,}489 \\ -1{,}221 \cdot 10^{-5} R^3 + 4{,}583 \cdot 10^{-3} R^2 - 0{,}742 R - 48{,}85 \end{cases}$$

де R – протяжність інтервалу, складає 210 м – значення при якому проводились досліди; L_0 – втрати при розповсюдженні в умовах NLOS.

На основі отриманих даних було продемонстровано покриття одного з районів м. Києва в залежності від типу модуляції. Представлений розрахунок є тільки наглядним зображенням методики і не враховує навантаження на БС та частотно-територіальний поділ.

УДК 004.056.6 (043.2)

Б.Е. Журиленко, Н.К. Николаева, З.О. Самосуд
Национальный авиационный университет, г. Киев

ПОИСК ЗАКЛАДНОГО УСТРОЙСТВА С ПОМОЩЬЮ ЛАЗЕРНОГО ЛУЧА

Поиск закладных устройств (ЗУ) осуществляется в радиодиапазоне с помощью индикаторов поля, частотомеров, анализаторов спектра, панорамных приемников с программой DigiScan EX 1.6 или другого типа, локализирующих место нахождения радиозакладки. Поиск других типов ЗУ может осуществляться универсальными приборами, пользующимися наибольшей популярностью: OSC-5000 («Oscor»), СРМ-700 («Акула»), ST 031, ST 032 («Пиранья»). Для определения ЗУ в проводных линиях используется локатор проводных линий «Бор», обеспечивающего определение дальности до ЗУ с точностью до (2,5–5) метров с непосредственным подключением к телефонным, пожарным, охранным и силовым электрическим линиям.

Поисковые мероприятия и локализация ЗУ с помощью перечисленных приборов, требует значительных затрат времени. Чтобы сократить время поиска и локализации ЗУ, предложен прибор с акустической локализацией микрофона и указанием места его положения лазерным лучом. Поскольку осуществляется локализация микрофона ЗУ, то луч указывает непосредственно либо на него, либо на путь, по которому звук достигает микрофона.

При поиске ЗУ в основном используется тестовый сигнал, который может быть и тональным. Трудности, возникающие при использовании тонального сигнала, заключаются в том, что в помещениях, заполненных различной мебелью или другими вещами, возникают стоячие волны, которые мешают локализации ЗУ. Чтобы избавится от стоячих волн, используется импульсный метод локации сигнала, например, DigiScan EX 1.6. Недостатком данного метода и системы локализации ЗУ является расположение акустических колонок и микрофона на одной линии, расстояние между которыми измеряется с помощью рулетки, и отметка, задержанных сигналов, оператором. Первый из перечисленных недостатков приводит к неоднозначности в определении места положения ЗУ и требует дополнительных исследований помещений, что при загруженности помещения мебелью, может быть нелегкой задачей. Второй – связан с точностью определения места положения ЗУ и требует дополнительных исследований по поиску ЗУ путем перемещения микрофона и колонок.

В предлагаемом методе используется прибор, основной частью которого является акустическая антенна с расположением колонок в вершинах правильного треугольника. В центре треугольника расположен лазерный целеуказатель с лучом, перпендикулярным плоскости расположения колонок. Колонки излучают импульсные сигналы, задержка между которыми подстраивается равной, путем регулирования плоскости акустической антенны. После подстройки, когда задержки от всех колонок становятся равными, включается лазерный целеуказатель, который лучом указывает на место положения ЗУ. Если ЗУ будет запрятано, то лазерный луч будет указывать на место, через которое звук будет проникать на микрофон. Например, если микрофон ЗУ запрятан в вентиляции, то луч будет показывать на вентиляционное отверстие в помещении. Если же утечка будет через телефонную линию связи в телефонном аппарате, то – на телефон.

Таким образом, данный метод и прибор позволят осуществлять поиск ЗУ в любых каналах утечки информации, для которых существуют приемники этой информации.

Преимущества предлагаемого метода поиска и прибора проявляются в том, что уже после первого измерения, направлением луча указывается и локализуется направление, в котором находится ЗУ. Дополнительные измерения, связанные с перемещением акустической антенны, будут все более уточнять место расположения ЗУ. Этим экономится время поиска и не требуется выносить мебель из помещения.

УДК 004.383.3:004.623 (043.2)

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

КАНАЛИ СТЕГАНОГРАФІЧНОГО ПЕРЕДАВАННЯ ДАНИХ У СИСТЕМАХ ЦИФРОВОГО МОВЛЕННЯ

Цифрове мовлення (ЦМ), що нині інтенсивно впроваджується у країнах Європи, і, зокрема, в Україні, відкриває принципово нові можливості у передаванні аудіовізуальних і мультимедійних програм, які, крім того, можуть містити у собі додаткову звукову, графічну і текстову сервісну інформацію (СІ), а у перспективі — й конфіденційну інформацію (КІ). Відомі способи ЦМ (*DAB*, *DVB*) і їх варіанти (-*T*, -*C*, -*S*, -*H*) засновані на механізмах кодування аудіовізуальних сигналів програм за відомими методами компресії аудіо- та відеоданих (стандартами *MPEG*) і розділення каналів за допомогою ортогональних несних (*OFDM*). При цьому аналогові сигнали від первинних джерел кожної програми перетворюються на окремі цифрові потоки, що стискаються із втратами і після завадостійкого кодування, вирівнювання спектру і часового перемежовування об’єднуються з окремо створеними каналами сервісних даних у цифровий потік головного каналу. Недоліком є потреба існуючих способів у створенні окремого відкритого каналу передавання СІ, пропускна здатність якого за багатьох конфігурацій мультиплексу є порівнянною із швидкістю цифрового потоку основних аудіовізуальних даних програми. Це призводить до неекономного використання радіочастотного ресурсу (РЧР) або ж до погіршення якості відтворення аудіовізуальних сигналів. Крім того, зростаючі об’єми аудіо- та відеоінформації, СІ та КІ,

а також розширення кола її споживачів зумовлює потребу контролювати достовірність інформації, забезпечувати захист від спотворення, втрати чи несанкціонованого відтворення.

Комплексне врахування зазначених вище особливостей можливе із створенням для передавання СІ/КІ прихованих каналів стеганографічного передавання даних (КСПД) на основі аудіовізуальної інформації трансльованих програм: сигнали від джерел СІ/КІ вводяться до головного каналу шляхом вбудовування до окремих аудіо- чи відеопотоків програм (контейнерів), що стискаються з урахуванням психоакустичної чи візуальної моделі — у результаті застосування адаптованих алгоритмів цифрової стеганографії. Вбудовування здійснюється за допомогою стеганокодека, який пропонується додатково ввести до складу аудіо- чи відеокодека *MPEG* кожної програми.

Використання КСПД у складі систем ЦМ має наступні переваги: при розширенні сфер послуг ЦМ зникає потреба у створенні додаткових окремих субканалів перенесення СІ/КІ, що дає можливість або збільшити кількість програм, трансльованих у смузі частот одного каналу (збільшити ефективність і прибутки від використання РЧР), або ж збільшити бітову швидкість цифрових аудіовізуальних потоків довільного набору програм мультиплексу (підвищити якість надаваних послуг); виникає можливість використання систем ЦМ для організації мереж передавання КІ — завдяки прихованню самого факту існування відомостей закритого характеру при їх транспортуванні.

На основі отриманих результатів можливе створення і вдосконалення національних стандартів ЦМ.

УДК 629.735.05: 53.087.61 (043.2)

О.В. Соломенцев, М.Ю. Заліський,
О.В. Зуєв, Д.О. Соловйов
Національний авіаційний університет, м. Київ

СТАТИСТИЧНІ МОДЕЛІ ЙМОВІРНОСТІ БЕЗВІДМОВНОЇ РОБОТИ ЗАСОБІВ ЗВ'ЯЗКУ

Для вирішення практичних задач розробки та модернізації систем експлуатації зазвичай використовуються узагальнені по-

казники якості, за допомогою яких можуть бути обчислені ризики аеронавігаційного обслуговування, порогові рівні характеристик функціонування засобів зв'язку тощо. Одним із таких показників може бути, наприклад, коефіцієнт оперативної готовності, коефіцієнт готовності, ймовірність безвідмовної роботи тощо.

Розглянемо основні статистичні характеристики ймовірності безвідмовної роботи. Загально відомо, що під ймовірністю безвідмовної роботи $P(t)$ розуміється ймовірність того, що за певних умов експлуатації в заданому інтервалі часу або у межах заданого напрацювання t не відбудеться жодної відмови. У загальному випадку вихідними даними для розрахунку показників надійності є статистичні дані щодо напрацювань t_i та відновлень τ_i засобів радіотехнічного забезпечення польотів.

Для обчислення ймовірності безвідмовної роботи вичерпною може бути інформація щодо напрацювання на відмову. За випадку експоненціальних напрацювань на відмову вираз для щільності розподілу ймовірності безвідмовної роботи

$$f(t,\ P) = \frac{n^n t^n}{P\Gamma(n)(T_0)^n \left|\ln^{n+1} P\right|} e^{\frac{nt}{T_0 \ln P}},\ 0 \le P \le 1,$$

де n – кількість зафіксованих відмов, за якими здійснюється оцінка середнього напрацювання відмову; T_0 – математичне сподівання оцінки середнього напрацювання на відмову; $\Gamma(n)$ – неповна гамма-функція.

Розглянемо випадок нормальних напрацювань на відмову. Використовуючи під час розрахунків розкладання експоненти у ряд Тейлора (для простоти розрахунків візьмемо два перші члени ряду), отримаємо наступну щільність розподілу ймовірності безвідмовної роботи

$$f(t,\ P) = \frac{2\sigma^2\sqrt{n}}{\sqrt[3]{\left(6\sigma^3\sqrt{2\pi}(1-P) - 6\sigma^2 t\right)^2}} e^{\frac{-n\left(t+\sqrt[3]{6\sigma^3\sqrt{2\pi}(1-P)-6\sigma^2 t}-T_0\right)^2}{2\sigma^2}},$$

$$0 \le P \le 1,$$

де σ – середньоквадратичне відхилення оцінки середнього напрацювання на відмову.

Отримані аналітичні співвідношення збігаються зі статистичним моделюванням, що підтверджує їх достовірність. Результати досліджень можуть бути використані в системах експлуатації засобів зв'язку, системах менеджменту якості виробництва продукції та надання послуг тощо.

УДК 519.246:621.3.095.2 (043.2)

Ю.В. Тимченко
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ ВИПАДКОВИХ ПРОЦЕСІВ ІЗ ЗАДАНИМИ ВЛАСТИВОСТЯМИ

При вивченні властивостей каналів передачі інформації, сигналів та завад абстрагуються від їх конкретної фізичної природи та призначення і оперують з їх моделями. Оцінка електронних систем потребує виявлення кількісних співвідношень між основними параметрами джерела інформації і системи, тому дослідження здійснюється на математичних моделях. За допомогою моделювання випадкового процесу стає можливим проаналізувати та передбачити результат проходження завади через нелінійний елемент, що є суттєвим при проектуванні генератора шуму для захисту інформації від витоку по електричному або радіоканалу.

Радіотехнічні процеси володіють специфічними властивостями, основними з яких є статистична природа та висока швидкість протікання. Це призводить до необхідності розробки алгоритмів формування випадкових процесів, при цьому дані алгоритми мають бути максимально спрощені для того, щоб підвищити швидкість виконання.

У загальному випадку повною характеристикою випадкового процесу є його багатовимірна щільність імовірностей. Для моделювання випадкових величин, можливі значення яких не виходять за межі деякого обмеженого інтервалу (a,b), а також випадкових величин, закони розподілу яких можна апроксиму-

вати усіченими кривими, досить універсальним є метод Неймана, що полягає в наступному.

З датчика рівномірно розподілених в інтервалі (0,1) випадкових чисел x_1, x_2 з яких формуються перетворені пари $x_1^* = a + (b - a)x_1$; $x_2^* = w_m x_2$, де $(a;b)$ – інтервал можливих значень випадкової величини з заданою функцією щільності $w(y)$; w_m – максимальне значення функції $w(y)$. Як реалізація випадкової величини обирається число x_2* з тих пар x_1*, x_2*, для яких виконується нерівність:

$$x_2^* < w\left(x_1^*\right). \qquad (1)$$

Пари, що не задовольняють нерівності, відкидаються.

Неважко переконатися в справедливості такого методу моделювання випадкових величин. Пари випадкових чисел x_1*, x_2*, що задовольняють умову (1), є координатами випадкових точок площини, всередині прямокутника *aa'b'b* під кривою $w(y)$. Імовірність того, що випадкова точка площини, що знаходиться під кривою $w(y)$, знаходитиметься в полосі $(y; y+\Delta y)$ пропорційна $w(y)$, а імовірність потрапляння точки під криву рівна одиниці за умовою, що і вимагалося.

УДК 519.246 (043.2)

В.Е. Осипова
Национальный авиационный университет, г. Киев

МОДЕЛИРОВАНИЕ СЛУЧАЙНЫХ ПРОЦЕССОВ С ЗАДАННЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

Моделировать случайные процессы с заданной корреляционной функцией можно в рамках корреляционной теории. Однако при формировании реализаций большой длины эти методы требуют большого количества вычислений и трудоемкой подготовительной работы.

К сожалению, более простых методов получения неограниченных во времени дискретных реализаций случайных процессов с заданной корреляционной функцией $R(t, t')$ до настоящего времени не известно.

Для стационарных нормальных случайных процессов найдены весьма экономичные моделирующие алгоритмы. В их основу положено линейное преобразование стационарной последовательности $x(n)$ независимых нормальных случайных чисел (дискретный белый шум) в последовательность $y(n)$, коррелированную по заданному закону.

При этом оператор линейного преобразования записывается либо в виде скользящего суммирования с некоторым весом $c_k = c(k)$, либо как рекуррентное уравнение.

Задачу цифрового моделирования с помощью скользящего суммирования и рекуррентных разностных уравнений можно рассматривать как задачу синтеза линейного дискретного формирующего фильтра, который преобразует белый шум на его входе в коррелированный дискретный случайный процесс с заданными корреляционно-спектральными характеристиками на его выходе.

Для цифрового моделирования случайных процессов с заданными корреляционными свойствами используются два основных метода:

1) Метод скользящего суммирования
2) Метод рекуррентных разностных уравнений.

При использовании метода скользящего суммирования весовые коэффициенты можно получать:

- путем решения нелинейной алгебраической системы уравнений;
- путем разложения функции спектральной плотности в ряд Фурье;
- методом факторизации.

При использовании метода рекуррентных разностных уравнений параметры рекуррентных алгоритмов получают:

- методом факторизации;
- методом дискретизации непрерывного формирующего фильтра.

По вычислительным затратам и точности метод разложения функции спектральной плотности в ряд Фурье является самым приемлемым.

УДК 004.056 (043.2)

Ю.Р. Гарасим [1], В.А. Ромака [2], О.Л. Полуектова [2]
[1]Smart Holding, м. Київ
[2]Національний університет «Львівська політехніка», м. Львів

ЗАСТОСУВАННЯ SWOT-ПІДХОДУ ДЛЯ СТРУКТУРИЗАЦІЇ ДАНИХ ПРО ПОДІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Важливою складовою управління в корпоративних мережах зв'язку (КМЗ) є процес збору та обробки даних про події від систем захисту інформації (СЗІ). Процес структуризації зібраних даних є необхідних для діагностики СЗІ в КМЗ. Схема структуризації зібраних даних від СЗІ в КМЗ передбачає декілька етапів. Побудова моделі починається з якісного опису проблемної ситуації, що містить структуризацію первинних представлень експертної групи про СЗІ в КМЗ.

В межах роботи запропоновано таку методику структуризації знань про СЗІ в КМЗ:

- побудова базової моделі M (G(X) – сукупність факторів, A – матриця взаємозв'язку факторів), X(0) – вектор початкових значень факторів), який містить базові фактори;
- вибір важливих факторів за допомогою виявлення SWOT-факторів на основі аналізу експертної інформації та експертної оцінки важливості їх впливу на СЗІ в КМЗ;
- включення вибраних факторів в базову модель, M*(G*, X*(0), U – вектор управління), і формування сценаріїв розвитку;
- сценарний аналіз їх впливу на розвиток системи, тобто порівняння сценаріїв розвитку ситуації без врахування SWOT-факторів – S і з їх врахуванням – S*.

Загальна схема експертної оцінки SWOT-елементів. Опис основних етапів аналізу за SWOT-схемою такий:

1. Визначення SWOT-факторів СЗІ в КМЗ, що містять 4 групи:

1.1. $S(s_1,...,s_n)$, де n – кількість виявлених сильних сторін;

1.2. $W(w_1,...,w_m)$, де m – кількість виявлених слабких сторін;

1.3. $O(o_1,...,o_l)$, де l – кількість виявлених вразливостей;

1.4. $T(t_1,...,t_k)$, де k – кількість виявлених загроз.

2. Оцінка вагомості виявлених SWOT-факторів шляхом групової експертної оцінки їх взаємовпливу. Групова оцінка будується з використанням алгоритму побудови медіана Кемені.
3. Інтегральна оцінка кожної групи SWOT-факторів за визначеними критеріями і поділ їх на класи вагомості.
4. Сценарний аналіз впливу визначених SWOT-факторів.

УДК621.396:621.376.6(043.2)

О.М. Борейчук
Національний авіаційний університет, м. Київ

ВИБІР ОПТИМАЛЬНОГО МЕТОДУ МОДУЛЯЦІЇ СИГНАЛУ В ЦИФРОВИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ

В даний час переважна більшість систем радіозв’язку і радіомовлення є цифровими. Ті системи, які в даний момент є в основному аналоговими найчастіше мають чітку, закріплену нормативними документами тенденцію переходу на цифрову основу. Цифровий радіозв’язок використовується в навігації, супутниковому мовленні, телефонії (DECT), спеціальних завданнях. При організації системи зв’язку найчастіше основним завданням є передача необхідної або максимальної кількості інформації за заданий час з необхідною якістю при мінімальних енергетичних витратах. Тільки цифрова передача даних дозволяє здійснити передачу інформації з будь заданою вірогідністю.

Що стосується вибору оптимального методу модуляції, при проектуванні системи зв’язку ставиться наступне завдання: є заданий рівень вірогідності помилки на біт, який не перевищуєть-

ся. Звичайно, задача системи зв'язку - забезпечити максимальну швидкість передачі даних.

Щодо практики, для систем комп'ютерного обміну прийнятний рівень BER системи радіозв'язку істотно нижче (порядку $10^{-9}...10^{-12}$). У даних системах додаткове зниження BER забезпечується протоколом більш високого рівня (TCP/IP), що призводить до результуючих значень BER (наприклад, 10^{-20}). Якщо відома залежність BER від E_b/N_0 (відношення енергії біта до щільності потужності шуму), то можна визначити для кожного виду модуляції, мінімальне значення E_b/N_0, що забезпечує задане значення BER_{max}.

Для видів модуляції з відсутністю кодування залежності BER від E_b/N_0 є приведені. Залежності BER від E_b/N_0 можуть дещо відрізнятися від для різних варіантів реалізації системи зв'язку. Тому, найбільш точним є отримання залежностей BER від E_b/N_0 за допомогою комп'ютерного статистичного моделювання такого як моделювання в середовищі AWR Design Environment.

Об'єктно-орієнтована база даних AWR Design Environment постійно синхронізована з редактором схем, майстром моделювання та топологічним редактором, що забезпечує користувача вичерпною інформацією на всіх етапах розробки пристроїв: від ідеї до реалізації.

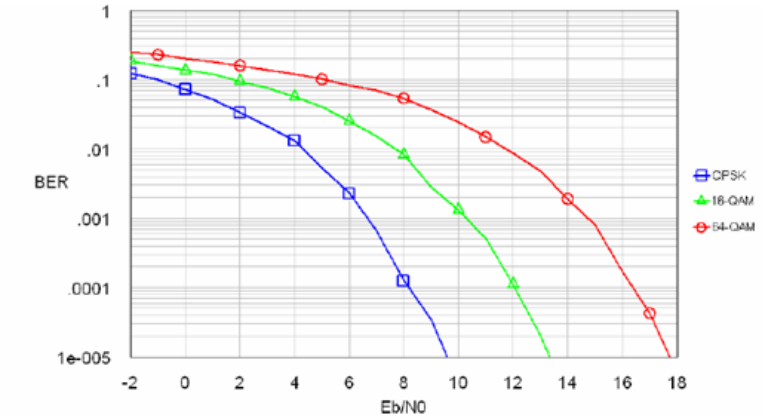

Рис.1. Залежності BER від E_b/N_0 для модуляцій QPSK, 16-QAM і 64-QAM без кодування

УДК 004.056.53 (043.2)

О.Г. Голубничий
Національний авіаційний університет, м. Київ

АНАЛІЗ ВИМОГ ТА РЕКОМЕНДАЦІЙ ІСАО ДО ЗАХИСТУ СЕАНСІВ ЗВ'ЯЗКУ «ЗЕМЛЯ–ЗЕМЛЯ» В МЕРЕЖІ ATN

Захист IP-рівня при проведенні сеансів зв'язку «земля – земля» в об'єднаній мережі ATN/IPS відповідно до вимог та рекомендацій ІСАО, які зокрема викладені у Doc 9896 AN/469, здійснюється за допомогою протоколу захисту мережного трафіка IPsec та протоколу обміну ключами в Інтернет, версія 2 (IKEv2).

IPsec як правило використовується для формування віртуальної приватної мережі VPN між шлюзами (NIST 800-77). Шлюзом може бути маршрутизатор або інший засіб захисту, наприклад брандмауер. В такому контексті іншими засобами захисту вважаються вузли ATN/IPS. Модель «від шлюзу до шлюзу» захищає зв'язок по мережах ATN/IPS між регіонами або між державами або організаціями в конкретному регіоні. IPsec може також використовуватися в режимі «від хоста до шлюзу», зазвичай для того, щоб дозволити хостам у незахищеній мережі отримати доступ до захищених ресурсів. IPsec також може використовуватися в конфігурації «від хоста до хоста», коли надається захист застосувань в режимі передавання даних між кінцевими системами.

Заходами забезпечення функціональної взаємодії в межах об'єднаної мережі ATN/IPS рекомендації ІСАО розглядають підтримку архітектури безпеки IPsec, протокол інкапсуляції захищених даних ESP та використання єдиного набору криптографічних алгоритмів. Їх архітектура описана в RFC 4301. Питання ESP розглядаються в RFC 4303, а криптографічні алгоритми, які можуть використовуватися, проаналізовані в RFC 4835. Документи ІСАО по ATN/IPS додатково уточнюють, що кодування за допомогою ESP є факультативним, однак автентифікація виконується завжди.

Ці документи також визначають, що вузли ATN/IPS при роботі в режимі «земля – земля» можуть використовувати протокол автентифікації заголовка IP (AH) (відповідно до вказівок

RFC 4302). При цьому зазначається, що AH може використовуватися в окремих виробах, однак все рідше застосовується в IPsec. В RFC 4301 зазначається: «Статус положення про підтримку протоколу AH понижений до "MAY" (факультативного), оскільки досвід показує, що лише в дуже обмеженій кількості випадків ESP не може надати необхідних заходів захисту. Слід мати на увазі, що ESP можна використовувати для забезпечення лише цілісності (без конфіденційності), так що він співставний з AH у більшості контекстів». Архітектура IPsec (RFC 4301) пропонує підтримку як ручного, так і автоматизованого управління ключами. Тенденція розвитку ATN/IPS показує, що частота ручного управління ключами буде зменшуватися. Тому в рекомендаціях ICAO зазначається, що вузли в умовах зв'язку «земля – земля» реалізовують протокол обміну ключами в Інтернет, версія 2 (IKEv2), який обумовлено в RFC 4306, для автоматизованого управління ключами. IKEv2 є останньою версією цього протоколу. Специфікації IKEv2 не такі складні як в першій версії протоколу, що повинно сприяти кращій функціональній сумісності різних схем реалізації.

Як і у випадку з ESP, протокол IKEv2 потребує використання набору обов'язкових алгоритмів для забезпечення сумісності. Даний протокол передбачає використання вузлами при здійсненні зв'язку «земля – земля» криптографічних алгоритмів, які визначені у RFC 4307.

УДК 621.396.2

К.Н. Яковишин, Э.В. Скрипчинская
Национальный авиационный университет, г. Киев

НОВОЕ В УЧЕБНОЙ ПРАКТИКЕ МОДЕЛИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

В докладе рассматриваются результаты практического применения в учебной практике технологий моделирования телекоммуникационных систем на примере программной модели тренажера для авиадиспетчера.

В докладе со ссылкой на статью [1] излагается новый взгляд на подготовку специалистов высокой квалификации для

телекоммуникаций. В докладе, как и в статье, обобщается опыт двухлетнего преподавания дисциплины "Информатика" в ИАН НАУ с направлением подготовки 6.050903 – "телекоммуникации".

В докладе подробно излагается главная идея статьи: специалист высшей квалификации по телекоммуникациям должен знать и уметь моделировать телекоммуникационные системы и протоколы в средах быстрого проектирования методами объектно-ориентированного программирования. Обращается внимание на то, что в основе практики обучения – примеры (проекты). Проектов – четыре. Описано содержание проектов, приведены ссылки на литературу. Ниже перечислены новые элементы учебной практики моделирования:

- во-первых, это формирование у студентов знаний и навыков по моделированию телекоммуникационных протоколов (таких как Ethernet, IP, UDP, TCP и других);

- во-вторых, это обучение исключительно на примерах, то есть никакой теории в отрыве от конкретных проектов;

- в-третьих, во время лекций по разработке приложений лучше всего показывать процесс разработки в реальном времени, то есть в среде быстрого проектирования; конечно, часть времени можно заполнить показом заранее заготовленных электронных лекций; разумеется, хорошие лекции должны содержать различную мультимедийную информацию, включая видео и звук;

- в-четвертых, это обучение методом нисходящего проектирования, то есть «от целого – к деталям и частностям», а не наоборот (как традиционно принято, «от деталей и частностей – к целому»);

- в-пятых, это обучение на примерах моделирования только интересных для студентов объектов, то есть объектов, которые вызывают у студентов живой интерес и сильную мотивацию к обучению.

В докладе и статье [1] на примерах показывается, как для моделирования телекоммуникационных систем и протоколов совместно используются следующие технологии программирования и проектирования – это:

- модульное программирование,

- структурное программирование,
- нисходящее проектирование,
- объектно-ориентированное программирование в среде быстрого проектирования программ.

Критерием истины является практика. Только практическое применение идей любой новой технологии может выявить ее достоинства и недостатки. Таким механизмом по оцениванию результатов практического применения в учебной практике технологий моделирования телекоммуникационных систем стала курсовая работа “Создание нового класса путем наследования”.

Курсовая работа выполнялась во 2-м семестре. На выполнение курсовой работы отводилось 36 часов самостоятельной работы студента. Курсовой работой и ее защитой завершается дисциплина и курс. При выполнении работы студент обязан достичь “высшего пилотажа” в освоении знаний и навыков по “Информатике”, технологиям программирования и проектирования телекоммуникационных систем.

Выполнение курсовой работы начинается с выбора каждым студентом индивидуального проекта из набора разнообразных по своей природе проектов. Проекты записаны на CD – приложении к книге Н.С. Культина [2].

Каждый проект представлен в отдельной папке. Каждая такая папка содержит все исходные тексты программ, а также построенный по ним уже готовый проект (то есть .exe – файл). Студент может открыть любую папку, запустить готовое приложение и оценить его работу. Понравившийся проект студент объявляет преподавателю. Таким образом, определяется экземпляр базового класса для каждого студента индивидуально.

На втором шаге курсового проектирования студент формулирует и утверждает у руководителя работы отличительные свойства и методы нового класса, который должен быть создан на основе базового класса путем наследования.

Подавляющее число студентов 1-го курса хорошо справились с выполнением курсовой работы и по форме и по содержанию. Некоторые студенты выполнили работу просто блестяще. Это студенты Е.В. Скрипчинская, А.В Емельянов, В.В. Кобец и другие.

В курсовой работе Э.В. Скрипчинской выполнено моделирование программного тренажера для авиадиспетчера. Листинг программы моделирования позаимствован из [3], где представлен .pdf-файлом. Далее листинг программы подвергнут распознаванию и преобразован в набор .cpp и .h-файлов. Затем эти файлы адаптированы для системы “Borland C++Builder 6”. Выполнена компиляция и построение приложения.

Работающее приложение (.exe – файл) создает из базового класса Airplane три экземпляра в виде моделей самолетов: Cessna 3238T, United Express 749, TWA 1040. Диспетчер может выбирать любой из этих самолетов и управлять его полетом, задавая параметры высоты, курса, скорости. Результаты моделирования полета самолетов представлены в докладе фотографиями (скриншотами) монитора диспетчера.

Список литературы

1. *К.Н. Яковишин*. VIP-специалисты для телекоммуникаций и IP-индустрии. // Збірник наукових статей V Международной научно-практической конференции „Проблеми і перспективи розвитку IT-індустрії”. – Харків, 2013. – Випуск 3(110). – С. 164-168.

2. *Культин Н.Б.* C++ Builder в задачах и примерах. Петербург, 2005. – 336 с: ил.

3. *Кент Рейсдорф* и *Кен Хендерсон*. Borland C++Builder. Освой самостоятельно, – 702с.

УДК 621.391.7

Ю.Є. Яремчук
Вінницький національний технічний університет, м. Вінниця

ПРО МОЖЛИВІСТЬ ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Представлено математичний апарат на основі рекурентної V_k –послідовності, в якій використовуються рекурентні співвідношення з коефіцієнтами, що пов’язані з початковими елементами. На його основі запропоновано методи цифрового підписування, суть яких полягає в заміні піднесення до степеня обчисленням елементу рекурентної V_k –послідовності з певним індек-

сом. Методи базується на використанні властивості V_k –послідовності, яка дозволяє обчислювати елементи цієї послідовності з можливістю адитивної зміни індексу, зокрема здійснювати обчислення елементів $v_{n+m,k}$ та $v_{-n+m,k}$. Крім того, на основі цієї властивості було запропоновано алгоритми прискореного обчислення елементів V_k –послідовності з можливістю мультиплікативної зміни індексу, що забезпечило можливість обчислення елементів $v_{n\cdot m,k}$ та $v_{-n\cdot m,k}$.

Представлені методи цифрового підписування дозволили одразу вирішити дві проблеми – підвищити стійкість цифрового підписування, оскільки замість числа $s = (b + a \cdot r) \bmod q$ згідно відомого методу тепер передається елемент послідовності $v_{s,k}$ з відповідним індексом, а також суттєво спростити обчислювальну складність процедури перевірки підпису, оскільки замість двох піднесень до степеня згідно відомого методу тепер необхідно виконувати лише одне обчислення елементу $v_{-a\cdot r,k}$ за прискореним алгоритмом обчислення елементів V_k –послідовності.

І, хоча при цьому виникає необхідність при формуванні підпису виконувати три обчислення елементів V_k –послідовності за прискореним алгоритмом замість двох піднесень до степеня згідно відомого методу, однак, існує багато задач, в яких перевірку цифрового підпису необхідно здійснювати значно частіше, ніж його формування, або перевіряти підпис від великої кількості його власників, як то в клієнт-серверних задачах.

Також слід враховувати, що в представлених методах цифрового підписування можна спростити обчислення, змінивши їх шляхом уникнення необхідності обчислення набору елементів для $v_{s,k}$, який передається потім від підписанта одержувачу, і передавання лише самого значення s, так як це робиться у відомому методі. При цьому дещо зменшиться стійкість методів.

Окрім того, що запропоновані методи є більш стійкими, ніж відомі аналоги, вони ще й дозволяють змінювати стійкість методу залежно від параметру k –порядку послідовності, а також мають значно простішу процедуру завдання параметрів.

УДК 621.391.83 (043.2)

П.Ю. Войдюк
Національний авіаційний університет, м. Київ

АНАЛІЗ ЗАХИЩЕНОСТІ ПРИМІЩЕНЬ ВІД ВИТОКУ ПО АКУСТИЧНОМУ КАНАЛУ ІНФОРМАЦІЇ

Інформацію, яку прийнято вважати конфіденційною, що поширюється в межах об'єкту інформаційної діяльності, як правило поширюється в акустичному вигляді (мовна інформація). Носієм мовної інформації являються акустичні коливання частинок в вигляді звукових хвиль різної довжини в пружних середовищах. При веденні переговорів в деякому приміщенні формується звукове поле, яке являється простором, в якому розповсюджуються звукові коливання. Ось тут і виникає акустичний канал витоку інформації, яку необхідно захистити при умові, що шум не буде заважати спокійному веденню переговорів. Вивчення даного питання дуже актуальне в сучасному суспільстві, так як існує потреба в захищенні конфіденційної інформації від шпигунів та зловмисників.

Дана тема на сучасному етапі розвитку суспільства являється дуже актуальною науковою і практичною задачею, оскільки інформація, записана в одній випадковій розмові може розкрити конфіденційні плани установ чи інших конкретних дій, визначити його стратегічний розвиток на деякий час.

Мета даної роботи – створення теоретичної моделі захищеності приміщення мовної інформації від викрадення по акустичному каналу витоку інформації, що циркулює в межах заданого приміщення з врахуванням параметрів даного приміщення, з врахуванням процесу реверберації, сигналу зашумлення та статистичних характеристик розбірливості мови.

Дана теоретична модель захищеності приміщення мовної інформації дозволяє більш раціонально використовувати засоби та час без використання дорого коштуючої апаратури на теоретичному рівні; при цьому захистити приміщення від викрадення по акустичному каналу витоку інформації, що циркулює в межах заданого.

Основним показником ефективності оцінювання мовного сигналу є поріг мінімальної розбірливості. Отже, основним кри-

терієм захищеності акустичних каналів слід вважати величину розбірливості мовного сигналу на виході оцінюваного каналу витоку інформації. Істотне значення на рівень розбірливості мови надає реверберація, обумовлена геометричними особливостями замкнутих приміщень.

Показник словесної розбірливості як похідне від загальної розбірливості, служить основою методики оцінки ефективності закриття технічних каналів витоку мовної інформації. Вибір завади при захисті акустичних каналів витоку здійснюється відповідно до забезпеченням мінімуму складової розбірливості мови. Отже, енергетичний спектр оптимальної маскуючої перешкоди повинен з точністю до постійного множника повторювати спектр акустичного сигналу.

УДК 004.056.5 (043.2)

Б.Е. Журиленко, Н.К. Николаева, Н.С. Пелих
Национальный авиационный университет, г. Киев

ФИНАНСОВЫЕ ЗАТРАТЫ НА ПОСТРОЕНИЕ КОМПЛЕКСА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Для защиты секретной, конфиденциальной и “ноу-хау” информации от утечки по техническим каналам необходимо создавать комплекс технической защиты информации (КТЗИ). Фирмы и предприятия, которые будут создавать такой КТЗИ, в первую очередь, будет интересовать экономическая выгода применения того или иного КТЗИ. Из всех возможных параметров понятных для экономических расчетов, являются величины рисков полных финансовых потерь и величины рисков вложенных потерь. Для расчетов этих рисков исходными параметрами могут быть начальные финансовые потери без защиты, вероятность взлома защиты при определенной попытке взлома и финансовые затраты на выбранную защиту с данной вероятностью взлома.

В связи с этим, целью данной работы были – попытка разработки метода расчета вероятности взлома КТЗИ в зависимости от вложенного на него финансирования. Попытка определе-

ния критерия для оптимизации расходов на построение КТЗИ и оптимизации финансовых потерь в случае взлома ТЗИ.

Теоретическое обоснование для метода расчета финансовых затрат на построение КТЗИ основывается на анализе допустимых рисков общих и вложенных финансовых потерь применяемого КТЗИ. В процессе анализа величины рисков в общем виде не ограничиваются и берутся в виде степенного ряда. Рассматриваются три возможных случая рисков финансовых потерь и эффективности используемой ТЗИ. Первый случай – это случай не эффективного вкладывания финансирования при разработке ТЗИ, когда даже при бесконечном вкладывании финансирования в данную защиту всегда существует некоторая вероятность ее взлома. Второй случая, когда вкладываемое финансирование на защиту является оптимальным, то есть выполняется принцип достаточности между вкладываемым финансированием на ее защиту и вероятностью взлома. И третий – это, когда "гарантируется" большая защищенность по сравнению с оптимальной защищенностью. Получены выражения, определяющие вероятность взлома и эффективность вложенного финансирования в построение КТЗИ.

На основании проделанной работы были сделаны следующие выводы.

Использование одноуровневой защиты (одиночной защиты) абсолютно неэффективно, потому что даже при бесконечном вложении финансирования на такую защиту нельзя получить достаточный уровень величин рисков финансовых потерь. Минимальное количество защит, которое может быть использовано для достижения необходимого уровня величины рисков, должно быть не менее двух. Использование многоуровневой защиты позволит более эффективно защитить информацию при одинаковых финансовых затратах.

Получены выражения для расчета вероятности взлома информации, как от величины вложенного финансирования, так и от количества попыток взлома. Определены оптимальные соотношения между попытками взлома и вкладываемым в защиту финансированием. Оказалось, что вполне достаточно рассчитывать защищенность до второй или третьей попыток взлома одиночной защиты, но для более существенного уменьшения вели-

чины рисков потерь необходимо использовать многоуровневую защиту.

В многоуровневой защите необходимо на каждую из единичных защит вкладывать одинаковое финансирование, что позволит добиться минимальных величин рисков финансовых потерь. Уменьшить вклад финансирования в разработку защиты может позволить долевая защита потерь каждой из одиночных защит.

Получены выражения для расчета величин рисков потерь соответствующие реальным системам защиты, которые получаются при использовании той или иной защиты. Определяется эффективность применения той или иной единичной защиты. Получено выражение, с помощью которого можно рассчитать величины рисков полных финансовых потерь любой многоуровневой защиты, определить эффективность не только одноуровневых защит, но и всего КТЗИ, а также использовать реальные параметры единичных защит таких как вероятность их взлома и затрат на их разработку или модернизацию.

При дальнейших экономических расчетах, зная прибыль от защищенной системы и необходимых затрат на защиту, можно обосновать экономическую выгоду при внедрении КТЗИ.

ЗМІСТ

Сорокун А.Д. Мережеві технології PLC в телекомунікаціях..... 3

Лисенко А.С. Побудова мережі мобільного зв'язку LTE у Солом'янському районі м. Києва..... 4

Василюк І.В. Телекомунікаційна мережа банківської установи. Розробка, проектування, розрахунок параметрів. Пропозиції щодо модернізації мережі..... 6

Кохан И.В., Кочубей А.Б. Методы скрытого подсоединения к оптоволокну..... 7

Бур'янцев Д.Б. Захист від несанкціонованого доступу до даних у хмарних сервісах..... 9

Романюк Ю.В. Бездротовий сегмент захищеної корпоративної мережі.....10

Ступаков Ю.В. Комплексна система захисту приміщення від витоку мовної інформації.....12

Бахтіяров Д.І. Захищена корпоративна мережа авіапідприємства на базі обладнання D-Link.....13

Черкай А.Ю. Підвищення ефективності управління пакетним трафіком.....15

Василенко О.І. Формування пакетного трафіка для забезпечення роботи засобів адаптивного управління.....16

Сказатня Є.В. Дослідження впливу параметрів надійності та завадостійкості каналу на ефективну швидкість передачі даних....18

Чуприна Ю.В. Удосконалення технологій резервування телекомунікаційного обладнання.....19

Солнцева М.М. Абонентський термінал GSM.....20

Євсєєв О.О. Оптимізація параметрів псевдовипадкових бінарних послідовностей в широкосмугових телекомунікаційних системах.....22

Шатирко А.Ф. Встановлення NGN в місті Києві. Розробка, проектування, розрахунок параметрів.....23

Севрюгіна К.В. Управління доступом до ресурсів мережі LTE.....25

Грищенко Т.А. Вопросы интеграции распределенных биометрических систем в общегосударственные базы персональных данных.....26

Сокирка Є.О. Моделювання ІКМ підприємства з балансуванням навантаження....29

Козак Я.О. Мережа підприємства на базі сучасних бездротових технологій....31

Несімока Д.М. Опорний сегмент мереж WiMAX для міських умов....32

Васюков Ю.В. Системи зв'язку з розширеним спектром сигналів....34

Тимошевська Т.Є. Використання хмарних технологій на авіапідприємстві....35

Павловський А.Ю. Радіопідсистема мобільної мережі LTE....37

Новікова А.В. Реалізація основних типів файерволів різних рівнів моделі OSI....38

Пантелеєв О.Ю. Протоколи захищеного каналу....40

Морозова Г.О. Відомча система зв'язку на базі обладнання Goodwin SPREE....41

Москвич Д.М. Телекомунікаційна мережа четвертого покоління із заданим рівнем якості обслуговування абонентів....43

Синьогуб С.Г. Створення механізмів налаштування протоколів маршрутизації маршрутизаторів CISCO....44

Шовковий Є.О. Системи захисту мереж мобільного зв'язку від несанкціонованого доступу....46

Антух А.И. Методика определения оптимальной топологии сети GSM для городского микрорайона....47

Рибак П.О. Оцінка якості обслуговування абонентів супутникових мереж зв'язку....48

Суман А.К. Организация защищенного доступа к серверу на базе ОС Microsoft Windows Server 2008....50

Зінченко Н.О. Проектування обладнання для передавання мовного трафіку каналами пакетної мережі....51

Кононенко Д.А. Розробка лабораторних робіт з дисципліни «Волоконно-оптичні системи передачі»....53

Величко К.В. Оптимізація структури захищеної корпоративної мережі....55

Піддубний В.В. Районована міська телефонна мережа в м. Пирятин....56

Корнієнко О.О. Система захисту інформаційних ресурсів мереж LTE....58

Сачук Р.С. Телефонна мережа м. Біла Церква....59

Кривоус В.Т. Оптимізація архітектури систем управління мереж 3G....61

Кукулевський І.О. Підвищення гарантованості захисту інформації в корпоративних мережах до рівня ГЗ....62

Антонюк О.В. Волоконно-оптична лінія зв'язку....63

Ткач А.В. Оцінка завадостійкості та швидкості передавання антенних систем MIMO....65

Хромов А.І. Виявлення загроз за допомогою методу ієрархій....67

Вовченко А.Є. Міська телефонна мережа з сегментом мережі NGN....68

Бабенко Є.М. Моделювання затухань в каналах зв'язку WiMAX....69

Журиленко Б.Е., Николаева Н.К., Самосуд З.О. Поиск закладного устройства с помощью лазерного луча....71

Пузиренко О.Ю. Канали стеганографічного передавання даних у системах цифрового мовлення....73

Соломенцев О.В., Заліський М.Ю., Зуєв О.В., Соловйов Д.О. Статистичні моделі ймовірності безвідмовної роботи засобів зв'язку....74

Тимченко Ю.В. Моделювання випадкових процесів із заданими властивостями....76

Осипова В.Е. Моделирование случайных процессов с заданными корреляционными свойствами....77

Гарасим Ю.Р., Ромака В.А., Полуектова О.Л. Застосування SWOT-підходу для структуризації даних про події в розподілених системах захисту інформації....79

Борейчук О.М. Вибір оптимального методу модуляції сигналу в цифрових системах радіозв'язку....80

Голубничий О.Г. Аналіз вимог та рекомендацій ІСАО до захисту сеансів зв'язку «земля–земля» в мережі ATN....82

Яковишин К.Н., Скрипчинская Э.В. Новое в учебной практике моделирования телекоммуникационных систем.....83

Яремчук Ю.Є. Про можливість цифрового підписування на основі рекурентних послідовностей.....86

Войдюк П.Ю. Аналіз захищеності приміщень від витоку по акустичному каналу інформації.....88

Журиленко Б.Е., Николаева Н.К., Пелих Н.С. Финансовые затраты на построение комплекса технической защиты информации.....89

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

3 – 6 ЧЕРВНЯ 2013 Р.

М. КИЇВ

ВІДПОВІДАЛЬНИЙ РЕДАКТОР КОНАХОВИЧ Г.Ф.

КОМП'ЮТЕРНА ВЕРСТКА ГОЛУБНИЧИЙ О.Г.

КОНТАКТНИЙ E-MAIL a.holubnychyi@nau.edu.ua

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

ПІДП. ДО ДРУКУ 13.05.2013 Р.
УМ. ДРУК. АРК. 6,0. ОБЛ.-ВИД. АРК. 5,6.

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

ЗМІСТ ТА СТРУКТУРА ЕЛЕКТРОННОЇ ВЕРСІЇ ЗБІРНИКА ТЕЗ
ПОВНІСТЮ ВІДПОВІДАЄ ЙОГО ДРУКОВАНІЙ ВЕРСІЇ.