УДК 355.40

МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ ЦИФРОВОГО МОВЛЕННЯ

ГОНЧАРУК Д.С., КОНОНОВИЧ В.Г.

ОРЦ ТЗІ ВАТ "Укртелеком", ОНАЗ

MECHANISMS OF INFORMATION SEQURITY OF THE DIGITAL BROADCASTING

GONSHARUK D., KONONOVICH V.

ORC TPI OAA "Ukrtelecom", ONAT

ВСТУП

За останні десятиліття в сфері телекомунікацій сталися вражаючі зміни. Традиційна телефонія, яка накопичила на Землі більше одного мільярда ліній стаціонарного телефонного зв'язку, досягла вершини свого розвитку. Інтернет став масовою технологією, кількість його користувачів нараховує близько 500 мільйонів, популярними є *IP* - телефонія, широкосмугові телекомунікаційні послуги, мультимедіа. Вимоги до інформаційної безпеки телекомунікацій зросли внаслідок лібералізації телекомунікацій; змін в технологіях та послугах; підвищення залежності суспільства від послуг телекомунікацій; підвищення національних і міжнародних вимог у відношенні захищеності інформації з метою забезпечення національної безпеки. Телекомунікації еволюціонують від аналогових телекомунікаційних мереж до цифрових мереж наступного покоління, які надають інформаційно-телекомунікаційні послуги.

Фахівці вважають [1], що приблизно кожні п'ять років наші уявлення щодо перспективних технологій, їх обладнання, організаційних аспектів, методів вирішення ключових задач і навіть щодо магістральних напрямів розвитку мереж переглядаються, у крайньому разі, майже наполовину. Телекомунікації досягли такого рівня свого кількісного розвитку, коли ліквідовано дефіцит каналів зв'язку, досягнута значна пропускна здатність. В результаті вартість такого ресурсу, як канали зв'язку, стала падати.

Продовжується процес підвищення ступеню інтеграції мереж. Будівельними елементами (модулями) телекомунікацій ставали (в порядку підвищення ступеню інтеграції): електричні та логічні елементи, інтегральні схеми та мікропроцесори, великі й надвеликі інтегральні схеми та мікро-ЕОМ, «інтегральні» функціональні блоки зі стандартизованими інтерфейсами для взаємодії з іншими блоками та *API* для взаємодії з користувачем, багатофункціональні (агрегатні) інтелектуальні модулі з автоматичним вибором режимів роботи та протоколів взаємодії із зовнішнім середовищем тощо. Тепер будівельним модулем телекомунікацій стають мережі: домашні, домові, локальні та корпоративні обчислювальні мережі, кластери інтелектуальних мереж. Раніше мережі зв'язку складались з пучків каналів зв'язку та вузлів комутації, де інформація розподілялась. Тепер телекомунікаційні системи будуть комплектуватись з мереж, які взаємодіють через шлюзи, де розподіл інформації буде здійснюватись програмними комутаторами [2]. Телекомунікації набувають властивості самоорганізації. В цих умовах інформаційна безпека мереж стає все більш актуальною.

Метою даної роботи є визначення функціональних профілів та механізмів захисту інформації в мережі цифрового мовлення як частини мультисервісної мережі.

АРХІТЕКТУРА МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Технологічною основою мультисервісної мережі є технічні засоби мережі наступного покоління (*NGN – Next Generation Network*). Мета створення *NGN*, яка декларується Рекомендаціями ITU-T Y.2001, Y.2011 [3, 4], полягає у наступному: забезпечення відкритого доступу до мереж; забезпечення універсальних умов та доступу до послуг (сервісів); сприяти рівним можливостям громадян; сприяти різноманіттю змісту, зокрема культурному і лінгвістичному; визнавати потреби всесвітнього співробітництва зі специфічною увагою до слабо розвинутих країн. Для *NGN* характерні цифровізація, пакетизація, конвергенція інформаційних та телекомунікаційних технологій і, як результат, невпинне зростання кількості і якості інформаційних та телекомунікаційних послуг, мультисервісних послуг передачі даних і голосових сервісів.

Технічною основою сучасного інформаційного середовища повинні стати мультимедійні системи, що забезпечують цифрову передачу динамічних зображень, мови, звуку, інших даних каналами різною пропускною спроможністю (відеотелефон, стаціонарний і мобільний конференц-зв'язок, інтерактивні телевізійні системи та ін.). Впровадження мультимедійних систем різного призначення при мінімальних капітальних і експлуатаційних витратах вирішує проблеми: створення високоякісних систем інтерактивного цифрового телебачення цифрового мовлення; розробки й впровадження принципово нових систем мобільного телебачення; створення принципово нових інтерактивних систем громадської думки; забезпечення діяльності органів державної влади; створення мобільного телеконференц-зв'язку між центральними установами районами, а також районів між собою; радіотехнології рухомих мереж третього і четвертого поколінь (3*G*, 4*G*).

Архітектуру NGN можна представити у вигляді набору рівнів або страт. Нижнім є рівень абонентського доступу, що базується на трьох середовищах передачі: металевому кабелі, оптоволокні й радіоканалах. До *NGN* будуть підключатись аналогові телефонні апарати, факси, *ISDN*-термінали, мобільні телефони, термінальні пристрої *GPRS* (*General Packet Radio Service* – загальний пакет радіопослуг), термінали *SIP* (*Session Initiation Protocol*), персональні комп'ютери, *IP*-телефони через персональні комп'ютери, цифрові музикальні пристрої (*digital set top boxes*), кабельні модеми (кодеки лінійного коду) тощо.

Далі йде рівень комутації − комутації каналів й/або на цьому рівні перебуває й структура мультисервісних вузлів доступу. Вище розташовуються програмні комутатори (*Softswitch*), складові рівня програмного керування. Ще вище перебуває рівень інтелектуальних послуг й експлуатаційного керування.

Транспортна мережа є опорною мережею в багаторівневій архітектурі телекомунікаційної мережі. Транспортна мережа повинна бути високопродуктивною й будуватися на основі волоконно-оптичних ліній зв'язку, що дозволить забезпечити більшу швидкість обміну (до 100 Мбіт/с), уникнувши заторів і колізій при маршрутизації потоків.

Функціональні можливості *NGN* можна розглянути за їх розподілом за стратами. Транспортні функції належать до транспортної страти, а функції обслуговування, які відносяться до застосувань, розміщуються в страті обслуговування (надання послуг).

Страта транспорту – це та частина *NGN*, яка забезпечує функції користувача, що передають дані та функції, що виконують керування та менеджмент транспорту ресурсів для переносу цих даних між кінцевими об'єктами. Дані, які переносяться, можуть бути даними користувача, управління (сигналізації та контролю) і/або керування (менеджменту). Динамічно чи статично може бути встановлене управління (контроль) і/або керування (менеджмент) передачі інформації між певними об'єктами. З точки зору архітектури передбачається, що кожна страта послуг включає в себе свої площини користувача (даних), сигналізації та контролю і менеджменту.

Транспортні функції забезпечують можливість з'єднання. Функції транспортної страти використовують для з'єднання об'єкти і функції мережного, канального та фізичного рівнів, визначені у основній семирівневій моделі *OSI*. Щоб взаємодіяти, мережа більш високого рівня запитує послуги від мережі більш низького рівня. Зокрема, транспортна страта дає можливість: з'єднання користувач-користувач; з'єднання платформи користувача з послугами; з'єднання платформи послуг з платформою послуг.

У транспортній страті можуть бути розгорнуті будь-які мережні технології, зокрема, орієнтовані на з'єднання: комутація каналів, комутація пакетів, не орієнтована на з'єднання комутація пакетів. Для надання послуг *NGN* та підтримки успадкованих послуг віддають перевагу застосуванню *IP*.

Страта послуг – це та частина *NGN*, яка забезпечує функції користувача, що передають зв'язані з послугами дані і функції, які виконують керування (сигналізацію і контроль) і менеджмент ресурсів послуг та ресурсів мережі, щоб забезпечити послуги користувачів та застосування. Послуги користувачів (обслуговування користувачів) можуть бути здійснені рекурсією багатократних рівнів послуги всередині страти. В страті послуг *NGN* розглядаються ті застосування і їх послуги, які функціонують між взаємодіючими (рівними за положенням) об'єктами. Приміром, послуги можуть відноситись до голосу, даних, або відеозастосувань, встановлених окремо або в деякій комбінації у випадку мультимедіа застосувань. З точки зору архітектури передбачається, що кожен рівень страти послуг включає в себе свої площини користувача (даних), сигналізації та контролю і менеджменту.

Сервісні платформи забезпечують використання послуг, таких як телефонне обслуговування, *WEB*-послуги тощо. Послуги забезпечуються сукупністю модулів прикладних функцій, які можуть бути викликані. В страті послуг можуть бути: голосові сервіси, зокрема телефонні послуги, аудіо, факс тощо; послуги передачі даних, зокрема *WWW, E-mail* тощо; відео послуги, зокрема без обмежень мовлення, кіно, телебачення тощо; комбінація послуг, приміром мультимедійні послуги типу відеотелефон та ігри. Послуги можуть надаватись у реальному часі і не в реальному часі. Послуги можуть надаватись як однонаправлені, широкомовні і радіомовні.

Розглянемо відношення між функціями, послугами та ресурсами, які повинні бути визначені для двох страт *NGN*. Послуги та функції зв'язані між собою, оскільки функції використовуються для побудови послуг. Але не існує безпосередніх зв'язків між функціями і послугами, тому вони повинні залишатись незалежними. Одна й та ж функція (приміром, автентифікація користувача) може бути використана для надання двох різних послуг.

Послуги можна поділити на: інфраструктурні та прикладні послуги; послуги проміжного програмного забезпечення; послуги базового програмного забезпечення, включаючи телекомунікаційні послуги; ресурси (такі як обробка і зберігання компонентів послуг). Зручно зібрати ці функції в дві окремі групи або площини і в одну включити всі функції управління, а в іншу включити всі функції менеджменту послуг. Групування функцій дозволяє визначені функціональні взаємозв'язки у межах даної групи, а також інформаційні потоки між функціями в даній групі. На рис. 1 наведена *загальна функціональна схема NGN*.

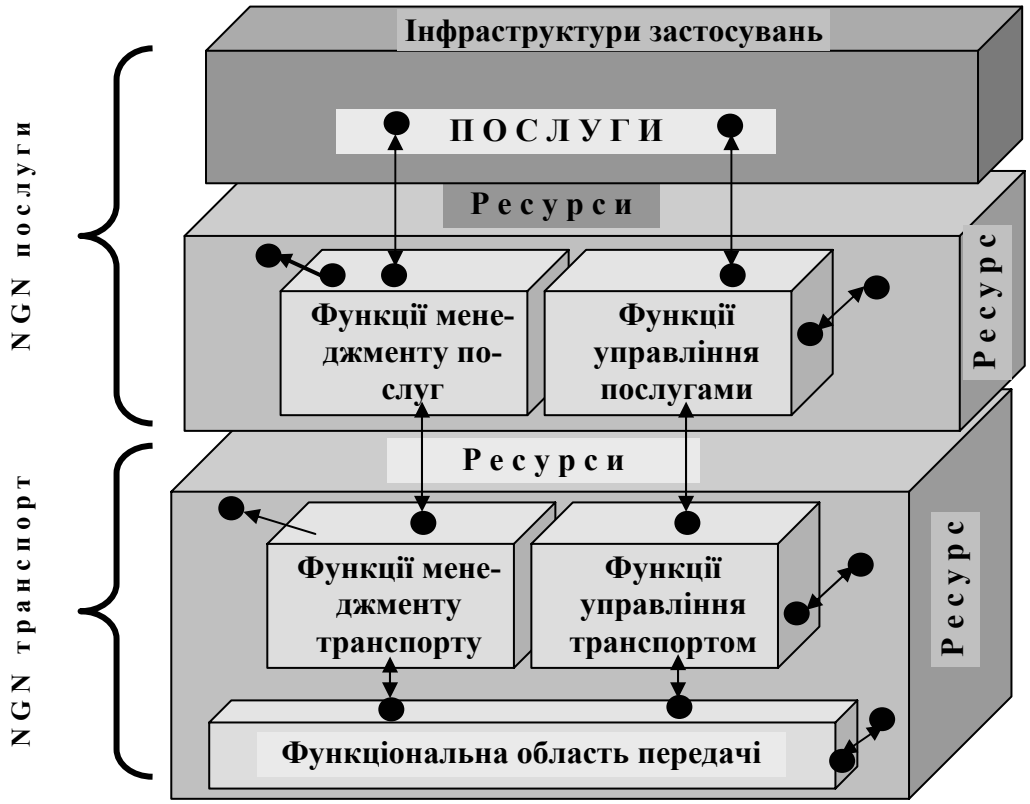

Рисунок 1 – Загальна функціональна схема *NGN*.

Ресурсами називають фізичні і логічні компоненти, які використовуються для створення мереж, засобів встановлення з'єднань та забезпечення послуг. Поняття ресурсів глобальної інформаційної інфраструктури включають у себе сукупність ресурсів, обробки і зберігання ресурсів та проміжне програмне забезпечення, які забезпечують надання послуг користувачам. Ресурси повної моделі *NGN* повинні бути незалежні від функцій та послуг. Функції менеджменту у взаємодії з ресурсами використовуються для побудови послуг. Функції управління і функції передачі взаємодіють послугам та ресурсами.

***Функції управління (сигналізації та контролю – Control*).** Підтримка мультимедійних та інших типів послуг в умовах можливостей узагальненої мобільності вимагає функцій управління, обслуговування залежить від розподілу ресурсів мережі функціями управління або менеджменту. Під «управлінням» розуміють процеси, які відносяться до процесу обслуговування викликів. Функції управління, залучені до процесу обслуговування виклику, можуть бути згруповані у дві сукупності, функції, які відносяться до управління послугами (наприклад, такі як автентифікація користувача, ідентифікація користувача, управління доступом до послуги, функції сервера застосувань) та функції, які відносяться до управління мережним транспортом (наприклад, такі функції, як управління доступом до мережі, управління ресурсами/політикою мережі, забезпечення діючих з'єднань).

***Функції керування* (*менеджменту - management*).** Необхідно мати на увазі, що деякі процеси дій клієнта дуже добре корелюють з процесом «виклику» при взаємодії з мережею, а також перед викликом послуги та після виклику послуги. Такі процеси зазвичай називають «менеджментом» на відміну від процесів управління під час обслуговування самого виклику (управління процесами надання послуги кінцевому користувачу). Вимоги площини менеджменту повинні розглядатись як процеси і вимоги менеджменту, визначені в *TMN*. Функції *TMN* менеджменту класифікують згідно функціональної області менеджменту, який позначають як категорії менеджменту *FCAPS* (*Fault, Configuration, Accounting, Performance, Sequrity*), а саме: менеджмент надійності (обробки несправностей, пошкоджень та помилок); менеджмент конфігурації (працездатності); менеджмент розрахунків (адміністрування); ме-

неджмент продуктивності (функціонування, постачання, забезпечення пропускної здатності тощо); менеджмент безпеки (надійності, конфігурації, розрахунків).

Менеджмент в страті транспорту добре вивчений, але менеджмент в страті послуг ще чекає свого вивчення. Очікується, що менеджмент двох страт *NGN* буде подібний відносно поведінки об'єктів менеджменту (наприклад конфігурація ресурсів послуг як конфігурація ресурсів транспорту). На відміну від традиційних мереж у структурі *NGN* утворено додатковий шар – керування комутацією транспортної мережі. Він організується за допомогою програмних комутаторів – *Softswitch* – які підтримують трансляцію основних протоколів *VoIP* у протоколи традиційних мереж при взаємодії з ними, керують обробкою телефонних викликів, що відбуваються в різних мережах, зокрема в мережах з комутацією пакетів.

Функції транспорту. Функції транспорту повинні зберігати незалежність від відповідного керування і менеджменту. Транспортна мережа повинна передавати як інформацію користувача, так і мережну інформацію (таку як інформація менеджменту або сигналізації та контролю). Для забезпечення безпеки необхідно розробити: всеохоплюючу архітектуру безпеки для *NGN*; підготувати експлуатаційні керівництва з безпеки *NGN*; експлуатаційну політику безпеки *NGN*; адекватні для *NGN* протоколи безпеки і *API* (програмні інтерфейси застосувань).

ФУНКЦІЇ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

Принципи забезпечення інформаційної безпеки знаходяться у руслі загальних принципів побудови *NGN*, серед яких розглядаються загальні принципи інформаційної безпеки, взаємозв'язок з іншими функціональними можливостями, безпека за рівнями, елементами мережі і безпека «з кінця в кінець» [5]. Інформаційна безпека *NGN* є специфічною проблемою, яка ще повинна бути вирішена поряд і у взаємозв'язку з проблемами впровадження голосових послуг в інфраструктурі *NGN*, якості обслуговування – *QoS,* при наданні голосових послуг у реальному часі (гарантованою смугою пропускання, гарантована затримка голосових пакетів, гарантована не втрата пакетів тощо). Питання забезпечення інформаційної безпеки в *NGN* ще є предметом майбутньої стандартизації і є стратегічною задачею. Забезпеченість безпекою взаємно залежать і розповсюджується на архітектуру, *QoS*, менеджмент мережі, білінг і платежі.

NGN повинна бути забезпечена механізмами безпеки для: захисту обміну вразливою інформацією в її інфраструктурі; захисту проти шахрайського використання послуг, які надаються провайдерами; захисту власної інфраструктури від зовнішніх атак. Безпека як послуга входить до складу послуг менеджменту мережі, поряд із задоволенням вимог до *NGN*: надійності, сталості, підзвітності, спостережності, експлуатаційних властивостей, адміністрування клієнта, навантаження (трафік), керування маршрутизацією (*fault, configuration, accounting/charging, performance, security, customer administration, traffic and routing management*).

Дані щодо найменувань та нумерації мережі є важливими даними, які можуть безпосередньо впливати на функціонування мережі. Вони є також вразливими комерційними даними, які відображають структуру і політику функціонування мережі. Безпека є складовою частиною вимог до системи вибору (розподілу) імен та нумерації. Як мережа загального користування, *NGN* повинна відповідати вимогам надійності, цілісності, захищеності і суверенності. Система вибору (розподілу) імен та нумерації безпосередньо зв'язана з функціонуванням мереж загального користування. Тому важливо, щоб системи вибору (розподілу) імен та нумерації не приводили до протиріч. Повні бази даних для переводу найменування в номер повинні мати дійсні і надійні дані, так щоб результат переводу не порушував цілісність бази в умовах розподіленого використання.

Відповідно, система вибору (розподілу) імен та нумерації має використовуватись лише цією мережею, і повинна мати перевірені (надійні) засоби безпеки. Безпека, головним чином,

підтримується засобами автентифікації доступу користувачів, безпеки (захисту) даних, безпеки (захисту) приватності, синхронізації даних мережі й відновлення після збоїв (пошкоджень та помилок).

Архітектурою безпеки є вимоги, які відносяться в контексті безпеки викликів *NGN* до мережі і постачальників (провайдерів) послуг, підприємств та споживачів. Архітектура безпеки направлена на безпеку менеджменту, сигналізації (управління) та використання інфраструктури мережі, послуг і застосувань. Архітектура безпеки в *NGN* повинна забезпечити всеохоплюючу, зверху-вниз, з кінця в кінець перспективу безпеки мережі і може бути застосована до елементів мережі, послуг, і застосувань для виявлення, прогнозування та коригування вразливостей безпеки.

В табл. 1 наведено розподіл механізмів безпеки за рівнями моделі архітектури ВВС та площинами моделі мереж наступного покоління.

Таблиця 1 − Розподіл механізмів безпеки за рівнями моделі архітектури ВВС та рівнями моделі мереж наступного покоління.

Механізми безпеки	Рівні моделі мереж наступного покоління						
	абонентського доступу		комутації	програмного управління	інтелектуальних послуг та експлуатаційного управління		
	Рівні моделі архітектури ВВС						
	1	2	3	4	5	6	7
1. Шифрування	Так	Так	Так	Так			Так
2. Цифровий підпис			Так	Так			Так
3. Контроль доступу			Так	Так			Так
4. Цілісність даних			Так	Так			Так
5. Обмін автентифікацією			Так	Так			
6. Заповнення трафіка	Так		Так				Так
7. Контроль маршрутизації	Так	Так	Так	Так		Так	Так
8. Нотаріальне засвідчення							Так

Цифрами 1…7 позначені рівні архітектури ВВС: 1 – фізичний, 2 – канальний, 3 – мережний, 4 – транспортний, 5 – сеансовий, 6 – представний, 7 – прикладний.

Рівні абонентського доступу та *IP*-комутації відповідають рівню інтелектуального транспортування трафіка, рівень програмного комутатора відповідає за рівень встановлення з'єднань, а вище є рівень платформи послуг.

Механізми безпеки мають розподілятись за елементами об'єкта захисту. Розглянемо *NGN* як об'єкт інформаційної безпеки. Вимоги до системи інформаційної безпеки повинні враховувати особливості телекомунікаційних мереж наступних поколінь. Архітектура інформаційної безпеки повинна бути узгоджена з архітектурою головних архітектурних рішень. В архітектурі інформаційної безпеки телекомунікаційних систем визначені такі механізми безпеки:

- конфіденційності (техніки криптографії та шифрування), що повинна забезпечувати недоступність та не розкриття технологічної інформації мережі та даних споживачів користувачам, що не мають для цього необхідних повноважень. Крім того, повинна забезпечуватись конфіденційність інформації щодо системи захисту з моменту її інсталяції, навіть якщо використовуються відкриті засоби захисту;

- цифрового підпису;

- керування доступом, що повинна визначати множину припустимих для кожного суб'єкта операцій з кожним об'єктом і контролювати додержання цих специфікацій;

- механізм або служба цілісності даних, що повинна забезпечувати повноту, точність і достовірність переданої мережею інформації та даних споживачів у разі їх зберігання в базах даних мережі;

- автентифікація, що повинна забезпечувати встановлення справжності суб'єктів взаємодії за поданої ними ідентифікаційною інформацією;

- заповнення трафіка;

- контроль маршрутизації;

- неспростовність (нотаризація), що повинна забезпечувати неможливість відмови власника інформації від неї, неможливість спростування споживачами послуг документальних телекомунікацій факту передавання чи приймання інформації.

ВИСНОВКИ

Інформаційна безпека системи цифрового мовлення невід'ємно інтегрована в систему інформаційної безпеки мереж наступного покоління. В цілому проблема захисту інформації в мережах наступного покоління потребує свого вдосконалення.

Література

1. Олифер В.Г., Олифер Н.А. Компъютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – Спб.: Питер, 2001. – 672 с.

2. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии/ Б.И. Крук, В.Н. Попантопуло, В.П. Шувалов; под ред. проф. В.П. Шувалова.– М: Горячая линия – Телеком, 2004.–647 с. Том 2 – Радиосвязь, радиовещание, телевидение/ Г.П. Катунин, Г.В. Мамчев, В.Н. Попантопуло, В.П. Шувалов; под ред. проф. В.П. Шувалова.– М: Горячая линия –Телеком, 2004.–672 с. Том 3– Мультисервисные сети/ В.В. Величко, Е.А. Субботин,, В.П. Шувалов, А.Ф. Ярославцев; под ред. проф. В.П. Шувалова.– М: Горячая линия –Телеком, 2005.–592 с.

3. Рекомендація Y.2001 ITU-T. Глобальна інформаційна інфраструктура. Загальний огляд мереж наступного покоління (NGN).

4. Рекомендація Y.2011 ITU-T. Глобальна інформаційна інфраструктура. Загальні принципи і основні поняття моделі для мереж наступного покоління.

5. ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. C. 28.

6. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries. «Security Considerations for Voice Over IP Systems». Recommendations of the National Institute of Standards and Technology. – NIST SP 800-58, January 2005. – S. 93.