Cryptology. – 1995. – № 8. – P. 167-173. ***26.*** *Bierbrauer J., Gopalakrishnan K., Stinson D. R. Orthogonal arrays, resilient functions, error correcting codes and linear programming bounds // Advances in Cryptology – CRYPTO' 94, Proceedings. – Springer Verlag, 1994. – P. 247-256.* ***27.*** *Дельсарт Ф. Алгебраический подход к схемам отношений теории кодирования. – М.: Мир, 1976. – 134 с.* ***28.*** *Зиновьев В. А., Эриксон Т. О Фурье-инвариантных разбиениях конечных абелевых групп и тождестве Мак-Вильямс для групповых кодов // Проблемы передачи информации. – 1996.– Т. 32.– Вып. 1. – С.137 – 143.* ***29.*** *Кузьмин А. С., Нечаев А. А. Линейно представимые коды и код Кердока над произвольным полем Галуа характеристики 2 // Успехи матем. наук – 1994. – Т. 49. – № 5. – С. 165 – 166.* ***30.*** *Нечаев А. А. Код Кердока в циклической форме // Дискретная математика. – 1989. – Т. 1. – Вып. 4. – С. 123-139.* ***31.*** *Hammous A. R., Kumar P. V., Calderbrank A. R., Sloane N. J. A., Sole P. The Z_4-linearity of Kerdock, Preparata, Goethals and related codes // Bull. Amer. Math. Soc. – 1993. – V. 29. – №. 2. – P. 218-222.* ***32.*** *Кузьмин А. С., Нечаев А. А. Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа // Успехи матем. наук – 1992. – Т. 47. – № 5. – С. 183 – 184.*

УДК 681.321;322:621.395

АНАЛІЗ ПРОБЛЕМИ РОЗПОДІЛУ ВИТРАТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Володимир Кононович, Микола Тардаскін, Тетяна Тардаскіна*

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком",
**Одеська національна академія зв'язку*

Анотація: **Розглядаються проблеми розподілу засобів інформаційної безпеки по елементам інформаційно-телекомунікаційних систем, формулюється задача оптимізації витрат на інформаційну безпеку.**

Summary: **The problem of information security devices distribution on the elements of information telecommunication systems is considered and the task of optimization expenses for information security is formulated.**

Ключові слова: **Інформаційна безпека, автоматизовані системи, інформаційно-телекомунікаційні системи, загрози, послуги та механізми безпеки, функціональний профіль захисту.**

І Вступ

З розширенням ролі інформаційно-телекомунікаційних систем в роботі органів державного управління, в обробці електронних документів, в освіті, бізнесі та інших сферах інформаційної діяльності зростає увага до інформаційної безпеки. Вдосконалення сучасних мереж, як загального користування, так спеціальних і корпоративних здійснюється в умовах підвищення вимог до надійності функціонування зв'язку, сталості та інформаційної безпеки телекомунікаційних мереж, якості та безпеки телекомунікаційних послуг. Актуальною стає задача побудови "довіреного" телекомунікаційного середовища. За методами побудови серед систем забезпечення інформаційної безпеки виділяються накладені, тобто побудовані "поверх" існуючих систем [1, 2], та вбудовані як підсистеми захисту інформаційних ресурсів. Приміром, в АТМ-мережах рекомендуються до застосування три основні механізми захисту інформації: шифрування інформації з метою збереження її конфіденційності, автентифікації аспектів інформаційної взаємодії, контроль цілісності й незмінності даних при передаванні та зберіганні [3]. Міжнародні рекомендації щодо нових телекомунікаційних технологій включають вбудовані підсистеми інформаційної безпеки [4, 5].

При виборі функціонального профілю захисту інформаційно-телекомунікаційних систем або частин їх декомпозиції є актуальною задача оптимального розподілу послуг та механізмів безпеки поміж елементами інформаційно-телекомунікаційної системи. Необхідне використання механізмів захисту, які підвищують загальний рівень безпеки телекомунікаційної мережі й дозволяють дати більш високу гарантію відносно окремих вузлів і мереж у цілому.

Метою даної роботи є аналіз проблем оптимального розподілу послуг і механізмів безпеки в інформаційно-телекомунікаційних системах та пошук методів зниження загальних витрат на інформаційну безпеку.

II Взаємозалежність задач безпеки інформаційно-телекомунікаційних систем

Носії загроз безпеці поділяють на потенційні техногенні або стихійні і антропогенні. Як джерела загроз можуть виступати як об'єктивні прояви так і суб'єкти (особи). Техногенні чинники впливають як на зовнішню, так і на внутрішню безпеку, вони порівняно добре вивчені, місця їхньої дії локалізовані і в системі технічної експлуатації організовані заходи протидії завадам передаванню сигналів, збоям, відмовам обладнання тощо. Техногенні джерела загроз безпосередньо залежать від властивостей техніки та системи технічної експлуатації.

Відносно загроз техногенного і стихійного характеру взаємозалежність і взаємозв'язок задач безпеки і якості технології можна проілюструвати рис. 1, де суцільними стрілками показані відношення взаємозалежності та взаємозв'язку, а пунктирними – відношення опосередкованого входження.

Конфіденційність залежить від цілісності і, в свою чергу, від надійності. Якщо цілісність і надійність системи буде порушена, то, скоріш, знизиться ефективність механізмів конфіденційності [6]. Навпаки, порушення конфіденційності, приміром технологічної інформації, приведе до можливості обходу механізмів цілісності, доступності і спостереженості. Також, якщо буде порушена цілісність системи, то це приведе до компрометації механізмів доступності і спостереженості.

Показники доставки інформації – ймовірність втрат і перекручувань повідомлень (достовірність), час затримки, помилки адресації споживача і джерела повідомлень – впливають на ефективність механізмів конфіденційності і цілісності.

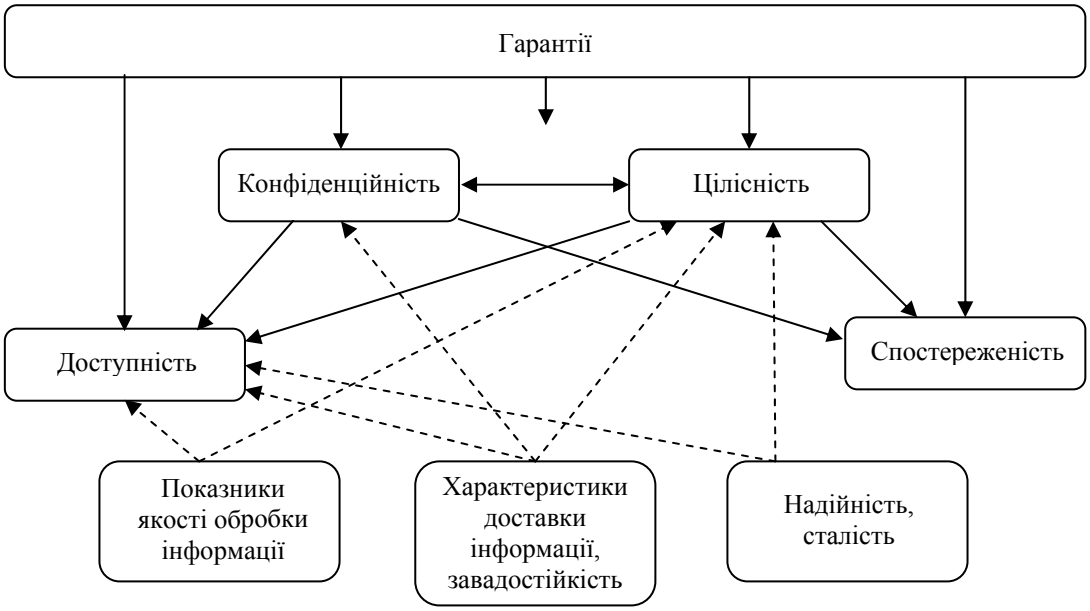

Рисунок 1 – Взаємозалежність задач безпеки і якості технологій

Показники якості в узагальненому вигляді входять у характеристики цілісності й доступності. Характеристики доставки інформації споживачеві та інших інформаційно-телекомунікаційних послуг в узагальненому вигляді входять у показники доступності і, частково, у показники конфіденційності й цілісності [7]. Достовірність і надійність опосередковано взаємопов'язані з властивостями конфіденційності, цілісності, доступності. Кількісна або якісна недостатність компонентів системи впливає на показники ефективності захисту інформаційних ресурсів.

Сказане підтверджується тим, що у міжнародних стандартах (BS ISO/IEC 7799:2000) спостерігається тенденція до суміщення сертифікації системи інформаційної безпеки із сертифікацією на відповідність стандартам якості ISO 9001 або 9002 [8].

Усі задачі інформаційної безпеки і якості залежать від розв'язку задач забезпечення гарантій.

Звичайно, що в технічній сфері і в сфері безпеки склалися різні підходи до ряду розглянутих понять і в різних сферах в них укладається різний смисл. Так поняття цілісності вміщує в себе не лише збереження кількісних характеристик інформації – бітів і байтів, а й семантичних характеристик інформації – змісту

повідомлень. В сфері безпеки властивості інформації розглядаються з точки зору як техногенного, так і антропогенного впливу. Проте різниця у поняттях не може бути перешкодою для комплексного аналізу. Показник цілісності є складною функцією надійності, завадостійкості, спостереженості й доступності. Розділити такі поняття, скоріш, неможливо.

Цілісність телекомунікаційних мереж, систем передавання, іншого обладнання забезпечується комплексом засобів і заходів: підвищенням надійності функціонування, живучості та ремонтопридатності; резервування на рівні елементів, блоків, систем, каналів, системи технічного обслуговування та технічної експлуатації.

Цілісність інформації, що передається мережею, забезпечується завадостійким кодуванням або системою зі зворотним зв'язком. Застосовуються системи з повторенням передавання даних, системи із інформаційним зворотним зв'язком, де рішення про повторне передавання блоку даних приймається джерелом на підставі порівняння переданих та прийнятих даних, системи з вирішуючим зворотним зв'язком, де рішення про повторення блоку даних приймається на прийомній стороні за допомогою коду з виявленням помилок.

Впливи техногенних джерел загроз здебільшого обмежуються місцем їхнього виникнення. Інший характер має вплив загроз антропогенного типу. Місця несанкціонованого доступу розподілені по системі. Людський фактор є найвразливішою ланкою у ланцюжку будь-якої безпеки. Місце несанкціонованого доступу до системи може не співпадати з місцем впливу. Порушник може діяти застосовуючи віддалений доступ. Можливість збереження анонімності збільшує небезпеку антропогенних загроз. Телекомунікаційна мережа є джерелом загроз системам, що її використовують. Зниження ризику загроз з боку кожної з ланок – це важлива вимога до телекомунікацій. Необхідні заходи боротьби не лише з наслідками реалізації загроз у місці впливу, але й у місці несанкціонованого доступу чи дії джерела загроз.

III Класифікація систем захисту по способу побудови та об'єктам розподілу

З точки зору проблем розподілу функцій можна виділити три типи концепцій побудови захисту: "бар'єрного" захисту (захисту периметра) [9], "лінійного" захисту і "розподіленого" захисту. У лінійних і розподілених системах захисту частина задач захисту може вирішуватись методом "компенсації".

Вузли зв'язку, прикінцеві системи зосереджені на порівняно невеликій території і мають систему захисту, побудовану за принципом „кругової оборони" чи захисту периметра. Всі об'єкти, які захищаються, розташовані у захищеному фізичному середовищі на території, яка охороняється. З теоретичних положень технічного захисту інформації відомо, що найслабіша ланка, яка не блокована організаційними і/або організаційно-технічними чи криптографічними засобами, визначає результуючий рівень захищеності.

Систему "лінійного" захисту можна було б розглядати як крайній випадок сильно витянутої "бар'рної" системи захисту. Але "лінійний" захист має суттєву відмінність від "бар'єрного". Системи передавання, канали, магістральні лінії характеризуються своєю протяжністю і проходять незахищеним середовищем. Системи захисту в них або розташовуються вздовж лінії, або побудовані за принципом „компенсації". У останньому випадку засоби захисту сконцентровані на прикінцевих (або транзитних) пунктах і забезпечують, так би мовити „компенсацію" загроз у незахищених ланках тракту передавання інформації. Так, система передавання зі зворотним зв'язком має на прикінцевому пункті засоби прийняття рішення про втрату цілісності інформації та формування запиту на повторне передавання помилкового блоку. Не всі послуги безпеки можна здійснювати методом "компенсації". Приміром, порушення доступності при DoS-атаках не може бути компенсоване у прикінцевому обладнанні, якщо нема обхідних шляхів для встановлення з'єднання. Найчастіше захист за "компенсаційним" принципом використовується при забезпеченні конфіденційності. Але при цьому доводиться розподіляти задачі невідмовності джерела повідомлення, невідмовності споживача повідомлення, невідмовності мережі, що приймає повідомлення від джерела для доставки адресатові. Такі ж міркування стосуються і розподілу задач автентифікації суб'єктів інформаційної взаємодії у мережі в процесі передавання інформації та між мережами різних операторів.

Концепція "розподілених" систем захисту має застосовуватись в IP-мережах. Поняття каналу передавання в таких мережах розмите. Тракт передавання може не закріплюватись за одним повідомленням. Повідомлення поділяється на пакети, кожен з яких може передаватись довільним маршрутом. Віртуальні канали створюються не для всіх повідомлень. Рівень захищеності такої мережі буде визначатись захищеністю найбільш слабкого маршруту з усіх можливих маршрутів. А захищеність маршруту визначається його найслабшою ланкою.

З точки зору забезпечення безпеки інформації, комплекс засобів захисту можна розглядати як набір функціональних послуг, що в сукупності створюють необхідний функціональний профіль захисту. Кожна послуга являє собою набір функцій, які дозволяють протистояти певній множині загроз. Політику безпеки може бути здійснено з використанням різних механізмів, окремо чи в комбінації, залежно від об'єктів

політики. Загалом механізми належатимуть до одного з трьох класів, які можуть перетинатись: запобігання, реєстрування, відновлення. Аби забезпечувати послуги, використовують механізми безпеки.

Згідно з міжнародними рекомендаціями [10, 11] служби безпеки в мережі будуються за ієрархічним багаторівневим модульним принципом: служба безпеки – сервіси безпеки – функціональні послуги безпеки – механізми безпеки. Один чи комбінація з декількох механізмів захисту утворюють послугу захисту. *Сервіс* – це використання механізмів захисту, які утворюють послугу.

Розглянемо варіанти постановки задачі розподілу послуг та механізмів захисту залежно від простору (середовища) розподілу. Можливі варіанти розподілу:

1) між рівнями архітектури взаємодії відкритих систем;

2) між компонентами, на які декомпозується інформаційно-телекомунікаційна система; тут можливі різні підваріанти:

- між вузлами, каналами, локальними мережами, системами обробки інформації, системами управління базами даних тощо;
- між прикінцевим обладнанням, елементами мережі доступу, цифровими комутаційними системами та транспортною мережею;
- між прикінцевими пунктами і мережею (системою) передавання;

3) між рівнями стеку мережних протоколів;

4) між процесами обробки інформації.

Розподіл засобів і систем захисту по стадіям життєвого циклу та інші такого роду способи розподілу тут не розглядаються. Існуюча нормативно-правова база чітко визначає розподіл заходів захисту у рамках комплексного підходу. Комплексний підхід реалізується через конкретні заходи на законодавчому, адміністративному, процедурному, програмно-технічному, фізичному рівнях. На законодавчому рівні напрацьовані закони, нормативні акти, інструкції та розпорядження щодо правових основ використання, збереження, організації доступу до інформаційних ресурсів та телекомунікаційних послуг. На адміністративному рівні визначаються вимоги політики безпеки, адміністративні інструкції, політика роботи з персоналом та споживачами. На процедурному рівні визначаються способи реалізації політики безпеки, організаційні заходи і процедури захисту, контроль за роботою персоналу. На програмно-технічному рівні реалізуються технічні рішення щодо захисту конкретних інформаційних ресурсів, засобів захисту й контролю.

IV Вирішення деяких задач розподілу послуг і механізмів захисту

1. Найбільш детально вирішена задача розподілу послуг та механізмів безпеки у еталонній моделі архітектури Взаємодії Відкритих Систем (ВВС). У моделі ВВС виокремлюються сім рівнів опрацювання інформації: 1 – фізичний; 2 – канальний; 3 – мережний; 4 – транспортний; 5 – сеансовий; 6 – представний; 7 – прикладний. Кожен рівень виконує певні завдання та функції й забезпечує умови функціонування суміжних рівнів. Архітектура безпеки також будується на принципах ієрархічної рівневої безпеки, тобто безпека забезпечується на кожному з рівнів моделі ВВС і функціональні послуги безпеки розподілено за цими рівнями і етапами зв'язку.

Досягнення високих рівнів безпеки неможливе без загальних механізмів безпеки, які застосовуються у будь-яких системах безпеки. Їхній вибір залежить від рівня потенційних загроз й цінності інформації, яка захищається. Окрім того, має застосовуватись низка механізмів, які повинні бути забезпечені поза межами відкритої системи: довірче функціонування та фізична безпека, грифи таємності, виявлення подій, що порушують безпеку, журнал реєстрування з безпеки, відновлювання нормального функціонування служби безпеки після порушення.

Довіра до методів зазвичай установлюється за межами середовища ВВС. Процедури, використовувані для забезпечування довіри, можуть бути розміщені в апаратних засобах та програмному забезпеченні. Ці процедури, в основному, дорогі й важко здійснювані. Проблеми можуть бути мінімізовані при виборі архітектури, яка дозволяє здійснювати функції безпеки в окремими модулях, котрі може бути забезпечено функціями, не пов'язаними з безпекою. Фізичні заходи захисту та захист від персоналу будуть завжди потрібні для гарантування повної безпеки. Всі системи в решті решт покладаються на певну форму фізичного захисту й на довіру персоналу, котрий використовує системи. Чинні процедури мають бути визначено відповідними операціями й доведено до відповідального персоналу.

2. Розглянемо розподіл окремих послуг безпеки між елементами архітектури, на які декомпозуються інформаційно-телекомунікаційні системи.

Конфіденційність забезпечує недоступність семантичної складової інформації для несанкціонованого доступу. Механізми забезпечення конфіденційності можна концентрувати на прикінцевих пунктах та/або вузлах чи розподіляти за складовими системи передавання. Довгий час інформаційній безпеці

телекомунікаційних мереж приділялось недостатньо уваги. Компенсаційний метод захисту був єдиною концепцією створення захищених каналів зв'язку. Це стало закріплюватись і у нормативній базі. Так в [12] встановлено, що конфіденційність інформації, яка є державними інформаційними ресурсами, під час передавання мережею передачі даних забезпечує власник автоматизованої системи (АС) або оператор, але за договором з власником АС.

При застосуванні шифрування адреса має бути виокремлена явно в пункті передавання й пункті доступу. За цією прикметою розрізнюють міжканальне шифрування й міжкінцеве (неперервне) шифрування. За міжканального шифрування дані зашифровуються в кожнім каналі й дешифруються (і тому є уразливі) у транзитних пунктах передавання чи пункті доступу. За міжкінцевого шифрування лише адреса (чи подібні керувальні дані) є наявні в чистому вигляді в пункті передавання чи пункті доступу. Текст залишається зашифрованим. Міжкінцеве шифрування є більш бажане, але має більш складне архітектурне виконання, особливо якщо включено розподіл електронних ключів (функцію керування ключами). Міжканальне й міжкінцеве шифрування можуть бути об'єднані.

Засоби захисту деяких властивостей безпеки принципово необхідно розподіляти по системі. Порушення доступності внаслідок, приміром, перенавантаження мережі при DoS-атаках неможливо компенсувати в прикінцевих пунктах. Послуги забезпечення доступності мають розподілятись по мережі рівномірно. Недостатність апаратних та програмних засобів мережі має бути усунена, а критичні за пропускною спроможністю ланки мережі мають бути доповнені необхідними додатковими ресурсами. Аналогічно рівномірно мають розподілятись засоби забезпечення спостереженості. Постійний аудит мереж зв'язку з метою виявлення їхньої вразливості та можливих загроз забезпечує виявлення слабкої ланки. А рівень захищеності слабкої ланки визначає, врешті решт, рівень інформаційної безпеки в цілому.

3. Телекомунікаційні мережі розвиваються в бік універсальності, мультисервісності. При цьому кількість і якість телекомунікаційних послуг невпинно зростає. Є деякі особливості в задачі розподілу систем захисту у мережах наступного покоління (NGN), в яких на мережному рівні передбачається застосування IP-орієнтованих протоколів. В NGN виділяють шари (площини): шар абонентського доступу, що базується на трьох середовищах передавання – металевому кабелі, оптоволокні і радіоканалах; шар комутації, – комутації каналів чи комутації пакетів; шар транспортного рівня з програмним управлінням, побудований на Softswitch – програмних комутаторах за технологією IP; шар інтелектуальних послуг та різноманітного сервісу; шар експлуатаційного управління. Створення в NGN фактичного єдиного централізованого експлуатаційного управління мережею гостро ставить проблеми інформаційної безпеки. NGN – це мережа, яка підтримує механізми якості обслуговування (QoS) та інформаційної безпеки. Відповідні елементи встановлюються, в основному, в шарі управління, а контрольовані параметри визначаються у транспортній мережі [13]. Слабким місцем поки що є низька захищеність протоколів сигналізації мереж IP. Стандарти безпеки сигнальної мережі, побудованої на основі IP-технологій, знаходяться у стадії розробки.

На кожному рівні і різних рівнях можуть взаємодіяти різні оператори. Над послугами оператора інфраструктури може знаходитись шар послуг сервіс-провайдера. Розподіл послуг та механізмів безпеки має забезпечити безпеку при будь-якій взаємодії суб'єктів відносин у мережі. Маємо задачу розподілу послуг безпеки між рівнями стеку мережних протоколів.

V Задача оптимізації загальних витрат на інформаційну безпеку

Задачу оптимізації витрат доцільно вирішувати як частину більш значимої задачі оптимізації побудови системи безпеки інформаційно-телекомунікаційної системи та оцінки її ефективності. Задача оптимізації побудови системи безпеки є процедурою вибору рішень і проектування заходів виконання політики безпеки інформаційно-телекомунікаційної системи, які забезпечують прийнятний рівень інформаційної безпеки при допустимому рівні витрат. Кожна послуга безпеки та механізми безпеки, які послугу реалізують, можуть включати декілька рівнів. Чим вище є рівень послуги, тим повніше забезпечується захист від певного виду загроз.

Для кожної долученої послуги має бути визначено рівень послуги, який передбачається реалізовувати. Має бути описано політику даної послуги: зазначення об'єктів, до яких застосовується дана послуга, і правил, відповідно до яких мають функціонувати механізми, що реалізовують послугу.

При постановці задачі оптимізації слід врахувати такі фактори: інтегральної оцінки рівня захищеності на сьогодні ще не сформовано, але можливо визначити рівні, що забезпечуються кожною конкретною послугою або механізмом безпеки; не всі показники рівня захищеності мають кількісні оцінки, показники, які залежать від антропогенних впливів, здебільшого мають якісні оцінки у порядкових шкалах, здобутих методом експертного опитування; показники захищеності являють собою систему взаємозв'язаних і взаємозалежних компонентів; до номенклатури показників окрім показників захищеності доцільно залучити показники якості інформаційно-телекомунікаційної системи (такі, як надійність, завадостійкість, показники доставки

повідомлень тощо); економічна частина цільових функцій має задаватись, виходячи з принципу розумної достатності, що витрати на інформаційну безпеку $B_{ІБ}$ мають бути менші за можливі збитки $B_З$ за реалізації загроз: $B_{ІБ} < B_З$.

Враховуючи сказане, задачу можна звести до задачі багатокритеріального вибору, яка давно і успішно вирішується для окремих видів виробів при оцінці якості промислової продукції [14]. Порядок розв'язку задачі такий: вибір показників захищеності та якості системи, розробка методик оцінки показників захищеності і якості системи; оцінка показників захищеності і побудова матриці показників для різних варіантів розподілу послуг по системі; вибір оптимального варіанту на основі розв'язання задачі оптимізації одним із методів, приміром методом векторної оптимізації [15].

Економічні показники мають враховувати загальні витрати, включаючи вартість придбання, монтажу (інсталяції) і технічної експлуатації засобу захисту. У варіанті розподілу послуг безпеки між прикладним рівнем і іншими рівнями загальні витрати на інформаційну безпеку можуть бути обчислені за виразом

$$B_{ІБ1} = \sum_{m=1}^{M} B_m(l_m) + \sum_{i=1}^{I}\sum_{m=1}^{M} B_{im}(l_{im}), \qquad (1)$$

де m – індекс механізму безпеки, m=1...M, M – кількість механізмів безпеки; $B_m(l_m)$ – величина витрат на реалізацію m-го механізму безпеки з показником захищеності $l_{m;}$ i – індекс рівня моделі ВВС, i=1...I, I – кількість рівнів за винятком прикладного рівня; $B_{im}(l_{im})$ – величина витрат на реалізацію m-го механізму безпеки на рівні i з показником захищеності l_{im}.

У варіанті розподілу послуг безпеки між прикінцевими пунктами і вузлами мережі загальні витрати на інформаційну безпеку $B_{ІБ}$ можуть бути обчислені за виразом

$$B_{ІБ2} = N\sum_{m=1}^{M} B_m(l_m) + V\sum_{j=1}^{J}\sum_{m=1}^{M} B_{jm}(l_{jm}), \qquad (2)$$

де N – кількість прикінцевих пунктів, V – кількість вузлів мережі, j – індекс блоку вузла мережі, j=1...J, J – кількість блоків на вузлі.

Припустимо, що при переносі засобів захисту з прикінцевого пункту у вузли мережі загальна захищеність не змінюється і не утворюються нові канали несанкціонованого доступу. Тоді з (2) випливає, що загальні витрати можуть зменшитись, бо $V<N$. Але питання залежності захищеності від перерозподілу засобів захисту у мережі вимагає подальшого дослідження.

VI Висновки

Детально розглянуто розподіл послуг безпеки за рівнями моделі архітектури взаємодії відкритих систем.

При формуванні функціонального профілю захищеності інформаційно-телекомунікаційних систем можна виділити групи функціональних послуг безпеки: загальні послуги, які мають бути реалізовані поза інформаційно-телекомунікаційною системою; послуги, які повинні бути розподілені, скоріш рівномірно, по інфраструктурі інформаційно-телекомунікаційної системи; послуги "компенсаційного" типу (такі як конфіденційність і цілісність), для яких дійсна постановка проблеми оптимального розподілу функцій між прикінцевими пунктами та інфраструктурою системи.

Проблема розподілу функцій та механізмів безпеки в інформаційно-телекомунікаційних системах вимагає подальших досліджень у частині формування номенклатури оптимальних показників характеристик системи як початкових даних для аналізу, розробки практичних методик оцінки показників, визначення залежності витрат на систему безпеки від рівня захищеності тощо, а також удосконалення практичних методик оцінки втрат від реалізації загроз інформаційній безпеці.

*Література: **1**. Александров А. М., Кравец Л. З., Петренко С. А., Эркин А. Г. Построение наложенных систем криптографической защиты // "Электросвязь", – М:, № 5, 2003. – С. 41-42. **2.** Мильковский А. Г. Обеспечение безопасности связи в телефонных сетях общего пользования // "Бизнес и безопасность", – К:, № 1, 2000. – С. 12-13. **3.** Кузьмин А. С., Бочков С. И., Ивин Ю. Э. Методы обеспечения информационной безопасности в АТМ-сетях. // "Электросвязь", – М:, № 9, 2001. – С. 28-32. **4.** ETSI TR 101 664: Intelligent Network (IN); IN interconnect security features, 1999. **5**. ETSI ETR 083: Universal Personal Telecommunication (UPT); General UPT security architecture, 1993. **6.** Бондаренко М., Скрыпник Л, Потий А. Перспективы применения международного стандарта ISO/IEC в Украине. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 3, 2001. С 7-26. **7.** Петренко С. Методические основы защиты информационных активов компании // – www.infosecurity.ru/-gazeta/content/031104/article03.-html. **8.** ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою. **9.** Гончарок М. Х., Островский В. В. Выбор параметров системы защиты информации в цифровых АТС с*

функциями ISDN. // "Вестник связи", № 4, 2000, – С. 99-105. ***10.*** *Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991;* ***11.*** *Протоколи информационно-вычислительных сетей: Справочник / С. А .Аничкин, С. А. Белов, А. В. Бернштейн и др. Под ред. И. А. Мизина, А. П. Кулешова. − М.: Радио и связь, 1990. 504 с.* ***12.*** *"Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах", затверджений наказом ДСТСЗІ СБУ № 76 від 24. 12.2001 р.* ***13.*** *Гладкова И. Г. Живой разговор о NGN // "Вестник связи", № 12, 2003. – С. 37-55.* ***14.*** *Панин О. А., Журин С. И. Оптимизация параметров систем охранной сигнализации как задача многокритериального выбора. // Защита информации. Конфидент № 1, 2004. – С. 84-87.* ***15.*** *Черноруцкий И. Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248.*

УДК 621.372.632

СИНТЕЗАТОРЫ ЧАСТОТЫ НОВОГО ТИПА

Виталий Козлов*, Анатолий Ситник, Борис Петруня, Владимир Мартыненко*, Михаил Прокофьев

*НИЦ «ТЕЗИС» НТУУ «КПИ», *НПП "ФОТОН"*

Анотація: **Излагается новая концепция частотного синтеза, позволяющая на порядок и более повысить быстродействие и спектральную чистоту сигнала. Приводятся экспериментальные результаты.**

Summary: **The article presents a new conception of frequency synthesis which allows to increase the agility and spectral purity by an order of magnitude and more. There are adduced the experimental results.**

Ключові слова: **Синтезатор частоты, быстродействие, спектральная чистота.**

I Введение

Наиболее важными характеристиками синтезатора частоты являются быстродействие и спектральная чистота сигнала. Достижение высокого уровня этих характеристик позволит создать измерительную и телекоммуникационную аппаратуру высокого качества с надёжной защитой передаваемой информации от несанкционированного доступа благодаря возможности кодирования информации с помощью быстродействующих приёмов частотной и фазовой модуляций.

Как известно, существующие прямые цифровые синтезаторы частоты (Direct Digital Synthesizers – DDS), обладая высоким быстродействием, не обеспечивают спектральной чистоты сигнала, достаточной для многих телекоммуникационных и измерительных систем. Лучшие образцы, такие, например, как AD9852, AD9858 фирмы Analog Devices, имеют гарантированный уровень дискретных помех не лучше, чем минус 52 дБ на верхней частоте диапазона, которая не превышает 400 МГц для AD9858. Чтобы достичь частоты сигнала, например 1000 МГц, используют дополнительные устройства умножения частоты, в результате чего уровень помех поднимается до – 44 дБ. Кроме того, следует отметить недокументированные характеристики синтезаторов DDS, которые проявляются при работе в широком диапазоне частот и различных соотношениях выходной и опорной частоты. В НИЦ «Тезис» НТУУ «КПИ» и ОАО «Институт радиоизмерительной аппаратуры» были проведены исследования спектральных характеристик DDS AD9852 в составе разрабатываемого генератора сигналов в диапазоне частот от 0,1 до 1200 МГц, которые показали наличие помех дробности значительно более высокого уровня, чем это приведено в описании микросхемы. Чтобы добиться результатов по минимизации нежелательных побочных спектральных составляющих до уровня – 50 дБ пришлось использовать в схеме синтезатора переключение частоты опорного генератора (8 значений) в зависимости от значения устанавливаемой частоты синтезатора, что значительно усложнило схему и уменьшило быстродействие генератора сигналов.

Синтезаторы с дробным коэффициентом деления (Fractional-N Synthesizers – FNS), производимые фирмами Analog Devices, Skyworks Incorporated, Philips, National Semiconductor и другими, характеризуются малым потреблением энергии (около 50 mW и менее) и малой стоимостью (не более $10), но имеют низкую спектральную чистоту сигнала, которая не превосходит аналогичные параметры в AD9858, и малое быстродействие (полоса пропускания ФАПЧ не более нескольких десятков кГц).

Поэтому, чтобы одновременно обеспечить высокие показатели быстродействия и спектральной чистоты, прибегают к многопетлевым структурам - громоздким, дорогим и неэкономичным по потреблению энергии.

Излагаемая ниже новая, патентованная концепция частотного синтеза [1, 2], будучи воплощённой в однокристальную интегральную микросхему, соединит в себе преимущества имеющихся в данное время на рынке лучших образцов подобного назначения, а именно: быстродействие синтезаторов прямого типа (DDS),