*for Cryptology. http://www.ecrypt.eu.org.* ***8.*** *AES discussion forum: http://aes.nist.gov.* ***9.*** *Preneel B., Biryukov. A, Oswald E. and others. NESSIE security report. Public Report, Deliverable D 20. 2002. Version 1.0: http://cryptonessie.org.* ***10.*** *Надежность и эффективность в технике: Справочник: Н17 В 10 т./ Ред. совет: В.С. Авдуевский (пред.) и др. –М.: Машиностроение, 1988. – (В пер.). Т - 3, Эффективность технических систем / Под общ. В.Ф. Уткина, Ю.В.Крючкова.–328 с.* ***11.*** *Потий А .В., Избенко Ю. А. Множество показателей оценки эффективности функционирования схем поточного шифрования // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2003. – № 133.* ***12.*** *Потий А. В., Избенко Ю. А. Исследование методов криптоанализа поточных шифров // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - НТУ "КПІ", ДСТСЗІ СБУ. - 2003. - № 6. - С. 34 – 49.* ***13.*** *M. Mihaljevic, J. Golić. A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence. // In Advances in Cryptology – AUSCRYPT'90, vol.453, Lecture Notes in Computer Science, Springer-Verlag, pp.165 – 175,1990.* ***14.*** *W. Maier, O. Staffelbach. Fast correlation attacks on stream ciphers. // In Advances in Cryptology – EUROCRYPT'88, vol.330, Lecture Notes in Computer Science, Springer-Verlag, pp.301 – 314, 1988.* ***15.*** *T. Siegenthaller, Decrypting a class of stream cipher using ciphertext only // IEEE Trans. Comput.,vol. C-34, pp.81 – 85, Jan. 1985.* ***16.*** *Фомичев В. М., Дискретная математика и криптология: Курс лекций / Под ред. Н.Д. Подуфалова. – М.: ДИАЛОГ-МИФИ, 2003. 400 с.* ***17.*** *J. Dj. Golić, A. Clark, and E. Dawson. Inversion attacks and branching. // Information Security and Privacy, Fourth Australasian Conference, ACISP'99, Lecture Notes in Computer Science, vol. 1587, J. Pieprzyk, R. Savavi-Naini, J. Seberry eds., Springer-Verlag, pp. 88 – 102, 1999.* ***18.*** *J. Golić, On the security of nonlinear filter generators. In Fast Software Encryption – Third International Workshop, Cambridge, February 1996, Lecture Notes in Computer Science, vol. 1039, pp. 173 – 188, Springer-Verlag, Berlin, 1996.* ***19.*** *Courtois N. Meier W. Algebraic attacks on stream ciphers with linear feedback, Eurocrypt 2003, Warsaw, Poland, Lecture Notes in Computer Science, vol. 2656, Springer, 2003, pp. 345 – 359.* ***20.*** *J. Seberry, X.-M. Zhang and Y. Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995.* ***21.*** *B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functions," in Lecture Notes in Computer Science 473; Advances in Cryplology: Proc. Eurocrypt'90, 1. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 161-173. Berlin: Springer-Verlag.* ***22.*** *R. A. Rueppel. Linear complexity and random sequences. Advances in Cryptilogy–EUROCRYPT'85 (LNCS 219), 167 – 188, 1986.* ***23.*** *Massey J. L., Shift-Register Synthesis and BCH Decoding // IEEE Transactions on Information Theory, January 1969. Vol. IT-15, no. 1.* ***24.*** *Потий А., Орлова С., Гриненко Т., Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вып. 2. С.206-214.* ***25.*** *Babbage S. A space/time tradeoff in exhaustive search attacks on stream ciphers. In European Convention on Security and Detection, volume 408 of IEE Conference Publication, May 1995.* ***26.*** *Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. М.: Наука, 1977. 248 с.*

**УДК 681.321;322:621.395**

# АЛГОРИТМ РОЗПОДІЛУ РЕСУРСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДОКУМЕНТАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ

***Володимир Кононович, Тетяна Тардаскіна****

*Академія зв'язку України, Одеський регіональний центр ТЗІ ВАТ "Укртелеком",*
**Одеська національна академія зв'язку*

*Анотація:* **Аналізується задача оптимізації витрат на інформаційну безпеку системи документальних телекомунікацій, яка зводиться до задачі багатокритеріального вибору. Пропонується інтерактивна процедура раціонального вибору варіанту розподілу витрат.**

*Summary:* **The expenses optimization task of information security of the documental telecommunication systems is analyzed. Whole thing comes to multi criteria choice task. The interactive procedure of rational choice of the expenses distribution variant is offered.**

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

## І Вступ

Забезпечення інформаційної безпеки документальних телекомунікацій має на меті створення перешкод

для будь-якого несанкціонованого втручання у процес функціонування мереж, від спроб викрадення, модифікації, виведення з ладу або знищення компонентів мережі, а також забезпечувати захист від викрадення, знищення, перекручення, блокування інформації, несанкціонованого витоку інформації або від порушення встановленого порядку її маршрутизації [1]. Для документальних телекомунікацій важливою стає задача побудови "довіреного" телекомунікаційного середовища. Задача розподілу ресурсів систем захисту у різних постановках вирішується у багатьох роботах [2 – 7]. Така задача є частиною більш широкої задачі оптимізації побудови системи інформаційної безпеки та оцінки її ефективності. Вона вирішувалась у багатьох суміжних областях безпеки, управління та прийняття рішень [6, 8, 9]. Але відносно телекомунікаційних систем і, зокрема документальних телекомунікацій, така задача не вирішена. **Метою даної роботи** є аналіз варіантів розподілу витрат на інформаційну безпеку системи документальних телекомунікацій і розробка методики вирішення задачі раціонального вибору варіанту розподілу витрат. **Постановка задачі.** Задача раціонального вибору варіантів 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. Система інформаційної безпеки може бути описана множиною показників захищеності та якості і задача її оптимізації зводиться до задачі багатокритеріального вибору згідно з деякою системою критеріїв. У загальному випадку процедура раціонального вибору варіанта побудови складається з послідовності: розробка стратегії (політики) інформаційної безпеки, яка визначає мету задачі і засоби системи захисту; вибору номенклатури показників захищеності і якості системи інформаційної безпеки; попередній відбір варіантів побудови системи інформаційної безпеки; оцінка показників захищеності і якості та побудова матриці показників для різних варіантів побудови системи; вибір оптимального варіанту на основі розв'язання задачі багатокритеріального вибору. При цьому необхідно уточнити метод та процедуру раціонального вибору варіантів, вирішні правила та множину критеріїв оптимізації. Аналогічні задачі оптимального розподілу функцій по елементам мережі вирішувались при забезпечуванні достовірності передавання даних і надійності функціонування телекомунікаційних систем. З практичної точки важливо, що в рамках системи технічної експлуатації телекомунікаційних мереж вироблено розвинуті засоби підтримки заданого рівня цих показників якості передавання інформації і такі показники споріднені показникам інформаційної безпеки.

## II Стратегія інформаційної безпеки документальних телекомунікацій

Під стратегію безпеки будемо розуміти з'ясування таких питань [10]: які загрози безпеці мають бути усунені і в якій мірі; які мережні ресурси (об'єкти) мають бути захищені і в якій мірі; за допомогою яких засобів має бути реалізована безпека; які мають бути обмеження по вартості забезпечення безпеки із врахуванням витрат на реалізацію й експлуатацію, а також можливих потенційних втрат внаслідок реалізації загроз. Загальні напрями забезпечення інформаційної безпеки задані Законом України "Про телекомунікації". *Необхідно захищати й узгоджувати* методи забезпечення інформаційної безпеки для усіх складових мережі, включаючи інформаційні ресурси: лінії, канали, обладнання, програмне забезпечення, інформацію, телекомунікаційні протоколи та персонал. Захисту підлягають: персональні дані, дані сигналізації (таблиці маршрутизації тощо), вміст бази даних тощо [11, 12].

Інформаційна безпека телекомунікаційних мереж має забезпечуватись в умовах інтеграції інформаційних та телекомунікаційних технологій, різних типів мереж та телекомунікаційних послуг, кількість і якість яких невпинно зростає, а також дії на мережах операторів різної форми власності. Адекватний рівень інформаційної безпеки може бути забезпечений лише на основі комплексного підходу, що передбачає планомірне використання фізичних, програмно-технічних і організаційних заходів та засобів. Захисту підлягають усі складові частини документальної інформаційно-телекомунікаційної системи: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Необхідно узгоджувати методи забезпечення інформаційної безпеки для різних компонентів інформаційно-телекомунікаційних систем та телекомунікаційних мереж, включаючи інформаційні ресурси, застосування, телекомунікаційні протоколи. Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення інформаційної безпеки, оскільки вразливість будь-якої ланки мережі може створити проблеми для усіх її учасників, як провайдерів та операторів, так і споживачів послуг. Кінцевою метою є вибір ефективних засобів протидії загрозам при реалізації системи інформаційної безпеки, які, в усякому разі, не перевищують вартість втрат, очікуваних від реалізації загроз.

За ознаками чинники *загрозі інформаційній безпеці* можна класифікувати як техногенні і антропогенні. Джерела загроз можуть діяти як всередині систем так і ззовні. Методи протидії внутрішнім і зовнішнім загрозам можуть бути різними. Зовнішня безпека передбачає захист телекомунікацій від стихійного лиха (пожежі, повені, землетрусу тощо) та від проникнення до телекомунікаційної мережі й вузлів з метою викрадення, одержання доступу до каналів та носіїв інформації, або виведення мережі з ладу. Внутрішня

безпека має гарантувати надійну та коректну роботу телекомунікаційної мережі та вузлів, цілісність програмного забезпечення, інформації та технологічних даних.

Техногенні чинники порівняно добре вивчені, місця їхньої дії локалізовані і вони враховуються при організації технічної експлуатації у вигляді комплексу заходів протидії завадам передаванню сигналів, збоям та відмовам обладнання. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми (мережі зв'язку, високовольтні лінії електропередачі, мережі інженерних комунікацій (електро- і водопостачання), стихійні лиха тощо) і внутрішніми (неякісні технічні засоби передачі і обробки інформації, неякісні програмні засоби комутації та обробки інформації, допоміжні засоби (охорони, сигналізації, службового зв'язку, інші технічні засоби, що застосовані в інформаційно-телекомунікаційних системах). У питаннях протидії техногенним чинникам накопичено значний досвід, і особливо у вирішенні проблеми розподілу засобів забезпечення достовірності передачі інформації, надійності функціонування систем та цілісності інформаційної сфери телекомунікаційних систем. Подібні проблеми вирішувались у минулому при створенні телеграфних мереж та мереж передавання даних. Телеграфний канал (рис. 1), який зв'язував телеграфні апарати (ТА), забезпечував ймовірність помилки в діапазоні $p_П = 10^{-3} \ldots 10^{-4,}$ , тобто допускалась одна помилка на тисячу переданих знаків. Передавання сигналів здійснювалось в умовах дії завад $h_к(t)$ і потоку збоїв та відмов $r_к(t)$. На прикінцеві апарати також діяв потік збоїв та відмов $r_а(t)$. Сигнал на виході каналу виражався функціоналом

$$S_{вих}(t) = F(S_{вх}(t), h_к(t), r_к(t)), \quad (1)$$

де $S_{вх}(t)$ – сигнал на вході каналу, а функціонал виражає як адитивну так і мультиплікативну залежність.

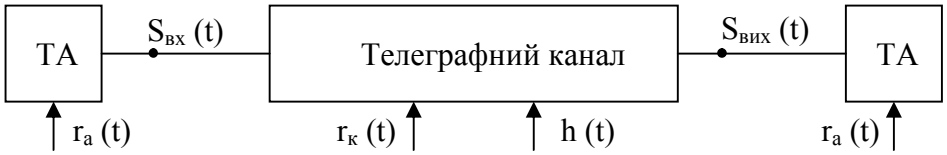


**Рисунок 1 – Техногенні впливи на телеграфні канали**

Необхідність віддаленого зв'язку з електронними обчислювальними машинами підвищили вимоги до якості і достовірності передавання даних. Для досягнення ймовірності помилки $p_П = 10^{-6} \ldots 10^{-9}$ можна розподіляти витрати на підвищення достовірності двома способами: підвищенням якості тракту передавання при застосуванні простих прикінцевих пристроїв, або використанням прикінцевих пристроїв зі складними засобами підвищення достовірності. Чим ймовірність помилки в каналі менше, тим менш жорсткі вимоги до підсистеми підвищенні достовірності в прикінцевих пристроях. Технічним рішенням стало застосування апаратури передавання даних (АПД) мережею загального користування (МЗК) (рис. 2), які використовували стандартні канали тональної частоти (СКТЧ). Замість телеграфних апаратів використовувались комплекси прикінцевого обладнання (ПО). Основу АПД складали блок перетворення сигналів (БПС) до виду, придатного для передавання мережею, і блок захисту від помилок (БЗП). Приміром, для низько швидкісної передачі даних (до 600 Бод) необхідно було досягти норми ймовірності помилки $p_П = 3 * 10^{-6}$. Розподіл помилок був такий: одна помилка на мільйон переданих знаків у СКТЧ, одна – у АПД (вторинного канало створення) і одна – у прикінцевому пристрої. Канали первинної мережі були дорогі і заходи підвищення достовірності в аналогових каналах були складними. Коли треба було досягти вірогідності помилки $p_П = 10^{-9}$, то у прикінцевих пристроях застосовувались потужні циклічні коди з виправленням помилок і системи зі зворотним зв'язком. Підтримання певного рівня достовірності в каналах досягалось, в основному, за допомогою заходів і засобів системи технічної експлуатації.

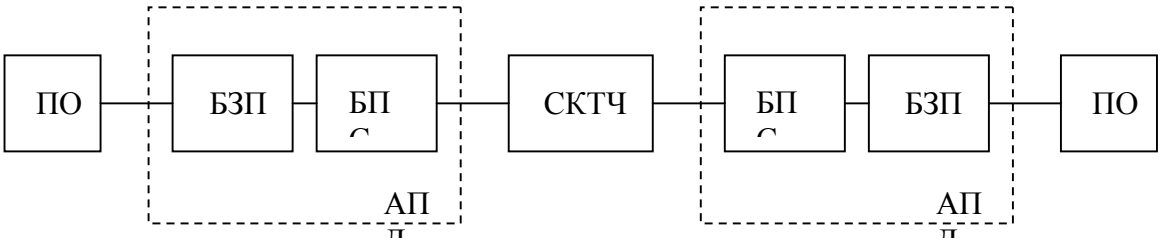


**Рисунок 2 – Канали передавання даних**

У сучасних цифрових системах передавання ймовірність помилки досягла рівня $p_П = 10^{-8} \ldots 10^{-9}$. Це дозволило перерозподілити витрати на підтримання достовірності. Для забезпечення достовірності передавання інформації у каналі застосовуються прості циклічні коди з виявленням помилок. У прикінцевому пристрої вимоги до блоку захисту від помилок також знизились. Виявлені помилки усуваються відповідними протокольними процедурами. Перехід до цифрових систем зв'язку значно підвищив також і надійність функціонування мереж. В аналогових мережах задача забезпечення надійності зв'язку вирішувалась, в основному, застосуванням у вузлах комутації процедури пошуку обхідних шляхів, якщо прямі канали було зайнято. У цифрових мережах канали значно надійніші і було здійснено перерозподіл задач підвищення надійності. Стали застосовуватись кільцеві резервовані оптоволоконні структури і механізми управління потоками в системах передавання цифрових потоків [13]. В IP-мережах надійність зв'язку ще більша і необхідний її рівень може підтримуватись за рахунок протокольних засобів. Характер техногенних впливів на інформаційну безпеку сучасного каналу передавання документальної інформації можна представити так, як на рис. 3, де показані: ПО – прикінцеве обладнання; ЦКС – цифрові системи комутації; $r_1(t)$, $r_2(t)$, $r_3(t)$, $r_4(t)$ – потоки збоїв та відмов обладнання відповідно у прикінцевому обладнанні, мережі доступу, ЦКС та транспортній мережі; $h_1(t)$, $h_2(t)$, - адитивні та мультиплікативні завади в трактах телекомунікацій відповідно в мережі доступу та транспортній мережі; $S_1(t)$, $S_2(t)$, - вхідні та вихідні сигнали.

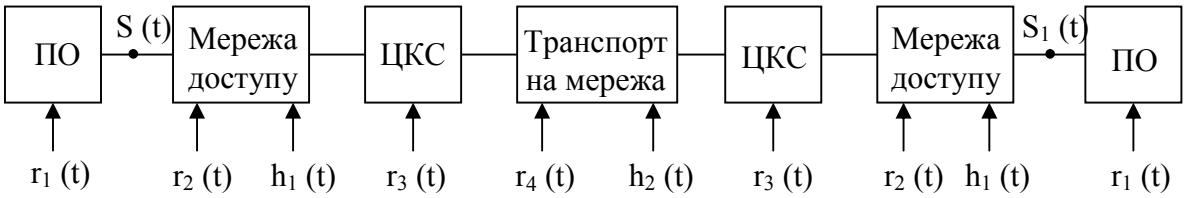


**Рисунок 3 – Характер техногенних впливів на інформаційну безпеку**

Транспортна мережа має підвищену якість та надійність порівняно з мережею доступу. Але протяжність каналів транспортної мережі збільшує вірогідність кожної з загроз як техногенного, так і антропогенного характеру.

Антропогенні чинники зумовлені діями зловмисників, помилками персоналу, користувачів, недооцінкою важливості системи інформаційної безпеки. Людський фактор є найвразливішою ланкою у ланцюжку будь-якої безпеки. Місце несанкціонованого доступу до системи може не співпадати з місцем впливу. Якщо впливи техногенних джерел загроз здебільшого обмежуються місцем їхнього виникнення, то вплив загроз антропогенного типу має інший характер. Місця можливого несанкціонованого доступу розподілені по системі, що можна ілюструвати рис. 4. Порушник може діяти застосовуючи віддалений доступ. Можливість збереження анонімності збільшує небезпеку антропогенних загроз.


**Рисунок 4 – Характер антропогенних впливів на інформаційну безпеку**

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.

Визначивши загрози, визначають задачі безпеки. 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. Аби забезпечувати послуги, використовують механізми безпеки. Згідно з міжнародними рекомендаціями [14] служби безпеки в мережі будуються за ієрархічним багаторівневим модульним принципом: служба безпеки – сервіси безпеки – функціональні послуги безпеки – механізми безпеки. Політику безпеки кожної послуги може бути здійснено з використанням різних механізмів захисту, окремо чи в комбінації, залежно від об'єктів політики. У еталонній моделі архітектури Взаємодії Відкритих

Систем (ВВС) інформаційна безпека забезпечується на кожному з рівнів моделі ВВС і функціональні послуги безпеки розподілено за рівнями ВВС (табл. 1) і етапами зв'язку.

Таблиця 1 – Розподіл послуг безпеки за рівнями моделі архітектури ВВС

| Послуги | Рівні ВВС | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7* |
| Автентифікування однорівневих об'єктів | · | · | + | + | · | · | + |
| Автентифікування джерела даних | · | · | + | + | · | · | + |
| Контроль доступу | · | · | + | + | · | · | + |
| Конфіденційність (засекречування) з'єднання | + | + | + | + | · | + | + |
| Конфіденційність (засекречування) без установлення з'єднання | · | + | + | + | · | + | + |
| Конфіденційність (засекречування) обраних полів | · | · | · | · | · | + | + |
| Конфіденційність (засекречування) трафіка (потоку даних) | + | · | + | · | · | · | + |
| Цілісність з'єднання з відновлюванням | · | · | · | + | · | · | + |
| Цілісність з'єднання без відновлювання | · | · | + | + | · | · | + |
| Цілісність обраних полів даних з'єднання | · | · | · | · | · | · | + |
| Цілісність без установлення з'єднання | · | · | + | + | · | · | + |
| Цілісність обраних полів без установлення з'єднання | · | · | · | · | · | · | + |
| Захист від відмовлення партнерів зі зв'язку від факту прийняття-передавання повідомлення з доказом щодо джерела | · | · | · | · | · | · | + |
| Захист від відмовлення партнерів зі зв'язку від факту прийняття-передавання повідомлення з доказом щодо доставляння | · | · | · | · | · | · | + |

В таблиці введені позначки:
цифри – є номерами рівнів від 1-го – фізичного до 7-го – прикладного рівня;
+ - сервіси має бути включено до стандартів для рівня як надавана опція;
· - сервіс не надається;
* - дані сервіси записано до 7-го рівня тому, що прикладні процеси в прикінцевих пристроях можуть самі надавати сервіси безпеки, користуючись при цьому й сервісами безпеки представного рівня. Розподіл функцій безпеки між прикладним та іншими рівнями має вирішуватись у результаті оптимізації витрат.

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 кожна з послуг безпеки та механізмів безпеки, які послугу реалізують, можуть бути декількох рівнів. Чим вище є рівень послуги, тим повніше забезпечується захист від певного виду загроз, але й тим більші витрати на реалізацію. Для кожної послуги має бути розроблено політику безпеки, яку буде здійснено інформаційно-телекомунікаційною системою.

Сервіси фізичного рівня є основоположними. Мета захисту фізичного рівня полягає в повному захисті фізичного потоку бітів даних (сервіс засекречування з'єднання) і забезпечуванні конфіденційності трафіка (сервіс засекречування потоку даних). Сервіси безпеки фізичного рівня використовуються окремо чи в комбінації. Повну конфіденційність з'єднання може бути забезпечено, наприклад, за дуплексного режиму синхронного, двохточкового передавання. За інших видів передавання, наприклад, за асинхронного, передавання може бути забезпечено за обмеженої конфіденційності з'єднання. Захист фізичного рівня забезпечується за допомогою пристрою шифрування.

Сервіси безпеки мережного рівня мають велике значення за своєю природою. Мережний рівень внутрішньо зорганізовано для забезпечення виконання протоколами таких операцій: доступ до мереж; зливання залежних підмереж; злиття незалежних підмереж; передавання і маршрутизація. Протоколи мережної служби ВВС, які виконують доступ до мереж, операції з'єднання й маршрутизації, застосовують ідентичні *механізми безпеки.* Послуги безпеки забезпечуються у такий спосіб:

- послуга автентифікації однорівневих об'єктів забезпечується обміном захищеної *автентифікації*, чи обміном захищеними паролями й *механізмами цифрового (електронного) підпису*;
- послуга автентифікації джерела даних може бути забезпечена шифруванням чи механізмами підпису;
- послуга контролю доступу забезпечується використанням механізмів *контролю доступом*;
- послуга конфіденційності з'єднання забезпечується механізмом *шифрування* та/чи контролем маршрутизації;

- послуга конфіденційності без установлення з'єднання забезпечується механізмом шифрування та/чи *керування маршрутизацією*;
- послуга конфіденційності трафіка досягається механізмом *заповнення трафіка фоновою інформацією* в сполученні з послугою конфіденційності на мережному чи канальному рівні та/чи контролем маршрутизації;
- послуга цілісності з'єднання без відновлення забезпечується використанням механізму *цілісності даних*, іноді в сполученні з механізмом шифрування;
- послуга цілісності без установлення з'єднання забезпечується використанням механізму цілісності даних, іноді в сполученні з механізмом шифрування.

Характеристики даних, які передаються між двома чи більше об'єктами, такі як цілісність, джерело, час і одержувач, можуть підтверджуватись за допомогою механізму *нотаріального засвідчення,* яке має бути забезпечено третьою довіреною стороною.

Керування доступом на мережному рівні дозволяє прикінцевій системі контролювати шифрування мережного з'єднання, а підмережам – контролювати використання ресурсів мережного рівня тощо. Механізми контролю доступом можуть використовуватися для контролю доступу до підмереж суб'єктів зв'язку і контролю доступу до прикінцевих систем. Досягнення високих рівнів безпеки неможливе без загальних механізмів безпеки, які застосовуються в будь-яких системах безпеки. Їхній вибір залежить від рівня потенційних загроз й цінності інформації, яка захищається. Окрім того, має застосовуватись низка механізмів, які мають 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 безпеки встановлюється за межами середовища ВВС. Процедури, використовувані для забезпечування довіри, можуть бути розміщені в апаратних засобах та програмному забезпеченні. Проблеми може бути мінімізовано 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. Більшість систем покладаються на певну форму фізичного захисту й на довіру персоналові, котрий використовує системи. Всі процедури мають бути визначені відповідними операціями й доведені до відповідального персоналу.

Існуючі системи захисту інформації можна віднести до заснованих на "бар'єрній" концепції (захисту периметра), "лінійній" концепції та до заснованих на концепції "розподіленого захисту" [7]. 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 мають 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. Довгий час інформаційній безпеці власне 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 [15] 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. У той же час, механізми забезпечення конфіденційності можна концентрувати на прикінцевих пунктах та/або вузлах чи розподіляти по відповідним складовим системи передавання.

## III Оцінка показників захищеності та побудова матриці показників

При вирішенні задачі раціонального вибору способу розподілу механізмів захисту слід врахувати такі фактори: інтегральної оцінки рівня захищеності на сьогодні не сформовано, але можливо визначити рівні, що забезпечується кожною конкретною послугою або механізмом безпеки; не всі показники рівня захищеності мають кількісні оцінки, показники, які залежать від антропогенних впливів, здебільшого мають якісні оцінки в 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 – витрати на інформаційну безпеку $B_{ІБ}$ мають бути менші за можливі збитки $B_З$ за реалізації загроз: $B_{ІБ} < B_З$.

Позначимо через $X_1, \ldots, X_n$ набір показників, які відображають показники призначення, захищеність інформації (конфіденційності, цілісності, доступності, спостережності), захищеності системи документальних телекомунікацій (надійності, сталості, живучості), їх якості (достовірності передавання інформації, завадостійкості, характеристик доставки інформації, якості послуг) та гарантії захищеності

(відносно всіх етапів життєвого циклу системи). Показник $X_n$ – величина витрат. Задача оцінки показників захищеності і якості є задачею їх "виміру" й відображення у деякій кількісній або якісній шкалі. Не всі характеристики можуть бути оцінені кількісно, особливо ті, які залежать від антропогенних чинників. Приміром важко оцінити кількісно надійність зв'язку чи якість керування системою безпеки. При неможливості оцінки показника кількісно його оцінюють якісно, відображаючи міру прояву даної прикмети, застосовуючи порядкові шкали і користуючись методом експертного опитування. Результатом оцінювання повинна бути матриця показників захищеності і якості системи розмірністю $n \times m$, де $n$ – кількість показників, $m$ – кількість варіантів побудови системи інформаційної безпеки. Кожному варіанту відповідає своя точка чи вектор у просторі показників $X_1, ..., X_n$, частина з яких є критеріями вибору.

Для прикладу розглянемо три варіанти техніко-економічної задачі раціонального розподілу послуг з декількома показниками захищеності і якості (табл. 2).

Таблиця 2 – Матриця показників захищеності та якості документальних телекомунікацій

| Показники захищеності і якості | Оцінки показників для варіантів розподілу послуг забезпечення безпеки і якості системи документальних телекомунікацій | | |
|---|---|---|---|
| | Варіант розподілу поміж рівнями ВВС та прикладною системою | Варіант розподілу між елементами мережі доступу, ЦКС, транспортної мережі | Варіант розміщення послуг у прикінцевих пунктах |
| Достовірності | $p_{П1}$ | $p_{П2}$ | $p_{П3}$ |
| Надійності | $Н_1$ | $Н_2$ | $Н_3$ |
| Конфіденційності | $К_1$ | $К_2$ | $К_3$ |
| Цілісності | $Ц_1$ | $Ц_2$ | $Ц_3$ |
| Доступності | $Д_1$ | $Д_2$ | $Д_3$ |
| Спостереженості | $С_1$ | $С_2$ | $С_3$ |
| Вартості | $В_{ІБ}$ | $В_{ІБ}$ | $В_{ІБ}$ |
| Гарантій захисту | *Рівень 1* | *Рівень 2* | *Рівень 3* |

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 [7]

$$B_{ІБ1} = \sum_{m=1}^{M} B_m(l_m) + \sum_{i=1}^{I}\sum_{m=1}^{M} B_{im}(l_{im}), \qquad (2)$$

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

$$B_{ІБ2} = N\sum_{m=1}^{M} B_m(l_m) + V\sum_{j=1}^{J}\sum_{m=1}^{M} B_{jm}(l_{jm}), \qquad (3)$$

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 (3) випливає, що загальні витрати можуть зменшитись, бо $V<N$. Проте питання конкретної залежності захищеності від перерозподілу засобів захисту у мережі вимагає подальшого дослідження.

## IV Попередній відбір варіантів побудови системи інформаційної безпеки

Методи відбору найбільш раціонального варіанта можуть бути такими: диференційний метод, метод багатокритеріального оцінювання, метод комплексного показника, інтерактивний метод.

При *диференційному методі* вибирається базовий аналог, значення показників якого задаються експертом. Оцінюваний варіант признається задовільним, якщо він не поступається аналогу по жодному з показників. У випадку, коли варіант за деякими показниками поступається аналогу, а за деякими переважає його, цей метод не застосовується. Диференційний метод зручно застосовувати при первинному відборі

варіантів для подальшого аналізу.

Узагальненням диференційного методу є *метод багатокритеріального оцінювання* варіантів по набору показників. У просторі показників задається таке правило порівняння *n*-мірних точок (вирішне правило): точка *x* має більшу перевагу ніж точка *y*, якщо вона має хоча б одну більшу компоненту і ні однієї меншої. Простір показників поділяється на три області: $X_A$ - множина точок, кожна з яких має більшу перевагу, ніж будь-яка точка базового варіанту; $X_B$ - множина точок, кожна з яких не має переваг над базовим варіантом; $X_C$ – множина точок, кожна з яких має меншу перевагу, ніж хоча одна точка, яка відповідає базовому варіанту. Відбір варіантів виконується відповідно до того, в яку область у просторі показників попадає відповідна точка. Але при цьому необхідна більш детальна оцінка відібраних варіантів.

*Метод комплексного показника* полягає у здобутті згортки показників до єдиного комплексного показника за формулами, одна з яких може мати вигляд:

$$F = \sum_{i=1}^{n} a_i X_i, \tag{4}$$

де $a_i$ – вагові коефіцієнти, які відображають "важливість" окремих показників. Цей метод простий, але його неможливо застосувати у нашому випадку, коли показники мають не однакову фізичну природу. Крім того, в комплексному показнику один показник може бути компенсований іншим. Приміром, занижений показник конфіденційності може компенсуватись завищеним показником продуктивності. Це недопустимо, якщо виходити з принципу "найменш захищеної ланки".

Більш досконалим є інтерактивний метод вибору раціонального варіанта, заснований на одній із задач теорії прийняття рішень [8]. Він характеризується використанням експертної інформації не лише для оцінки показників у якісних шкалах, а й для прийняття рішень щодо раціонального вибору. Порівняння багатокритеріальних альтернатив (точок простору показників) виконується за допомогою вирішних правил. Кожне правило базується на інформації, отримуваної від експерта. За допомогою вирішних правил проводиться часткове впорядкування (ранжирування) точок простору показників.

Задовільність деякого вирішного правила можна з'ясувати лише в процесі його застосування. Тому процедура вибору повинна бути кількакроковою. Якщо вирішне правило не забезпечує визначеності впорядкування варіантів, то на наступному кроці має бути отримана додаткова інформація і побудоване більш "сильне" вирішне правило, яке дозволило б усунути невизначеність впорядкування варіантів. Інформацію, отримувану від експерта необхідно перевіряти на змістовність, адекватність задачі і не суперечливість. Додаткова інформація на кожному кроці має порівнюватись із отриманою раніше. Тому процедура побудови вирішного правила має бути інтерактивною.

## V Вибір раціонального варіанту на основі розв'язання задачі багатокритеріального вибору

Враховуючи сказане, задачу можна звести до задачі багатокритеріального вибору, яка успішно вирішується для окремих видів виробів при оцінці якості промислової продукції [9]. Математична постановка задачі така. Задана область параметрів $P(x_1, \ldots, x_m)$ та цільові функції комплексного показника:

$$\begin{aligned} k_1 &= f(x_1, \ldots, x_m), \\ k_2 &= f(x_1, \ldots, x_m), \\ &\ldots \\ k_k &= X_n = f(x_1, \ldots, x_m), \end{aligned} \tag{5}$$

де $k_1, \ldots, k_k$ – вектор критеріїв.

Частину показників вибирають як критерії, так що $n=m+k$. Алгоритм процедури пошуку раціонального варіанту розподілу послуг наведено на рис. 2.

Спочатку формується загальна стратегія інформаційної безпеки, а на її базі часткові стратегії варіантів побудови системи захисту. Формуються вимоги до системи захисту і початкове вирішне правило.

В основному циклі процедури формуються варіанти побудови системи інформаційної безпеки на базі інформації експертів. Отримані варіанти ранжуються у просторі критеріїв і застосовується вирішне правило. Далі вилучається найгірший варіант. Якщо таким чином знайдено раціональний варіант, то процедуру закінчено. В іншому випадку формується інформація для наступної ітерації процедури: деталізуються часткові стратегії, деталізуються вимоги до варіантів і формується "підсилене" вирішне правило.

Перевагою цього методу є те, що збирається і аналізується інформація експертів з її ускладненням до наступних циклів. Тим самим уникається надлишковість інформації.

**Висновки.** Розглянуто розподіл послуг безпеки за рівнями моделі архітектури взаємодії відкритих систем та алгоритм вибору раціонального варіанту розподілу послуг. Напрямками подальшого дослідження є:

- пошук функціональних залежностей критеріїв раціонального вибору варіантів для подальшої формалізації задачі розподілу витрат на інформаційну безпеку та вирішних правил ранжування варіантів;
- використання отриманих результатів для вирішення задачі оптимізації побудови системи інформаційної безпеки документальних телекомунікацій.


**Рисунок 5 – Процедура вибору раціонального варіанту розподілу послуг**

*Література: **1**. Закон України "Про телекомунікації", № 1280-IV від 18. 11. 2003 р. **2** Хорошко В., Ковальова Ю., Плус Д. Розподіл ресурсів у багаторубіжній системі захисту. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 39-43. **3.** Васильцов І. Метод структурної надлишковості як протидія атакам апаратних помилок. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 108-115. **4.** Гончарок М. Х., Островский В. В. Выбор параметров системы защиты информации в цифровых АТС с функциями ISDN. // "Вестник связи", № 4, 2000, – С. 99-105. **5.** Александров А. М., Кравец Л. З., Петренко С. А., Эркин А. Г. Построение наложенных систем криптографической защиты // "Электросвязь", – М:, № 5, 2003. – С. 41-*

*42. **6.** Панин О. А., Журин С. И. Оптимизация параметров систем охранной сигнализации как задача многокритериального выбора. // Защита информации. Конфидент № 1, 2004. – С. 84-87. **7.** Кононович В. Г. Тардаскін М. Ф., Тардаскіна Т. М. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікаційних систем. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С 62-68. **8.** Черноруцкий И. Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248. **9.** Гафт М. Г. Методы оценки технического уровня, Интерактивный подход. //Проблемы информационных систем. – М.: № 2, 1987. – С. 1–21. **10.** Бельфер Р. А. Анализ систем связи в аспекте проектирования информационной безопасности. // "Электросвязь", № 3, 2004. – С 22 – 24. **11.** Додонов О. Г., Горбачик О. С., Кузнєцова М. Г. Захист інформації в інформаційно-аналітичних системах державних органів управління // Реєстрація, зберігання і обробка даних, 2000, Т. 2, № 2, – С. 66-72. **12.** Гайкович В., Першин А. Безопасность электронных банковских систем. –М. Единая Европа, 1994. – 351 с. **13.** Яновский Г. Г. Применение устойчивых пакетных колец в сетях следующего поколения // "Вестник связи", № 7, 2003, - с 54- 56. **14.** Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС). **15.** "Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах". Затверджений наказом ДСТСЗІ СБУ № 76 від 24. 12. 2001 р.*

**УДК 681.5.015: 004.056.57**

# АЛГОРИТМЫ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ С ТОЧНЫМ ВОССТАНОВЛЕНИЕМ ОСНОВНЫХ ПОКРЫВАЮЩИХ СООБЩЕНИЙ

***Ирина Маракова***
*Одесский национальный политехнический университет*

*Анотація:* **Розглянуто використання цифрових водяних знаків (ЦВЗ) для ідентифікації та підтвердження цілісності зображень. На відміну від інших технології, наприклад, цифрового підпису, ЦВЗ не потребує додаткового простору та є невіддільними від основного повідомлення. Фундаментальна проблема створення таких систем — відновлювання основного повідомлення без втрат після детектування ЦВЗ. Розглянуто модульний спосіб занурення та адаптивне детектування ЦВЗ, отримані аналітичні оцінки ймовірності помилок, виконано імітаційне та аналітичне моделювання**.

*Summary:* **A watermark (WM) application to assist in the integrity maintenance and verification of the associated images is considered. There is a great benefit of WM use in context authentication since WM is inseparable from cover message and it does not require additional storage space for supplementary meta-data, as cryptographic signatures for instance. However there is a fundamental problem: the restoration of cover message without any error after WM detection. The modulo addition of a mark and advanced WM detection are used. The formulas for the probabilities of errors are proposed. The analectic and imitation simulations are done.**

*Ключевые слова:* **Цифровые водяные знаки, основное покрывающее сообщение, верификация, цифровая подпись, модульное сложение.**

## I Введение

Технологии цифровых водяных знаков (ЦВЗ) могут использоваться не только для идентификации, но и для подтверждения целостности (верификации) сообщений [1]. В отличие от решающих аналогичные задачи криптографических методов, а именно, формирования цифровой подписи (ЦП), ЦВЗ не увеличивают размер сообщения и не могут быть удалены из стегасообщения (сообщения и ЦВЗ) без существенной потери надежности восприятия. С другой стороны, в качестве ЦВЗ можно использовать ЦП некоторого сообщения при выполнении требований по надежности восприятия стегасообщения (сообщения и ЦВЗ) и устойчивости к преобразованиям канала атаки. Основная проблема верификации на основе ЦП, заключающаяся в несанкционированном удалении ЦП, для ЦВЗ не актуальна. Однако возникает другая проблема: ЦВЗ должны быть инвертируемы, т. е. необходимо точное восстановление исходного основного покрывающего сообщения (ОПС) после детектирования ЦВЗ. Для решения данной проблемы представляется интересным использовать модульный способ погружения ЦВЗ.

При использовании технологий ЦВЗ для контроля копирования, предотвращения несанкционированного копирования, мониторинга рекламного вещания, электронного делопроизводства и т. д. полагается, что