УДК 621. 391.25

БЕЗПЕЧНА ПЕРЕДАЧА КЛЮЧОВИХ ДАНИХ НЕЗАХИЩЕНИМИ КАНАЛАМИ ЗВ'ЯЗКУ ДЛЯ МОДЕЛІ ДЖЕРЕЛА "УНІКАЛЬНИХ ПОВІДОМЛЕНЬ"

Юрій Сергієнко

Київський військовий інститут управління і зв'язку

Анотація: **розглядаються системи передачі ключових даних в умовах перехоплення та існуючі підходи до розв'язання проблеми передачі ключових даних незащищеними каналами зв'язку. Пропонується використання способу кодового захисту ключових даних для моделі джерела "унікальних повідомлень"**

Summary: **here are described the systems of the key data transfer in conditions of interception and existing approaches to the decision of a problem of the key data transfer on unprotection channels of communication. The application a way of code protection key given for model of a source " the unique messages" is offered**

Ключові слова: **незахищені канали зв'язку, ключові дані, кодовий захист, унікальні повідомлення, еквівалентна ймовірність помилки**

І Загальна модель системи передачі ключових даних

У криптографічних додатках найбільш складною організаційно-технічною проблемою є управління ключами. Під управлінням ключами розуміється їхня генерація, тестування, розподіл, введення в дію, зміна, облік, зберігання і знищення. У статті розглядається один з аспектів управління ключами - безпечна передача ключових даних незащищеними каналами зв'язку. Далі під каналом зв'язку розуміється канал доставки. Під ключовими даними (КД) розуміються власне криптографічні ключі або дані, що служать для їхнього виготовлення.

Розглянемо модель системи передачі КД, що включає трьох учасників - двох законних користувачів, що можуть виступати в ролі відправника або одержувача КД, і супротивника. Між відправником і одержувачем є незахищений канал зв'язку (будемо його також називати основним каналом). Супротивник веде перехоплення повідомлень, переданих по основному каналу, через канал перехоплення. Задача законних користувачів - установити загальний секретний ключ, скориставшись незахищеним основним каналом, і створити в каналі перехоплення перешкоди, що запобігають одержанню ключа супротивником. Перешкоди в каналі перехоплення розуміються в широкому розумінні, наприклад, необхідність розв'язання ворогом обчислювально складної задачі, у тому числі, необхідність перебору всіх можливих значень ключа, перешкода в теоретико-інформаційному змісті, створення невизначених ситуацій у процесі передачі КД, перекручене або неповне знання даних перехоплення та ін.

Законні користувачі можуть виконувати два основних сценарії: у першому випадку відправник генерує ключ і безпечним способом передає його одержувачу; у другому випадку користувачі реалізують безпечний протокол обміну даними, що служать для виготовлення загального секретного ключа за заданим алгоритмам.

Поведінка супротивника також може створювати різні ситуації в розглянутій моделі. Зокрема, дії супротивника можуть бути пасивними або активними. При пасивному нападі ведеться перегляд усіх переданих повідомлень і їх наступний криптоаналіз. При активному нападі супротивник виступає в ролі активного ретранслятора, або здійснює маскарад чи іншим способом порушує протокол. Слід зазначити, що в статті не розглядаються проблеми автентифікації користувачів і повідомлень.

Важливими в даній моделі є характеристики основного каналу і каналу перехоплення. На практиці в ролі основного каналу можуть виступати фізичні лінії, канали зв'язку різного типу (радіо-, проводні і т.п), канал читання з пристроїв зберігання КД, квантові канали, кур'єрський зв'язок і ін. Канал перехоплення теж може бути організований по різному: безпосереднє підключення до основного каналу, втручання в квантовий канал, копіювання з пристроїв зберігання КД, перехоплення по побічним електромагнітним випромінюванням і наведенням.

Розглянемо існуючі підходи до розв'язання проблеми передачі КД незахищеним каналах зв'язку.

Традиційно передача КД здійснювалася за сценарієм, коли відправник (наприклад, центр розподілу ключів) генерував ключ і безпечним способом передавав його одержувачу (одержувачам) для організації захищеного каналу. З погляду класичної криптографії, в основі якої лежать симетричні шифри, дана проблема є парадоксальною. КД передаються для організації захищеного каналу, але для їхньої передачі потрібно, у свою чергу, організувати захищений канал, тому що одним з основних допущень є можливість супротивника переглядати всі повідомлення в каналі. За даною логікою, найбільш простим методом захисту КД при передачі є їхнє шифрування, що вимагає попереднього розподілу ключів шифрування КД захищеними каналами. Даний метод широко використовується на практиці. Зокрема, починаючи з американського стандарту ANSI X9.17, пропонується використовувати дво- або трирівневі схеми розподілу ключів [1]. Ключі різних рівнів утворюють

ієрархію. Вищий в ієрархії ключ доставляється вручну, інші ключі передаються каналом зв'язку, зашифрованим на ключах більш високого рівня ієрархії [2]. Очевидно, що даний метод є
не рішенням, а відходом від проблеми: незахищений канал заміняється захищеним у традиційному сенсі, тобто реалізується засекречування переданих повідомлень. Крім того, фаза ручної доставки ключа не завжди припустима і для неї потрібно організовувати захищений канал.

Поява несиметричних криптосистем дещо знизила гостроту проблеми, але відразу слід зазначити як недолік, що їхня теоретична стійкість дотепер не доведена. У найбільше простому сценарії відправник зашифровує повідомлення на відкритому ключі одержувача, отриманому з загальнодоступного довідника, і передає результат одержувачу, що розшифровує повідомлення на своєму несиметричному секретному ключі. Даний метод лежить в основі гібридних криптосистем, у яких подібним способом передається ключ симетричного шифрування. Основні проблеми перебувають в автентичній доставці відкритих ключів користувачів у загальнодоступний довідник і забезпеченні довіри до довідника, тому що фальсифікація відкритих ключів дозволяє ворогу здійснити маскарад. Розв'язання цих проблем вимагає окремих, найчастіше складних організаційних і технічних рішень, наприклад, створення органів сертифікації відкритих ключів [3].

Окремо існує проблема забезпечення безпеки КД при рішенні задач їх автоматизованого децентралізованого виготовлення, обліку, збереження і дистанційного введення в апаратуру. У даний час для забезпечення безпеки КД у цьому випадку застосовують комплекс організаційно-технічних заходів [4, 5]. У цілому це дозволяє забезпечити необхідний рівень безпеки КД, однак часто вимоги виявляються настільки жорсткими, що їхнє виконання приводить або до надзвичайно великих розмірів контрольованих зон, або до ускладнення конструкцій, збільшення ваги і вартості устаткування.

II Кодовий захист ключових даних для моделі джерела "унікальних повідомлень"

Одним із способів захисту КД є кодовий захист (КЗ). Спосіб КЗ базується на теорії завадостійкого кодування і концепції каналу з витоком А.В. Вайнера [6] і відноситься до класу ймовірносно-криптографічних систем захисту.

Його сутність полягає в наступному. Фізичний датчик випадкових чисел формує послідовність рівноймовірних і взаємонезалежних двійкових символів $\gamma_{k'}$. Цю послідовність розбивають на блоки довжини $k=n-k'$, де n – загальна довжина блоку коду V. Блоки k вважають інформаційними символами коду V і для них у кодері по правилам цього коду знаходитися k′ перевірочних символів $f(\gamma_{k'})$. Перевірочні символи складають послідовно по *mod*2 з інформаційними символами S_k і суми $S_k + f(\gamma_k)$ відправляють у основний канал безпосереднього запису k-блоку випадкових символів $\gamma_{k'}$. Таким чином, A по каналу передає n-блоки наступного вигляду:

$$X_n=(\gamma_{k'},\ S_k + f(\gamma_{k'})), \qquad (1)$$

де $f(\gamma_k)$ - правило формування перевірочних символів коду V,

$\gamma_{k'}$ – блоки випадкових символів,

S_k – блоки інформаційних символів

На прийомному боці спочатку за отриманими $\gamma_{k'}$ випадковими символами формують k перевірочних символів (за однаковим з кодуванням правилом $f(\gamma_k)$), а після цього результат складають побітно з інформаційними k-блоками:

$$Y_n=S_k+f(\gamma_k)+f(\gamma_k)= S_k\ , \qquad (2)$$

де Y_n – отримана B інформація

З (2) слідує, що B отримує S_k без помилок.

В каналі перехоплення супротивник отримує Z_n з ймовірністю помилки p, що дорівнює накладанню вектора помилки E_n: $Z_n=Y_n+ E_n$

$$Z_n=(\gamma_{k'}+E_n, S_k+f(\gamma_k)+E_n), \qquad (3)$$

де E_n - вектор помилки довжиною n, $p(E=1)=p$, $p(E=0)=1-p$.

Це приводить до значного розмноження помилок, тому при $n\to\infty$ кількість інформації в каналі перехоплення відносно переданої інформації $I(S_k/Z_n)$ прямує до нуля, що виключає можливість правильного декодування перехопленної інформації. Ефект досягається ціною ускладнення кодування і створення лише деякого погіршення якості каналу перехоплення в порівнянні з каналом одержувача. При такому підході передбачається, що супротивник має у своєму розпорядженні такою ж самою апріорну сукупність відомостей, що і законний

користувач, тобто ніякі секретні дані (ключові дані) для реалізації способу кодового захисту не використовуються.

Внаслідок особливостей моделі беззбиткових джерел (КД, як повідомлення, відносяться до такого класу джерел), повідомленнями якого є КД, можливості й оцінки ефективності кодового захисту КД також мають специфіку.

КД, як повідомлення джерела, мають властивість унікальності. У [7] було введене поняття "унікального повідомлення" (УП). УП має ту властивість, що до моменту початку його передачі в точці прийому вже є інформація, що дозволяє, у принципі, єдиним способом визначити це повідомлення. Це може бути зроблено, наприклад, повним перебором усіх можливих повідомлень і перевіркою їх на допустимість. Необхідність передачі УП по каналах зв'язку пояснюється трудомісткістю цієї процедури.

Варто розрізняти УП зі штучною або природною надмірністю, де також можна перевірити допустимість прийнятих повідомлень, але повний перебір принципово не дозволяє виділити єдине повідомлення.

Нехай E = f (S) - обчислювально необоротна функція (ОНФ) [8], тобто така, що зворотна функція S = φ(E) існує, однак, обчислення S за відомим E вимагає невиконанно великого числа операцій або ємності устаткування. Тоді, якщо E відомо в точці прийому, то S при передачі по каналу зв'язку буде являти собою УП. Найбільше важливим випадком УП, що і аналізується в даній статті, є КД для спеціальної апаратури, що можуть зберігатися, оброблятися і передаватися сполучними лініями або навіть спеціальними каналами зв'язку.

Можна також вважати, що УП у вигляді КД "передаються" каналом зв'язку з перешкодами й у тому випадку, коли робиться спроба несанкціонованого зчитування КД із запам'ятовувальних пристроїв шифраторів після виконання процедури аварійного стирання їхнього вмісту. Характерною рисою УП у вигляді КД є їх відносно малий об'єм і рівноймовірність, тобто відсутність збитковості.

Якщо як E розуміти криптограму спеціальної апаратури, отриману з використанням КД X, то при довжині криптограми, що перевищує відстань одиничності, повний перебір усіх X дозволить визначити єдино правильний ключ [9].

З іншого боку, знання криптограми E не дозволяє для спеціальної апаратури обчислити ключ X у доступний для розрахунків час, що остаточно підтверджує властивість "унікальності" для КД.

Існує декілька критеріїв оцінки ефективності застосування КЗ УП. Один з них – оцінка за критерієм еквівалентної ймовірності помилки. Еквівалентна ймовірність помилки P_e – це така ймовірність помилки, яку необхідно було б забезпечити в каналі перехоплення без КЗ, щоб отримати таку ж якість перехопленої інформації, яку при використанні КЗ забезпечує ймовірність помилки в каналі перехоплення p.

Для кодів Хеммінга

$$P_э = \frac{1}{2}\left(1 - (1 - 2 \cdot p)^{\frac{n+1}{2}}\right), \tag{4}$$

Залежність P_e від p для різних параметрів кодів приведена на рисунку 1.

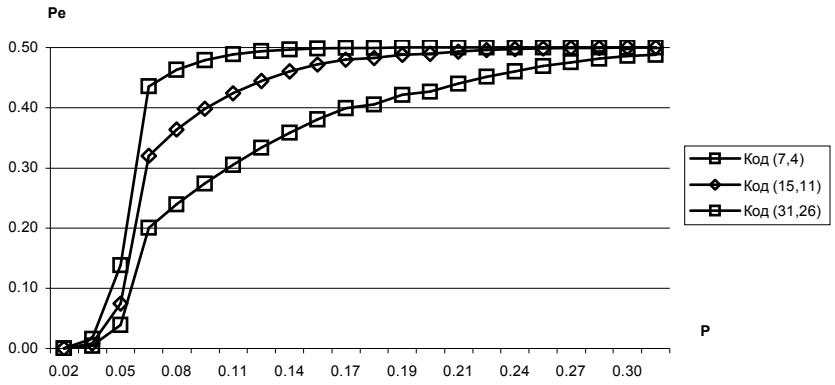

Рисунок 1

З отриманих результатів слідує, що чим довше коди, тим ефективніше кодовий захист, тим ближче канал перехоплення до "обриву" (ймовірність помилки в ньому наближається до 0,5).

Також в залежності від умов застосування КЗ УП, можна визначити найбільш оптимальний код для визначеної області значень p.

Крітерій P_e простий та зручний для розрахунків, але ж він не може одностайно визначити ефективність КЗ УП. Наприклад, при використанні тривіального коду з *r* однаковими перевірочними символами, отриманими як поелементна сума за mod2 усіх інформаційних, дає максимальне значення P_e. Тому велике значення P_e є необхідною, але недостатньою умовою ефективності застосування КЗ УП, що вимагає проведення розрахунків за іншими критеріями.

Наступними шляхами досліджень застосування КЗ при передачі УП незащищеними каналами зв'язку є оцінка ефективності за критерієм оптимальної обробки при декодуванні списком об'єму N з мінімальною ймовірністю помилкового декодування $P_{пд}$.

Література: 1. American National Standard X9.17-1985. Financial Institution Key Management (Wholesale), ANSI. 2. D.M.Balenson. Automated Distribution of Cryptographic Keys Using the Financial Institution Key Management Standard// IEEE Comm. Magazine, vol.23, No.9, Sept 1985, pp.41-46. 3. ISO/IEC 9594-8. Information Technology - Open Systems Interconnection - Directory: Authentication Framework. 2nd ed. 1995-09-15. 4. Безопасность связи. Часть 1/Под общей редакцией А.Н. Авсюкевича, А.П. Аксенова, В.Г. Ефимова, В.Ф. Комаровича / - М.: Военное издательство.- 1985.-248с. 5. Белов А.И. Обеспечение непрерывности управления и связи при ведении операций // Военная мысль.-1985.-№2(27).-С.82-96. 6. Wyner A. D. The wire-tap channel // Bell Syst. Techn. J.-1973. V. 54. № 8. P. 1335-1368. 7. Коржик В.И. Помехоустойчивое кодирование "уникальных сообщений" в сетевых системах. Доклад на 7 всесоюзной школе-семинаре по вычислительной технике. Ереван, 1982, с. 73-77. 8. Rivest R.L., Adleman L. And Shamir A. A method obtaining digital signatures and public-key cryptosystems. Somm. ACM 21.2, <Feb. 1978>, p.120-126. 9. Diffie W., Hellman M.E. New directions in cryptography. IEEE Trans. It.- 1976, v.22, № 6, p. 644-654.