DOI 10.31891/2307-5732-2018-267-6(2)-209-212
УДК 621.39

В.І. СТЕЦЮК, В.В. МІШАН, О.В. БОЖЕНОК
Хмельницький національний університет

МЕТОДИ КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

З урахуванням стрімкого розвитку телекомунікаційних систем та інформаційних ресурсів, питання, пов'язані з захистом інформації, мають першочергове значення. Вирішення цих питань нерозривно пов'язане зі створенням унікальних телекомунікаційних систем і забезпеченням їх безпеки в умовах широкого використання нових інформаційних технологій і дії внутрішніх і зовнішніх загроз інформаційної безпеки. В даній роботі уточнена класифікація методів шифрування та захисту інформації стосовно телекомунікаційних систем і мереж. Розкрито питання несанкціонованого доступу в каналах передачі телекомунікаційних даних. Наведені структурні схеми та математичні моделі симетричної та асиметричної криптографічних системи. Здійснено аналіз переваг та недоліків кожної з систем. Так, поряд з обчислювальною простотою та інтуїтивною зрозумілістю симетричних криптосистем, вони мають ряд серйозних недоліків: проблема поширення симетричних ключів і їх зберігання. Перевагою асиметричного протоколу є наявність загальнодоступних відкритих ключів, що не вимагає секретності і закритих ключів, які зберігаються у користувачів. Разом із тим, асиметричні криптосистеми також мають свої недоліки, наприклад необхідність захисту відкритих ключів від підміни та менша швидкодія в порівнянні із симетричними. Найбільш досконалі рішення полягають у поєднанні алгоритмів обох видів шифрування, тобто побудова гібридних криптосистем. Саме вони являються найбіль перспективними з точки зору застосування в телекомунікаційних мережах і системах.

Ключові слова: мережа, безпека, інформація, захист, несанкціонований доступ, криптосистема, алгоритм, шифрування, дешифрування, протокол.

V.I. STETSIUK, V.V. MISHAN, O.V. BOZHENOK
Khmelnytskyi National University

CONTROL METHODS OF INFORMATION FLOWS IN TELECOMMUNICATION SYSTEMS

Modern society is accompanied by the rapid development of information resources and the growing role of the information sphere, which represents a set of information, information infrastructure, entities that collect, compile, disseminate and use information. Information sphere is a system-forming factor of society's life and actively influences the state of all components of security of the country. The material basis of the information sphere is the united information and telecommunication space of the country as the basis for solving the tasks of socio-economic, political, military, scientific and cultural development of the country and ensuring its security. In such conditions, the role of information is significantly increased and the problem of forming a single information space of the country and the transition from the industrial to the information society is actualized. A prerequisite for solving this problem is the improvement of information provision of the bodies of state administration, scientific, industrial, banking and other structures on the basis of reliable, timely, complete, systemically organized and safe information as the basis for effective management, security of the individual, society and the state. The solution of these issues is inextricably linked with the creation of unique telecommunication systems and the provision of their security in the widespread use of new information technologies and the actions of internal and external threats to information security. In view of this, the provision of information security implies the existence of an effective system for the administration and control of information security on telecommunications objects, the results of which are implemented a set of adequate methods of sustainable protection against threats, inextricably linked with the use of the results of in-depth studies of the fundamental aspects of information security, development scientifically grounded methods of providing information security protection in conditions of uncertainty, risk, external actions and dynamic changes in the objects of activity. The classification of methods of encryption and protection of information concerning telecommunication systems and networks is specified in the work. Issues of unauthorized access in telecommunication data transmission channels are disclosed. Structural schemas and mathematical models of symmetric and asymmetric cryptographic systems are presented. The analysis of the advantages and disadvantages of each system is analyzed.

Keywords: network, security, information, protection, unauthorized access, cryptosystem, algorithm, encryption, decryption, protocol.

Вступ.

Сучасне суспільство супроводжується стрімким розвитком інформаційних ресурсів. В таких умовах істотно підвищується роль інформації і актуалізується проблема формування єдиного інформаційного простору країни та переходу від індустріального до інформаційного суспільства. Необхідною умовою вирішення цієї проблеми є вдосконалення інформаційного забезпечення діяльності органів державного управління, наукових, промислових, банківських і інших структур на основі надання достовірної, своєчасної, повної, системно організованої і безпечної інформації, як основи ефективного управління, безпеки особи, суспільства і держави.

Вирішення цих питань нерозривно пов'язане зі створенням унікальних телекомунікаційних систем і забезпеченням їх безпеки в умовах широкого використання нових інформаційних технологій і дії внутрішніх і зовнішніх загроз інформаційної безпеки [1–4]. Яскравим проявом таких загроз є широкомасштабні «інформаційні війни», несанкціонований доступ до захищених інформаційних ресурсів, недостатня інформованість посадовців органів державного управління при аналізі технічних, соціально-економічних, політичних, військових, екологічних та інших ситуацій.

З урахуванням цього забезпечення інформаційної безпеки припускає наявність ефективної системи адміністрування і контролю безпеки інформації на телекомунікаційних об'єктах, за результатами

функціонування якої реалізується комплекс адекватних методів стійкого захисту від загроз, нерозривно пов'язаних з використанням результатів глибоких досліджень фундаментальних аспектів інформаційної безпеки, розробкою науково обгрунтованих методів забезпечення захисту інформації в умовах невизначеності, ризику, зовнішніх дій і динамічних внутрішніх змін об'єктів діяльності.

Основна частина.

Захист інформації в сучасних телекомунікаційних мережах – сукупність заходів і відповідних засобів, які забезпечують захист програм, баз і банків даних від несанкціонованого доступу, використання, руйнування або завдання шкоди в будь-якій іншій формі. Необхідність в інформаційній безпеці випливає із самої природи мережних служб, сервісів і послуг. Криптографічний захист інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування / відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1]. З точки зору несанкціонованого доступу канал передачі телекомунікаційних даних можна представити наступним чином:

Рис. 1. Канал передачі даних

Процедури шифрування і дешифрування можна представити в наступному вигляді:

$$c = E_{k_e}(p); \quad p = D_{k_d}(c) \tag{1}$$

де p і c відповідно – відкритий і зашифрований тексти, k_e і k_d – ключі шифрування і дешифрування; E_{k_e}, D_{k_d} – функції шифрування з ключем k_e і дешифрування з ключем k_d відповідно, причому для будь-якого відкритого тексту справедливе співвідношення:

$$D_{k_d}(E_{k_e}(p)) = p \tag{2}$$

Шифрування і дешифрування повідомлень відбувається на вході і виході каналу передачі даних. Несанкціонована особа (НО) аналізує процес передачі інформації по каналу зв'язку і має можливість формувати свої власні повідомлення.

Розрізняють наступні типи алгоритмів шифрування: симетричні (із закритим або секретним ключем), асиметричні (з відкритим ключем) та гібридні (рис. 2).

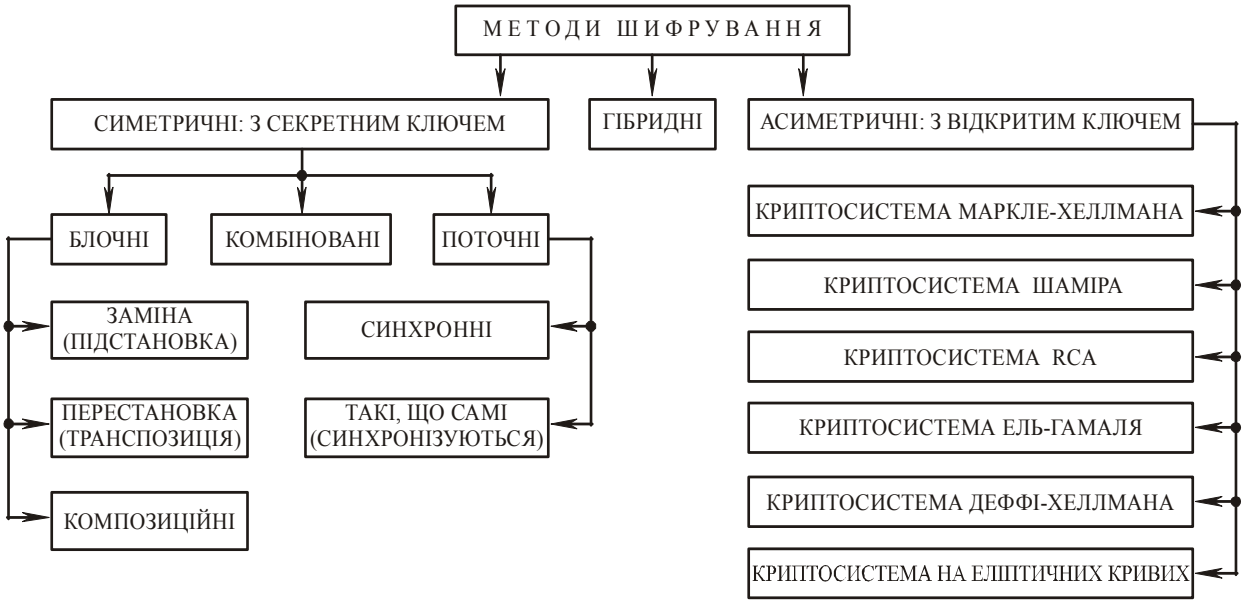

Рис. 2. Класифікація методів шифрування інформації

При симетричному методі ключ шифрування збігається з ключем дешифрування (рис. 3).

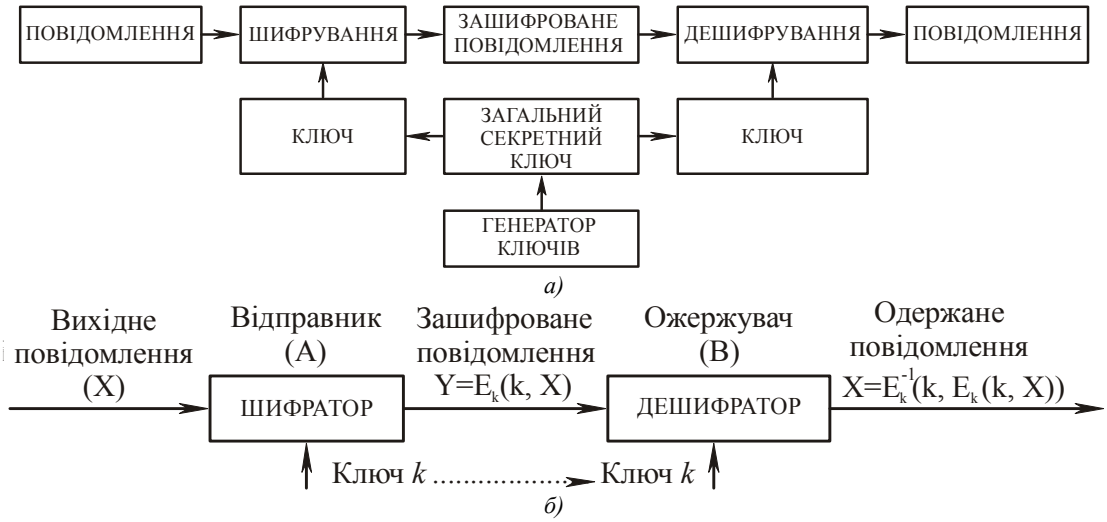

Рис. 3. Схема симетричної криптосистеми:
а) структурна схема; б) математична модель

В асиметричних алгоритмах (рис. 4) для шифрування і дешифрування використовуються різні ключі, причому знання одного з них не дає практичної можливості визначити інший.

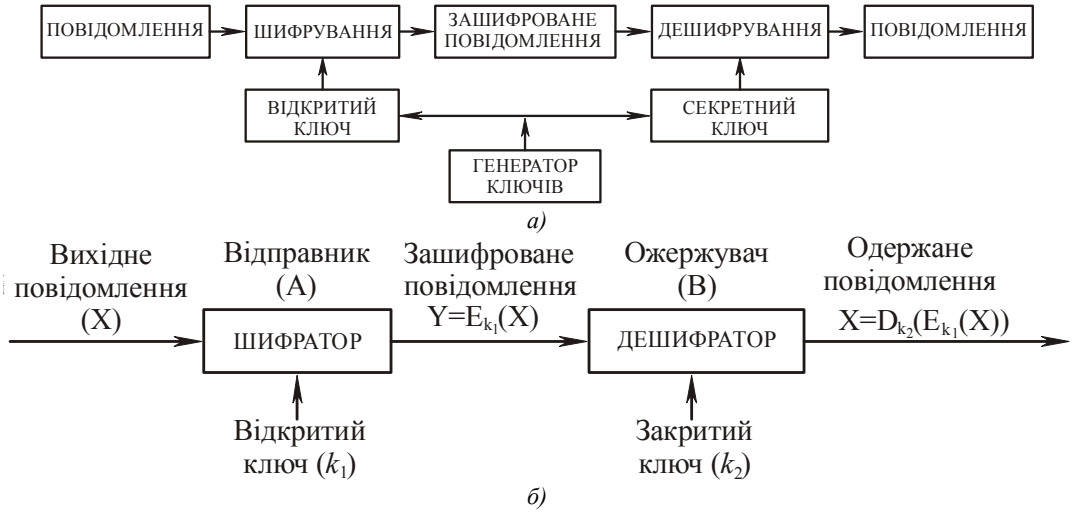

Рис. 4. Схема асиметричної криптосистеми:
а) структурна схема; б) математична модель

Асиметричні системи характеризуються тим, що для шифрування і дешифрування використовуються різні ключі, пов'язані між собою певною залежністю. При цьому дана залежність така, що встановити один ключ, знаючи інший, з обчислювальної точки зору дуже важко. Один з ключів (наприклад, ключ шифрування) може бути зроблений загальнодоступним, і в цьому випадку проблема отримання загального секретного ключа для зв'язку відпадає. Якщо зробити загальнодоступним ключ розшифрування, то на базі отриманої системи можна побудувати систему аутентифікації переданих повідомлень.

Асиметричні алгоритми шифрування визначається трьома алгоритмами: генерації ключів, шифрування і розшифрування. Алгоритм генерації ключів відкритий і вільно можна подати йому на вхід випадковий рядок r потрібної довжини та у відповідь отримати пару ключів (k_1, k_2). Один з ключів (наприклад, k_1) публікується, він відкритий, а другий (секретний), зберігається в таємниці. Алгоритми шифрування E_{k_1} і дешифрування D_{k_2} такі, що для будь-якого відкритого тексту m: $D_{k_2}(E_{k_1}(m)) = m$.

Висновки

Переваги та недоліки симетричного протоколу. Поряд з обчислювальної простотою та інтуїтивною зрозумілістю симетричних криптосистем, вони мають ряд серйозних недоліків: проблема поширення симетричних ключів і проблема їх зберігання. При використанні симетричних криптосистем для шифрування інформації між користувачами криптографічного мережі необхідно забезпечити безпечну передачу ключів шифрування між усіма учасниками криптографічного обміну. При цьому передача ключа шифрування обов'язково повинна здійснюватися по закритому каналу, так як перехоплення зловмисником даного ключа веде до компрометації всієї криптографічної мережі, і подальше шифрування інформації втрачає сенс. Однак наявність закритого каналу зв'язку дозволяє передавати і сам відкритий текст з даного каналу. Таким чином, необхідність шифрування як би відпадає. Проблема зберігання симетричних ключів шифрування полягає також і в тому, що всі учасники криптографічної мережі повинні володіти ключем

шифрування, тобто мати до нього доступ. При великій кількості учасників криптографічного обміну даний факт значно підвищує ймовірність компрометації ключів шифрування. У зв'язку з цим, використання симетричних алгоритмів передбачає наявність взаємної довіри сторін. Несумлінність відносини одного з тисячі учасників криптографічного обміну до питання зберігання ключів може призвести до витоку ключової інформації, через що постраждають всі учасники, в тому числі і ті, що сумлінно ставляться до своїх обов'язків зі зберігання ключів. Імовірність компрометації ключів тим вище, чим більша кількість користувачів входить в криптографічний мережу. Це є великим недоліком симетричних криптосистем.

Переваги та недоліки асиметричного протоколу. Перевагою протоколу є те, що розподіл відкритих ключів не вимагає секретності. У мережі зв'язку нерідко відкриті ключі користувачів містяться в загальнодоступній базі даних, а закриті ключі зберігаються у користувачів.

Переваги асиметричних криптографічних систем перед симетричними криптосистемами:

- в асиметричних криптосистемах вирішена складна проблема розподілу ключів між користувачами, так як кожен користувач може згенерувати свою пару ключів сам, а відкриті ключі користувачів можуть вільно публікуватися і поширюватися мережевими комунікаціями;

- зникає квадратична залежність числа ключів від числа користувачів; в асиметричній криптосистемі число використовуваних ключів пов'язане з числом абонентів лінійною залежністю (в системі з N користувачів використовуються $2N$ ключів), а не квадратичною, як в симетричних системах;

- асиметричні криптосистеми дозволяють реалізувати протоколи взаємодії сторін, які не довірнюють один одному, оскільки при використанні асиметричних криптосистем закритий ключ повинен бути відомий тільки його власнику.

Недоліки асиметричних криптосистем:

- на даний момент немає математичного доказу незворотності використовуваних в асиметричних алгоритмах функцій;

- асиметричне шифрування істотно повільніше симетричного, оскільки при шифруванні і розшифровці використовуються досить ресурсомісткі операції; з цієї ж причини реалізувати апаратний шифратор з асиметричним алгоритмом істотно складніше, ніж реалізувати апаратно-симетричний алгоритм;

- необхідність захисту відкритих ключів від підміни.

Якими б недоліками і перевагами не володіли асиметричні та симетричні криптографічні методи шифрування, необхідно відзначити, що найбільш досконалі рішення – це ті, які вдало поєднують в собі алгоритми обох видів шифрування, тобто гібридні. Саме вони являються найбільш перспективними з точки зору застосування в телекомунікаційних мережах і системах.

Література

1. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях : навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса : ОНАЗ ім. О. С. Попова, 2011. – 184 с.

2. Стецюк В. І. Аналіз методів кодування інформації в цифровому телебаченні / В. І. Стецюк // Вимірювальна та обчислювальна техніка в технологічних процесах : міжнародний науково-технічний журнал. – 2000. – № 3. – С. 78–82.

3. Стецюк В. І. Вплив психовізуальної надлишковості телевізійних повідомлень на спектр частот відеосигналів / В. І. Стецюк // Вимірювальна та обчислювальна техніка в технологічних процесах : міжнародний науково-технічний журнал. – 2001. – № 3. – С. 77–79.

4. Стецюк В. І. Аналіз систем обмеженого доступу в мережах кабельного телебачення / В. І. Стецюк // Вимірювальна та обчислювальна техніка в технологічних процесах : міжнародний науково-технічний журнал. – 2002. – № 2. – С. 172–178.

References

1. Zakharchenko M. V. Asymetrychni metody shyfruvannia v telekomunikatsiiakh : navch. posib. / M. V. Zakharchenko, O. V. Onatskyi, L. H. Yona, T. M. Shynkarchuk. – Odesa : ONAZ im. O. S. Popova, 2011. – 184 s.

2. Stetsiuk V. I. Analiz metodiv koduvannia informatsii v tsyfrovomu telebachenni / V. I. Stetsiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh : mizhnarodnyi naukovo-tekhnichnyi zhurnal. – 2000. – № 3. – S. 78–82.

3. Stetsiuk V. I. Vplyv psykhovizualnoi nadlyshkovosti televiziinykh povidomlen na spektr chastot videosyhnaliv / V. I. Stetsiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh : mizhnarodnyi naukovo-tekhnichnyi zhurnal. – 2001. – № 3. – S. 77–79.

4. Stetsiuk V. I. Analiz system obmezhenoho dostupu v merezhakh kabelnoho telebachennia / V. I. Stetsiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh : mizhnarodnyi naukovo-tekhnichnyi zhurnal. – 2002. – № 2. – S. 172–178.

Рецензія/Peer review : 20.11.2018 р. Надрукована/Printed :19.12.2018 р.
Рецензент: д.т.н., доц. Любчик В.Р.