властивості кореляційної імунності першого порядку. Приклад такого S-блоку наведено у роботі [3]. У цьому випадку усі кореляційні коефіцієнти дорівнюють 0.5, отже, буд-який "вихід" статистично не залежить від "входу", що унеможливлює застосування запропонованого методу.

Список літератури

1. *Siegenthaler T.* Correlation immunity of non-linear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. –1984. –V.30. –P.776-780.

2. *Siegenthaler T.* Decrypting a class of stream ciphers using ciphertext only // IEEE Trans. Comput. –1985. – V.34.

3. *Л.Скрипник, О.Дирда.* Порівняльний аналіз методів побудови та властивостей S-блоків ряду сучасних криптографічних алгоритмів. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, –К.: 2005. –Вип.10. –С.85–98.

Надійшла 17.05.2007 р.

УДК 681.3.07

Жердєв М.К., Лєнков С.В., Пампуха І.В.

СПОСІБ ЗАШИФРУВАННЯ - РОЗШИФРУВАННЯ ІНФОРМАЦІЇ З ВИПАДКОВИМ, ВІДКРИТИМ І АДАПТИВНИМ КЛЮЧЕМ

Спосіб зашифрування – розшифрування інформації з випадковим, відкритим і адаптивним ключем (ВВАК) призначений для криптографічного перетворення інформації в мережі, захисту від атак вірусів і несанкціонованого доступу (хакерів) в комп'ютери через цю мережу. Він може бути реалізований програмно, апаратно і програмно-апаратно.

Кращим захистом від способів криптоаналізу є вибір ключового слова по довжині, рівного довжині відкритих даних (ВД), яке відрізняється від відкритих даних за статистичними показниками. Таку схему було запропоновано інженером компанії AT&T Гілбертом Вернамом в 1918 р., у якій оперують не буквами, а двійковими числами. Коротко це можна виразити формулою [1]:

$$C_i = p_i \oplus k_i,$$

де:

p_i – *i-е* двійкове значення ВД;

k_i – *i-е* двійкове значення ключа;

C_i – *i*-е двійкове значення закритих даних (ЗД);

$\oplus$ – операція «виключення АБО».

Таким чином, ЗД генеруються шляхом побітового виконання операції виключення «АБО» для ВД й ключа.

Основною проблемою при цьому є спосіб генерування ключа, який за статистичними показниками відрізнявся б від ВД. Вернам запропонував використовувати закільцьовану стрічку, тобто циклічне повторення ключового слова, тому насправді виконувалась операція зашифрування ВД, хоч і з дуже довгим, але все-таки ключем, який повторюється. Незважаючи на те, що така схема, в силу дуже великої довжини ключа, значно ускладнює завдання криптоаналізу, схему можна «зламати», маючи в розпорядженні досить довгий фрагмент ЗД, відомі або ймовірно відомі фрагменти ВД або й те, і інше відразу.

При цьому способі зашифрована інформація «злому» не піддається, якщо в якості ключа використовувати випадкову інформацію, тобто в цьому випадку статистичні характеристики ВД й випадкового ключа не корельовано.

Офіцером армійського корпуса зв'язку Джозефом Моборном були запропоновані такі поліпшення схеми Вернама, які зробили цю схему винятково надійною [1]. Він запропонував відмовитися від повторень, а випадковим чином генерувати ключ, довжина якого дорівнює довжині ВД. Така схема одержала назву стрічки однократного використання (або схеми з одноразовим блокнотом) і «злому» не піддається. В результаті її застосування на виході формується випадкова послідовність, яка немає статистичного взаємозв'язку з ВД. Оскільки в цьому випадку ЗД не дають ніякої інформації про ВД, немає способу й «зламати» ключ. Ця ідея була практично реалізована на механічних пристроях.

Основним недоліком схеми Джозефа Моборна є низька швидкість передачі інформації. Тому з розвитком електронних засобів зашифрування - розшифрування інформації ця схема втратила актуальність.

Складність практичного застосування цього способу полягає в тому, що й відправник, й одержувач повинні мати один і той же випадковий ключ і можливість захищати його від сторонніх [1]. Тому, незважаючи на переваги способу Вернама перед іншими способами, виконаними на електронних пристроях, на практиці його реалізувати складно й дуже дорого.

Основна трудність є те, що генератори випадкових чисел на передавальній і прийомній сторонах повинні працювати синхронно й синфазно.

Авторам запропонованого способу зашифрування - розшифрування інформації з випадковим, відкритим і адаптивним ключем вдалося забезпечити синхронну й синфазну роботу випадкових генераторів на передавальній і прийомній сторонах, при цьому відправник й одержувач мають один і той же випадковий ключ. Таким чином, у запропонованому способі зашифрування - розшифрування інформації з випадковим, відкритим і адаптивним ключем реалізована схема Вернама на електронних пристроях. В способі використовуються випадкові (з рівноймовірним розподілом ключі на множині 2^n, де n – розрядність випадкового генератора), особисті і адаптивні ключі, для яких математично доведено, що їх визначити практично не можливо. При цьому ключі спеціально не генеруються, нікому не назначаються і не розподіляються, а автоматично формуються випадковими генераторами, які працюють синхронно й синфазно на передавальній й прийомній сторонах в процесі зашифрування - розшифрування інформації. Ця обставина дозволяє скоротити до мінімуму вплив людського фактору на надійний захист інформації і скоротити сили й засоби, які виділяються в інших способах зашифрування - розшифрування інформації для забезпечення конфіденційності.

Запропонований спосіб дозволив усунути недоліки існуючих способів, спростити процес зашифрування - розшифрування інформації й може бути реалізований за допомогою найпростіших мікроконтролерів, в яких передбачено програмно-апаратний захист від несанкціонованого доступу.

Розглянемо реалізацію способу зашифрування – розшифрування інформації з випадковим, відкритим й адаптивним ключем у пристрої захисту мереж і терміналів (ПЗМТ-1) від несанкціонованого доступу на прикладі роботи між двома абонентами.

Структурна схема включення ПЗМТ-1 в мережу обміну між двома абонентами зображено на рис. 1. Відкриті дані з виходу персональної електронно-обчислювальної машини подаються на пристрій ПЗМТ-1. Після ПЗМТ-1 ЗД подаються на модем, у якому перетворюється і подається в лінію зв'язку. По лінії зв'язку ці дані (через автоматизовану телефонну станцію (АТС) і інші елементи) подаються на модем приймальної частини. З виходу модему ЗД подаються на ПЗМТ-1, в якому вона розшифровується і передається на ПЕОМ. З рис. 1 видно, що ПЗМТ-1 включено в мережу послідовно з ПЕОМ, тому він виконує роль фільтра для інформації, яка надходить з мережі в ПЕОМ. Якщо ця інформація не відповідає ключу розшифрування, то вона руйнується на виході ПЗМТ-1, тобто не поступає на ЕОМ. Таким чином, пристрій захищає не тільки інформацію

в мережі, але і ПЕОМ, як від атак вірусів так і від несанкціонованого доступу до неї через цю мережу.

Рис. 1. Структурна схема включення ПЗМТ-1 в мережу обміну між двома абонентами

Структурна схема організації обміну між абонентами приведена на рис. 2. Абонентам присвоюються попарно особисті і випадкові ключі на етапі виробництва при програмуванні мікроконтролера ПЗМТ-1, пам'ять якого надійно захищена від несанкціонованого доступу програмно-апаратно. Наприклад, для абонентів A_1 і A_2 присвоюється ключ $K_{12} = K_{21}$. Для мережі (рис. 2) принцип побудови ключів приведений в табл.1. Для кожного абонента з табл.1 вибирається стовпчик, що відповідає номеру цього абонента. В залежності від числа абонентів мережі з цього стовпчика табл.1 вибирається необхідна кількість ключів.

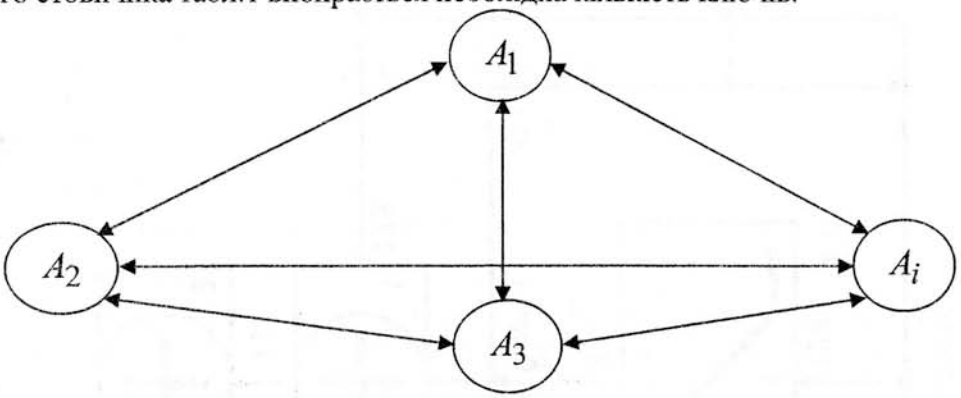


Рис. 2. Структурна схема організації обміну між абонентами

Таблиця 1.

A_i / A_j	A_1	A_2	A_3	…	A_j
A_1		K_{12}	K_{13}	…	K_{1j}
A_2	K_{21}		K_{23}	…	K_{2j}
A_3	K_{31}	K_{32}		…	K_{3j}
…	…	…	…		…
A_i	K_{i1}	K_{i2}	K_{i3}	…	

Структурна схема алгоритму криптографічного перетворення (криптосхема) при зашифруванні ВД (див. рис. 3) складається з трьох частин:

а) підалгоритма формування ключів;

б) підалгоритма зашифрування ВД;

в) генератора випадкових чисел (ГВЧ) з рівноймовірним розподілом блоків, з якого при встановленні в вихідний стан використовується 16 Байт (один блок).

СПОСІБ ЗАШИФРУВАННЯ - РОЗШИФРУВАННЯ ІНФОРМАЦІЇ З ВИПАДКОВИМ, ВІДКРИТИМ І АДАПТИВНИМ КЛЮЧЕМ

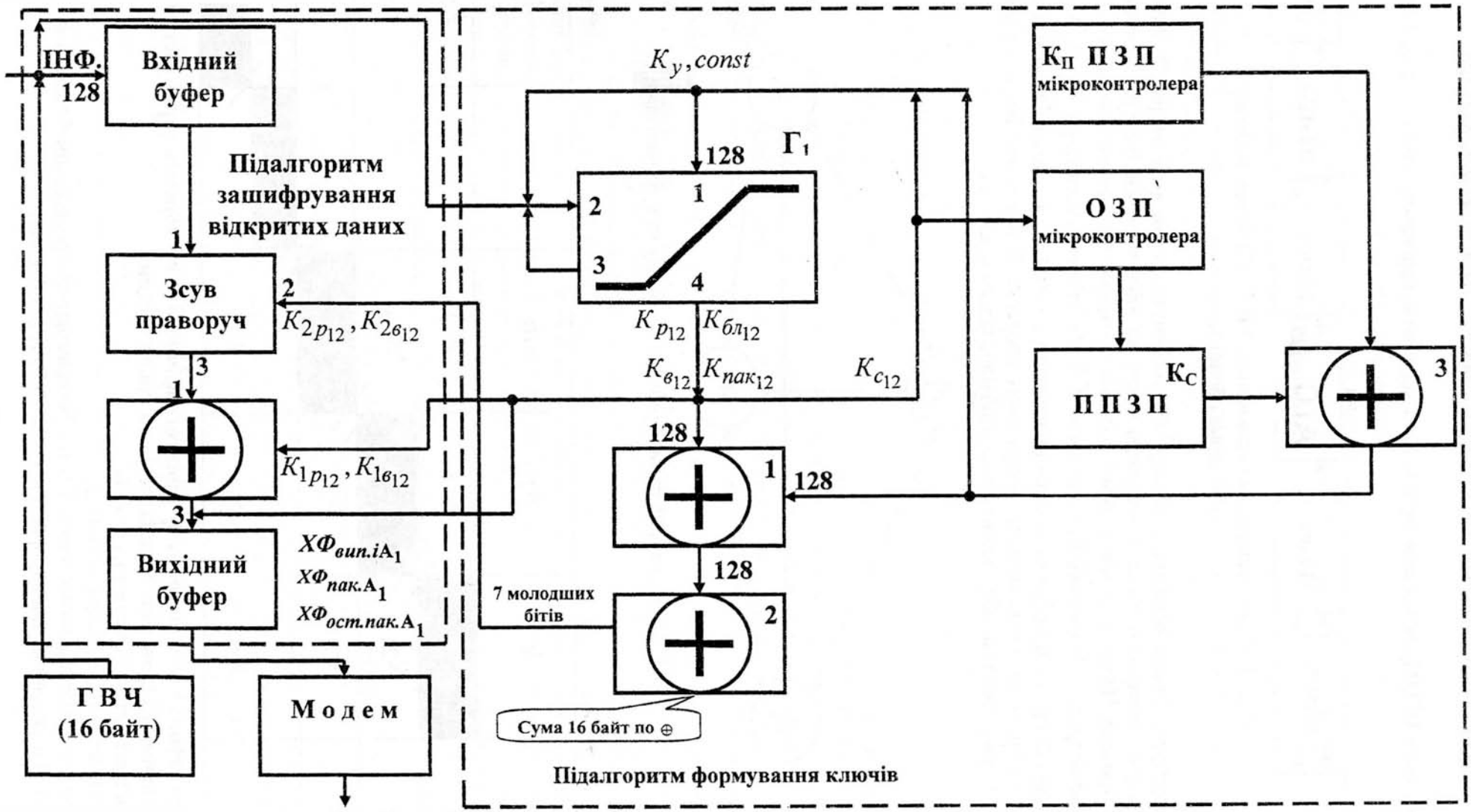


Рис. 3. Структурна схема криптографічного перетворення при зашифруванні відкритих даних

Структурна схема підалгоритму формування ключів містить (див. рис. 4):

І. Керований, випадковий, нелінійний і адаптивний елемент (КВНАЕ-1) - Γ_1 (рис. 4) з керованими параметрами, який має два входи і два виходи.

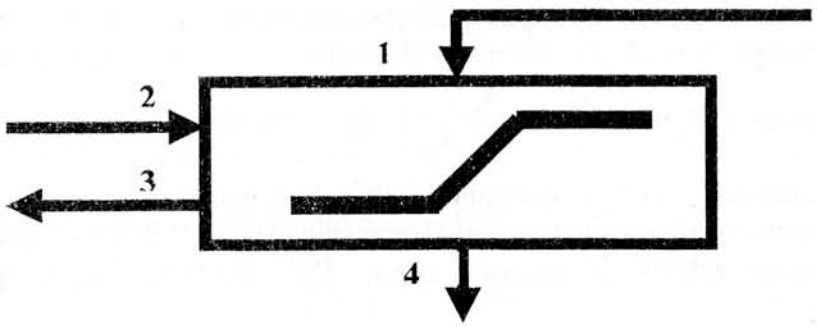


Рис. 4. КВНАЕ-1

На входи надходять:

1 - ключ управління режимами (паралельний код) $K_{\text{у}}$, в якості якого використовуються ключі $K_{\text{п}} \oplus K_c$ (початковий ключ, сеансовий ключ), або $K_{бл.}$ (ключ блока), або $K_{пак.}$ (ключ пакета) з рівноймовірним розподілом;

2 - $K_{\text{у}}$ або випадкова інформація або ВД в послідовному коді.

З виходів знімаються:

3 - хеш-функція - $ХФ$, яка розраховується автоматично і дозволяє автоматично в сукупності з індивідуальними ключами здійснювати цифровий підпис, аутентифікацію і т.і.

Примітка: особливістю цієї $ХФ$ є те, що при спотворенні хоча б одного біта інформації, яка передається вона змінює своє значення. При існуючих способах формування хеш-функції можуть виникнути випадки коли при зміні визначених біт в інформації, хеш-функція не змінює свого значення. Тому вона не може використовуватися для синхронного й синфазного керування випадковими генераторами;

4 – випадкові – початковий (сеансовий) $K_{\text{п}}(K_c)$, або вихідний $K_в$, або робочий $K_р$, або сеансовий $K_{\text{с}}$, або пакетний $K_{пак.}$ ключі, які є випадковими з рівноймовірним розподілом. Ключ K_1 ($K_{1в}$, $K_{1р}$, $K_{1пак.}$, $K_{1\text{с}}$) є вихідними для формування ключа K_2 ($K_{2в}$, $K_{2р}$, $K_{2пак.}$, $K_{2\text{с}}$). Ключі K_1 і K_2 подаються на підалгоритм зашифрування ВД.

Елемент Γ_1 може бути виконаний програмно, апаратно або програмно-апаратно.

Властивості КВАНЕ-1:

1) управляємість елемента визначається залежністю вихідної інформації (вих. 4) від синхронності і синфазності інформації на входах 1, 2 – табл. 2;

2) випадковість елемента КВАНЕ-1 визначається його внутрішнім станом, видом інформації на входах 1, 2, послідовністю надходження цієї інформації на елемент і розподілом інформації між входами 1, 2 - табл. 2. Інформація на виході 4 являється випадковою (з рівноймовірним розподілом ключів), тобто на просторі ключів 2^n ключ зустрічається в випадковому місті цього простору тільки один раз з ймовірністю $P = 1 - \frac{1}{2^n} \approx 1$;

3) нелінійність елемента підтверджується нелінійною залежністю вихідної (вих. 4)

інформації від вхідної (вх. 1, 2);

4) незворотність визначення ключа і хеш-функції обумовлено структурою функціонала, за допомогою якої вона розраховується;

5) автоматичний розрахунок хеш-функції.

II. Постійний запам'ятовуючий пристрій, зокрема постійний запам'ятовуючий пристрій (ПЗП) мікроконтролера, в який для кожного абонента записується два стовпчики з табл. 1. Наприклад для абонента A_2 стовпчики A_i/A_j і A_2 - табл. 2.

III. Оперативний запам'ятовуючий пристрій (ОЗП) мікроконтролера.

IV. Перепрограмуємий запам'ятовуючий пристрій (ППЗП). В підалгоритмі формування ключів за допомогою ППЗП за рахунок зміни K_c змінюється структура підалгоритму формування ключів.

V. Елемент сума по модулю два перший, в якому здійснюється операція сума по модулю два $K_в(K_p, K_{пак.}) \oplus (K_п \oplus K_c)$.

Таблиця 2.

A_i/A_i	A_2
A_1	K_{12}
A_2	
A_3	K_{32}
...	...
A_i	K_{i2}

VI. Елемент сума по модулю два другий, в якому здійснюється побайтова операція сума по модулю два. З отриманого байта вибирається сім молодших розрядів для керування зсувом, що є ключем K_2.

VII. Елемент сума по модулю два третій здійснює операцію сума по модулю два $K_п \oplus K_c$.

Структурна схема підалгоритму зашифрування ВД (див. рис. 3) містить:

I. Вхідний буфер на 128 біт.

II. Елемент «Зсув вправо» (регістр зсуву на 128 розрядів), в якому здійснюється зсув на i-розрядів вправо в залежності від ключа K_2.

III. Суматор по модулю два на 128 біт, в якому здійснюється операція додавання два значення K_1 і інформації з виходу елемента «Зсув вправо».

IV. Вихідний буфер на 128 біт.

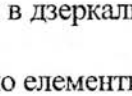
Структурна схема алгоритму криптографічного перетворення (криптосхема) при розшифруванні ЗД (див. рис. 5).

Структурна схема алгоритму складається з двох частин:

а) підалгоритму розшифрування ЗД;

б) підалгоритму формування ключів.

Структурна схема підалгоритму формування ключів містить (див. рис. 5) ті ж елементи, що і структурна схема підалгоритму формування ключів структурної схеми алгоритму криптографічного перетворення при за шифруванні ВД.

Структурна схема підалгоритму розшифрування ЗД (див. рис. 5) містить всі ті ж елементи, що і структурна схема підалгоритму за шифрування ВД, при цьому елементи «Сума по модулю два» і «Зсув вліво» включені в дзеркальному відображенні відносно підалгоритму зашифрування ВД, а також додатково введено елементи "Порівняння" -  і "Регістратор".

Спосіб зашифрування - розшифрування інформації з випадковим, відкритим і адаптивним ключем має три режими роботи: режим максимальної швидкодії; режим середньої швидкодії; режим мінімальної швидкодії.

Режим максимальної швидкодії.

Зашифрування (розшифрування) ВД (ЗД) в режимі максимальної швидкодії проводиться, коли $K_{\text{у}} = K_{\text{п}} \oplus K_c$.

Принцип роботи способу розглянемо на прикладі передачі інформації від абонента A_1 до абонента A_2, тобто абонент A_1 проводить зашифрування ВД (рис. 3), а A_2 - розшифрування ЗД (рис. 5).

I. Установка у вихідний стан елементів схеми криптографічного перетворення при за шифрування (розшифруванні) ВД (ЗД) при першому вмиканні.

На відкритому ключі встановлюється зв'язок $A_1 \leftrightarrow A_2$.

Якщо зв'язок установлений, то A_2 видає квитанцію A_1 про готовність до роботи. Абонент A_1 із табл. 3 відповідно до набраного номера телефону запам'ятовує відкритий номер абонента (наприклад 1582051 - 0002) і по цьому номеру з табл. 4 записують у програму закритий ключ $K_{\text{п}_{1,2}} = K_{\text{п}_{2,1}}$ (наприклад 111...10). Крім цього видає свій відкритий номер (0001) абонентові A_2. Абонент A_2 із табл. 5 відповідно до цього відкритого номера зчитує з ПЗП мікроконтролера в програму закритий ключ $K_{\text{п}_{2,1}} = K_{\text{п}_{1,2}}$ (наприклад 111...10).

Таблиця 3.

№ телефону	Відкритий номер абонента
4339077	0001
1582051	0002
.....	.....
4832051	4095
4852051	4096

Таблиця 4.

Відкритий номер абонента	Закритий ключ (16 байт)
0001	
0002	111...10
.....	.....
4095	011...00
4096	101...11

Таким чином, на A_1 і A_2 з ПЗП мікроконтролера на елемент $Г_1$ видається $K_{П_{1,2}} \oplus K_{c_{1,2}} = K_{П_{2,1}} \oplus K_{c_{2,1}}$, так як при першому включенні $K_{c_{1,2}} = K_{c_{2,1}} = 0$ то на вхід 1 паралельним кодом, а на вхід 2 послідовним кодом поступає $K_{П_{1,2}} = K_{П_{2,1}}$.

З виходу 4 елемента $Г_1$ знімається ключ $K_в = K_{1в}$, який подається на елемент сума по модулю два підалгоритму зашифрування ВД.

Таблиця 5.

Відкритий номер абонента	Закритий ключ (16 байт)
0001	111...10
0002	
.....	.....
4095	011...00
4096	101...11

Крім цього ключ $K_в$ використовується для формування другого вихідного ключа $K_{2в}$, який подається на елемент "Зсув вправо" підалгоритму зашифрування ВД (див. Рис. 3).

Аналогічно формуються ключі в підалгоритмі формування ключів в алгоритмі криптографічного перетворення при розшифруванні ЗД.

Таким чином, у абонентів A_1 і A_2 встановлюються вихідні ключі з рівно ймовірним розподілом ключів, які у вигляді гамма-шифру подаються на пвдалгортм зашифрування (розшифрування) ВД (ЗД).

II. Установка випадкового робочого ключа для криптографічного перетворення при зашифруванні ВД.

На A_1 (див. рис. 3) з генератора випадкових чисел надходить випадкова послідовність довжиною 128 біт послідовним кодом на:

а) вхідний буфер;

б) елемент $Г_1$ (вхід 2) підалгоритму формування ключів.

З виходу "Вхідного буфера" випадкова інформація подається паралельним кодом на елемент «Зсув вправо», на другий вхід якого, подається ключ $K_{2в_{12}}$. З виходу цього елемента інформація подається на елемент сума по модулю два (вхід 1), а на вхід 2 паралельним кодом ключ - $K_{1в_{1,2}}$. В цьому елементі здійснюється операція сума по модулю два. З виходу 3 цього елемента зашифрована випадкова інформація через «Вихідний буфер» подається на модем і після нього в лінію.

Крім цього, випадкова інформація з ГВЧ замість $K_у$, як і у випадку формування вихідного ключа, надходить послідовним кодом на вхід 2 елемента $Г_1$, а на вхід 1 продовжує надходити ключ $K_{П_{12}}$.

Формування робочих ключів здійснюється таким же чином, як і формування вихідних ключів (п. I).

Для цього з виходу 3 знімається паралельним кодом хеш-функція випадкової інформації, яка подається послідовним кодом на вхід 2 елемента $Г_1$ і проходить всі ті ж операції, як і випадкова інформація. З виходу 4 хеш-функція $ХФ_{вип.і.A_1}$ надходить на вхід "Вихідного буфера".

Ключ K_{2p} подається на елемент «Зсув вправо» підалгоритму зашифрування ВД (див. рис. 3).

Таким чином, підалгоритм формування ключів сформував випадкові, індивідуальні, адаптивні робочі ключі $K_{1p_{1,2}}$ і $K_{2p_{2,1}}$, які будуть використані для зашифрування (розшифрування) першого блока ВД (ЗД).

III. Установка випадкового робочого ключа для розшифрування ЗД в алгоритмі криптографічного перетворення при розшифруванні ЗД (див. рис. 5).

Аналогічно формуються робочі ключі підалгоритмом формування ключів алгоритму криптографічного перетворення при розшифруванні ЗД (див. рис. 5).

Зашифрована випадкова інформація з модему через "Вхідний буфер" надходить на вхід 1 елемента сума по модулю два, а на вхід 2 цього ж елемента подається паралельним кодом ключ $K_{1в_{21}}$.

З елемента сума по модулю два інформація паралельним кодом надходить на вхід елемента «Зсув вліво», а на вхід 2 цього ж елемента ключ $K_{2в_{21}}$.

Розшифрована інформація паралельним кодом знімається з виходу 3 елемента «Зсув вліво» і подається на "Вихідний буфер", з виходу якого надходить послідовним кодом на вхід 2 елемента $Г_1$ підалгоритму формування ключів і "Регістратор".

Принцип формування робочих ключів такий же, як у A_1: формуються випадкові робочі ключі $K_{1p_{21}} = K_{1p_{12}}$ і $K_{2p_{21}} = K_{2p_{12}}$ з рівноймовірним розподілом ключів, які будуть використані для розшифрування першого блока ЗД.

В силу того, що робочі ключі формувались автономно, виникає необхідність в перевірці їх рівенства. Для цього використовуються хеш-функції, що виробляються елементами $Г_1$ для абонентів A_1 і A_2, які зашифровуються наступним чином: з виходу 3 елементів $Г_1$ абонентів A_1 і A_2 знімаються і подаються на входи 2 елементів $Г_1$ і ними зашифровуються. Після зашифрування знімаються з виходу 4 елементів $Г_1$.

Від абонента A_2 зашифрована хеш-функція з виходу 4 елемента $Г_1$ подається на вхід 2 елемента порівняння [=].

Хеш-функція абонента A_1 зашифровується таким же чином, подається на "Вихідний буфер" абонента A_1, модем і в лінію. Із лінії хеш-функція надходить на модем, "Вхідний буфер" абонента A_2, з виходу якого надходить на вхід 1 елемента порівняння [=].

В елементі порівняння [=] здійснюється порівняння $ХФ_{вип.і.A_1}$ і $ХФ_{вип.і.A_2}$. Якщо:

а) $ХФ_{вип.і\ A_1} \neq ХФ_{вип.і\ A_2}$, то з A_2 видається квитанція для повторної установки ключів $K_{1p_{21}} = K_{1p_{12}}$ і $K_{2p_{21}} = K_{2p_{12}}$;

СПОСІБ ЗАШИФРУВАННЯ - РОЗШИФРУВАННЯ ІНФОРМАЦІЇ З ВИПАДКОВИМ, ВІДКРИТИМ І АДАПТИВНИМ КЛЮЧЕМ

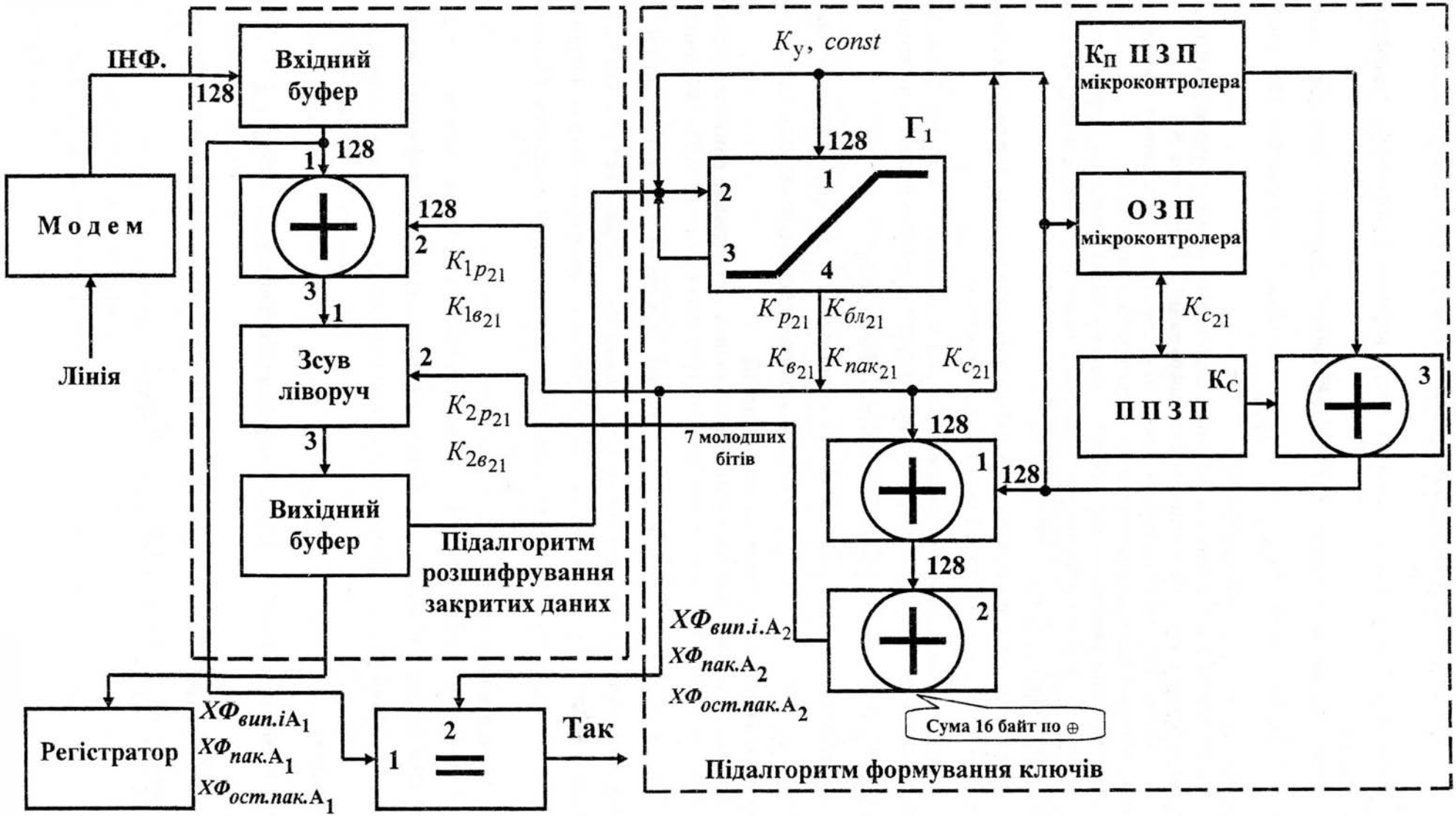


Рис. 5. Структурна схема алгоритму криптографічного перетворення при розшифруванні закритих даних

б) $ХФ_{вип.і\ A_1} = ХФ_{вип.і\ A_2}$, то з A_2 видається квитанція про те, що випадкові робочі ключі рівні, тобто $K_{1p_{21}} = K_{1p_{12}}$, $K_{2p_{21}} = K_{2p_{12}}$ і абоненти готові до обміну інформацією.

IV. Обмін інформацією між абонентами A_1 и A_2.

Обмін інформацією проводиться пакетами, які складаються з блоків по 128 біт.

Зашифрування, розшифрування блока ВД (ЗД) здійснюється таким же чином, як і зашифрування, розшифрування випадкової інформації при установці випадкових робочих ключів $K_{p_{21}} = K_{p_{12}}$. При цьому:

а) формуються нові випадкові робочі ключі $K'_{1p_{21}} = K'_{1p_{12}}$ і $K'_{2p_{21}} = K'_{2p_{12}}$, які адаптовані до інформації блока;

б) хеш-функція блока не використовується в алгоритмах криптографічного перетворення при зашифруванні блока ВД.

Наступний блок ВД зашифровується вже на нових випадкових, робочих ключах $K'_{1p_{21}} = K'_{1p_{12}}$ і $K'_{2p_{21}} = K'_{2p_{12}}$.

Таким же чином послідовно передаються всі блоки пакета. Наприкінці пакета здійснюється перевірка правильності передачі інформації по хеш-функції пакета абонентів ($ХФ_{пак.\ A_1}$ і $ХФ_{пак.\ A_2}$), якщо:

а) $ХФ_{пак.\ A_1} \neq ХФ_{пак.\ A_2}$, то з A_2 видається квитанція для повторної передачі пакета, при цьому знову встановлюються ключі $K'_{1p_{21}} = K'_{1p_{12}}$ і $K'_{2p_{21}} = K'_{2p_{12}}$;

б) $ХФ_{пак.A_1} = ХФ_{пак.A_2}$, то з A_2 видається квитанція про те, що пакет прийнято правильно і A_2 готовий до прийому наступного пакету.

По закінченні сеансу перевіряється правильність установки ключа сеансу $K_{1p_{21,\ ост.пак.}} = K_{1p_{12,\ ост.пак.}} = K_{c_{12}} = K_{c_{21}}$ по хеш-функції останнього пакета ($ХФ_{ост.пак.A_1}$ і $ХФ_{ост.пак.A_2}$). Якщо:

а) $ХФ_{ост.пак.A_1} \neq ХФ_{ост.пак.A_2}$, то з A_2 видається квитанція для повторної установки ключів $K_{1p_{21,\ ост.пак.}} = K_{1p_{12,\ ост.пак.}} = K_{c_{12}} = K_{c_{21}}$;

б) $ХФ_{ост.пак.A_1} = ХФ_{ост.пак.A_2}$, то приймається рішення, що ключі $K_{c_{12}} = K_{c_{21}}$. При цьому вони записуються в ПТЗП.

При наступному сеансі ключі $K_{c_{12}} = K_{c_{21}}$ використовуються сумісно $K_{п_{12}} = K_{п_{21}}$ з ключами $K_{п_{12}} = K_{п_{21}}$.

Режим середньої швидкодії.

Зашифрування (розшифрування) ВД (ЗД) у режимі середньої швидкодії проводиться, коли $K_y = K_{пак.}$.

Процес обробки інформації в режимі середньої швидкодії такий же, як і у режимі максимальної швидкодії.

Режим мінімальної швидкодії.

Зашифрування (розшифрування) ВД (ЗД) в режимі мінімальної швидкодії проводиться, коли $K_y = K_{бл}$.

Процес обробки інформації в режимі мінімальної швидкодії такий же, як і у режимі максимальної швидкодії.

При цьому способі ключі нікому не призначаються і не розподіляються. Ця обставина дозволяє додатково забезпечити надійний захист інформації і скоротити сили та засоби, які виділяються в інших системах для забезпечення конфіденційності.

Стислий криптоаналіз способу зашифрування - розшифрування інформації з випадковим, відкритим і адаптивним ключем.

Рівняння зашифрування:

$$\vec{b}_i = (\vec{a}_i \rightarrow \vec{И}_i) \oplus \vec{K}_{1i},$$

де:

$\vec{b}_i$ - вихідний вектор з 128 біт при i-му ключі;

$\vec{K}_i$ - i-й вектор ключа, який змінюється зі зміною кожного блока ВД (128 біт);

$\vec{И}_i$ - i-й вектор процедури зсуву в залежності від вектора i-го ключа (7 біт);

$\vec{a}_i$ - i-й вектор ВД (128 біт).

Рівняння розшифрування ЗД є оберненим процесом зашифрування ВД:

$$\vec{a}_i = (\vec{b}_i \oplus \vec{K}_{1i}) \leftarrow \vec{И}_i.$$

Призначення і характеристики способу:

1. Спосіб призначений для криптографічного перетворення інформації в мережі, захисту від атак вірусів і несанкціонованого доступу (хакерів) в комп'ютери через цю мережу.

2. Спосіб адаптивний відносно інформації, що передається і збоїв в будь-якому елементі системи.

3. Ключі, формуються випадковим чином, нікому не назначаються і не розподіляються, являються особистими, випадковими і адаптивними.

4. При реалізації способу забезпечується:
   - автоматичний контроль правильності обміну інформацією між абонентами;
   - високий ступінь криптографічного захисту інформації з еквівалентною довжиною ключа $K = 2^{2\times n} \times 2^n \times n$, де n - число розрядів в слові, що обробляється (блоці);
   - висока надійність передачі інформації;
   - потенційна швидкодія розробленого способу становить:
     а) при реалізації на персональній електронно-обчислювальній машині з параметрами: система Microsoft Windows XP Home Edition версія 2002; процесор: Intel (R) 4, частота 3,2 ГГц; об'єм ОЗП – 512 МБайт; частота системної шини – 800 МГц. – **800 МБіт/с**;
     б) при реалізації на програмуємих логічних інтегральних схемах – **2 ГБіт/с**.

Перспективи використання розробленого способу:

1. Телефонні мережі.
2. Факси.
3. Мобільні телефони.
4. Системи радіолокаційного розпізнавання як військових, так і цивільних об'єктів.
5. Супутникові системи зв'язку.
6. Системи охоронної сигналізації.
7. Системи супутникової охорони і спостереження за об'єктами.
8. Захист банківських рахунків і операцій в банкоматах.
9. Захист інформації на електронних носіях.
10. Захист глобальної мережі Інтернет.
11. Захист корпоративних мереж шляхом захисту вхідного потоку інформації.

Список літератури

1. Криптография и защита сетей: принципы и практик, 2-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.

Надійшла 30.03.2007 р.

УДК 519.688 **Ерохин В.Ф.**

СТРУКТУРНАЯ СХЕМА И МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОТОКОВОЙ ЭЛЕКТРОМАГНИТНОЙ СТЕГАНОСИСТЕМЫ

В работе [1] предложено следующее определение цифровой стеганографии: "… наука о незаметном и надежном скрытии одних битовых последовательностей в других, имеющих аналоговую природу." Такое определение позволяет расширить область правомерности понятия "цифровая стеганография" на случай, когда скрываемое сообщение встраивается в контейнер не внутри некоторого устройства, а непосредственно в канале связи, аддитивно. Область применения стеганографических методов, когда скрываемое сообщение (СС) встраивается в основное сообщение (ОС) без ограничения на его длину непосредственно в пространстве, назовем потоковой электромагнитной стеганографией.

Цель статьи – формализованное описание стеганографической системы, в которой контейнер представляет собой электромагнитное поле, являющееся цифровым радиосигналом, а физическое встраивание скрываемого сообщения происходит аддитивно, в пространстве.

Для компьютерной стеганографии характерно, что СС обычно встраивается в места расположения младших значащих битов ОС (изображения, аудио-видеофайла) или в биты, замена которых не приводит к заметному для человека изменению результата – например, в биты, определяющие градации синего цвета в изображении. Выбор стеганопути такого типа обусловлен, в частности, особенностями восприятия органов чувств человека [1, 2]. Относительно же электромагнитной стеганографии вопрос оказывается сложнее – мы непосредственно воспринимаем лишь видимое электромагнитное излучение. Поэтому в таком случае выбор стеганопути в первую очередь будет определяться возможностями аппаратуры анализа электромагнитного спектра и соответствующих демодуляторов, а уже потом – возможностями человеческого глаза (уха) обнаружить возможное изменение.

Очевидно одно – при аддитивном встраивании электромагнитного излучения (ЭМИ) СС в ЭМИ ОС необходимо будет позаботиться о том, чтобы напряженность поля в используемой полосе частот, создаваемая передатчиком ОС, на некоторую требуемую величину превышала напряженность поля, создаваемую в той же полосе передатчиком СС, и чтобы это превышение соблюдалось в любой точке пространства, в которой может находиться нарушитель. Такое превышение определяется рядом факторов: требованиями к энергетической и временной скрытности [3] передатчика СС, которая, в свою очередь определяется уровнем априорных знаний нарушителя о неинформационных параметрах несущего излучения СС, а также о прекодере и стеганокодере передающей части стеганосистемы.

Если мы имеем дело с длительно работающим передатчиком ОС, то можно говорить о потоковом электромагнитном контейнере (ПЭК). В общем виде структурная схема потоковой электромагнитной стеганосистемы (ПЭС) представлена на рис.1.

Передатчик маскирующего излучения (цифрового радиосигнала ОС) создает пустой ПЭК, параметры которого оцениваются (фильтруются) в блоке оценки параметров (БОП) пустого ПЭК на передающей стороне электромагнитного стеганоканала (ЭС) и в блоке оценки неинформационных параметров (БОНП) на приемной стороне ЭС. Особенностями