УДК 681.3.06:519.248.681

О. А. ЗАМУЛА, канд. техн. наук, Є. В. ПОПОВИЧ, Ю. І. ГОРБЕНКО

УМОВИ ТА МОЖЛИВОСТІ СТВОРЕННЯ БЕЗУМОВНО СТІЙКИХ КРИПТОСИСТЕМ

Вступ

На сьогодні використовуються, удосконалюються та розроблюються криптографічні системи (криптосистеми), які забезпечують різноманітний рівень криптостійкості. В ряді джерел [1-3] наведено умови створення криптосистем з різними рівнями стійкості. Проведений аналіз [1] показав, що, якщо в основу класифікації покласти рівень стійкості, то існуючі криптосистеми можна поділити на чотири класи:

1. Безумовно стійкі криптосистеми (БСК).
2. Розрахунково стійкі криптосистеми.
3. Доказуємо стійкі криптосистеми (імовірно стійкі).
4. Розрахунково нестійкі криптосистеми (тимчасової стійкості).

Умови та можливості реалізації таких криптосистем залежать від рівня розвитку математичних методів та систем криптоаналізу, тому створення умов і можливостей їх реалізації змінюються з часом. На сьогодні, на наш погляд, вже можна говорити та створювати криптосистеми та засоби, які забезпечують в різноманітних інформаційних технологіях вказані рівні стійкості. Особливо актуальними є задачі створення безумовно стійких криптосистем.

Метою статті є розгляд умов та можливостей створення на сучасному етапі розвитку безумовно стійких криптосистем.

1. Модель взаємодії користувачів

На рис. 1 наведена спрощена схема інформаційних співвідношень між двома абонентами А1 та А2.

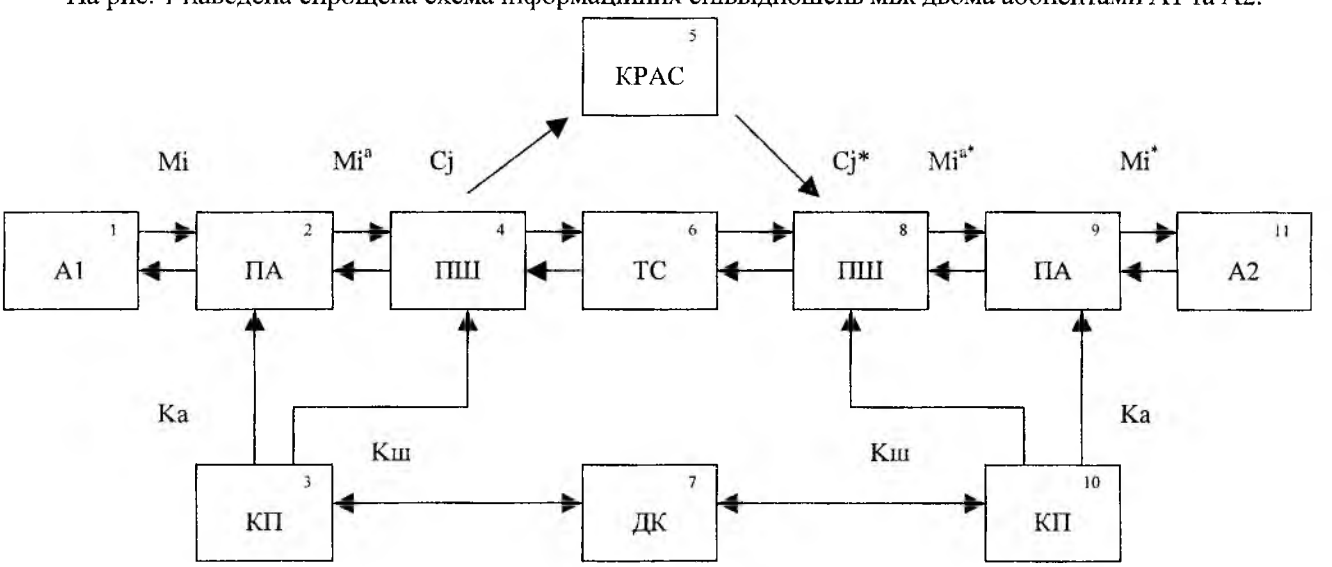

Рис. 1

На рис. 1 введені такі позначення: 2, 9 – пристрої автентифікації; 4, 8 – пристрої шифрування;3, 10 – ключові пристрої; 7 – джерело ключа; 5 – криптоаналітична система (криптоаналітик); 6 – комунікаційна система.

Будемо вважати, що А1 та А2 являють собою джерела інформації M_i з довільною потужністю алфавіту m та з відомою апріорною статистичною ймовірністю $P(M_i)$ для усіх повідомлень ($i = \overline{1, n_m}$) та ентропією джерела інформації $H(M_i)$. Аналогічно для А2 – m, $P(M_j)$ для усіх $j = \overline{1, n_m}$, *та* $H(M_j)$.

Оскільки повідомлення передається відкритою телекомунікаційною системою, то повинні бути забезпечені конфіденційність та автентичність відповідного рівня. Будемо вважати, що пристрій автентичності забезпечує надання користувачу послуг цілісності та справжності, а пристрій шифрування – послугу конфіденційності.

З метою забезпечення цих послуг використаємо криптоперетворення відповідних класів. Для реалізації криптоперетворень будемо використовувати ключі аутентіфікації K_a та ключі шифрування / розшифрування $K_ш$. Також будемо вважати, що ключі генеруються джерелом ключів та за слушними протоколами розповсюджуються абонентам А1 та А2.

Протидію системі здійснює криптоаналітична система (криптоаналітик). В подальшому будемо розглядати цю систему як зовнішню, так і внутрішню, наприклад, санкціонований користувач. Будемо вважати, що криптоаналітик перехоплює криптограми з необхідною йому імовірністю. Пристрій аутентифікації здійснює криптографічні перетворення за ключем K_a з метою забезпечення цілісності та достовірності повідомлення M_i. В подальшому будемо його подавати як M_i^a:

$$M_i^a=F_a(M_i,K_a,P_r), \tag{1}$$

де F_a – функція аутентіфікації; P_r – параметр перетворювання.

Пристрій шифрування здійснює зашифровування або розшифровування повідомлення M_i^a. Будемо вважати відомою статистику появи шифрограми $P(C_j)$ та статистику появи шифрограми M_i^a – $P(C_j/M_i^a)$ після їх зашифрування. При цьому:

$$C_j=F_з(M_i^a,K_з,P_r), \tag{2}$$

де $F_з$ – функція зашифрування.

Криптоаналітична система, що перехоплює криптограму C_j, має можливість розрахувати апостеріорну статистику $P(M_i^a/C_j)$ – ймовірність того, що C_j містить в собі M_i^a.

Абонент А2 приймає криптограму C_j^* – (знак "*" означає, що вона могла бути випадково або навмисно викривлена). Пристрій шифрування 8 здійснює розшифрування даної криптограми, при цьому M_i^{a*} утворюється як:

$$M_i^{a*}=F_p(C_j^*,K_p,P_r), \tag{3}$$

де F_p – функція розшифрування.

Пристрій аутентифікації здійснює криптоперетворення повідомлення M_i^{a*} з метою контролю цілісності та достовірності змісту повідомлення M_i^*. Якщо повідомлення M_i^* достовірне та цілісне, воно видається абоненту А2. При цьому на вхід А2 надходить повідомлення M_i^*, і, якщо $M_i^* = M_i$, то ми будемо вважати, що передача здійснена без порушення автентичності та цілісності, а якщо $M_i^* \neq M_i$, то порушена цілісність та автентичність при передачі повідомлення.

Будемо також вважати, що джерело ключів формує на своєму виході ключі K_i^a та $K_j^ш$ рівноймовірно, випадково та незалежно з ентропією джерела ключів $H(K^a)$ та $H(K^ш)$ з відповідними параметрами, і що інформаційна система здійснює періодичне передавання криптограм, і криптоаналітик їх перехоплює. Також будемо вважати, що на основі апріорної та апостеріорної статистики криптоаналітик розрахував $P(M_i/C_j)$ для $i = \overline{1, n_M}$ та $j = \overline{1, n_C}$. При цьому розмірність апостеріорного ряду

$$n_p = n_м \times n_c. \tag{4}$$

Якщо розмірність ряду, що визначена формулою (4) дуже велика, то практично побудувати або розрахувати ряд неможливо. В зв'язку з цим криптоаналітик повинен вести криптоаналіз з використанням апостеріорної ентропії H(M/C). При цьому апостеріорна ентропія розраховується згідно співвідношень:

$$H(M/C_j)=-\sum P(M_i/C_j)\ log_2P(M_i/C_j), \tag{5}$$

Та

$$H(M/C)=\sum_j P(C_j)H(M/C_j)=\sum_{j=1}^{n_c}\sum_{i=1}^{j n_m} P(C_j)\ P(M_i/C_j)\ log_2P(M_i/C_j). \tag{6}$$

До початку ведення криптоаналізу криптоаналітик має невизначенність (ентропію) відносно повідомлення:

$$H(M)=-\sum_i^{n_m} P(M_i)\ log_2P(M_i). \tag{7}$$

$H(M)$ – отримано при умові, що криптоаналітик знає апріорний ряд $P(M_i)$ – ймовірність появи повідомлення на виході джерела повідомлень. Після перехвату необхідної кількості криптограм невизначеність криптоаналітика відносно джерела повідомлень визначається за формулою (6).

2. Умови реалізації безумовно стійкої криптосистеми

Розглянемо умови реалізації безумовно стійкої криптосистеми, використовуючи модель, приведену на рис. 1.

Визначимо, перш за все, яку кількість інформації може отримати криптоаналітик. Умовна ентропія $H(M/C)$ характеризує невизначеність криптоаналітика після значної кількості отриманих криптограм, причому $H(M/C)$ характеризує середню невизначеність криптоаналітика відносно джерела повідомлень. Кількість інформації, яку він отримує про джерело повідомлень після проведення криптоаналізу, визначається формулою:

$$\Delta I=H(M)-H(M/C). \tag{8}$$

При умові, що криптоаналітик не отримує ніякої інформації про джерело повідомлень ($\Delta I=0$), маємо:

$$H(M)=H(M/C). \tag{9}$$

Умова (9) і є умовою реалізації безумовно стійкої криптосистеми. Причому, скільки б шифрограм не перехоплював криптоаналітик, він не збільшить своїх знань про джерело інформації. В цьому випадку криптоаналіз є безглуздим.

Коли криптоаналітик розкриває систему, тобто ($H(M/C)=0$), то $\Delta I=H(M)$. Це означає, що кількість інформації, яку він отримав, дорівнює ентропії джерела повідомлення Н(М). В більшості криптосистем:

$$0<H(M/C)<H(M). \tag{10}$$

Співвідношення, що наведено вище, торкається конфіденційності.

Наведемо теорему [1], яка визначає необхідні та достатні умови реалізації безумовно стійких криптосистем. При цьому зазначимо, що за сучасним поглядом співвідношення (9) є як необхідною, так і достатньою умовою, але воно не визначає практичних методів досягнення мети.

Теорема 1. Необхідною та достатньою умовою забезпечення безумовної стійкості у системі, схема якої наведена на рис. 1, є наступне:

$$P(C_j/M_i)=P(C_j), \tag{11}$$

тобто ймовірність появи криптограми не повинна залежати ні від того, яке повідомлення вибрано на виході джерела повідомлень, ні від того, який ключ з'явився на виході джерела ключів.

З (11) випливає, що в безумовно стійких криптосистемах (теоритично стійких системах) кожне повідомлення M_i повинно з однаковою ймовірністю відображатися в кожну криптограму. При цьому ми не накладали обмежень ні на потужність алфавіту повідомлення та ключа, ні на довжину повідомлень та криптограм.

Будемо вважати, що джерело повідомлень має алфавіт m_M, джерело криптограм – m_C, а довжина повідомлень та криптограм відповідно – l_M та l_C.

Доведення теореми 1. Для доведення теореми розглянемо апостеріорні ймовірності $P(M_i/C_i)$, уважаючи, що криптоаналітик перехвачує необхідну йому кількість криптограм. Тобто криптоаналіз відбувається в умовах вибору криптотексту (при відомому криптотексті). Використовуючи теорему Байєса, Р (M_i/C_i) може бути визначена як:

$$P(M_i/C_i)=\frac{P(M_i)P(C_i/M_i)}{P(C_j)}=\frac{P(M_i)P(K_{ij})}{\sum_{i=1}^{n_m}P(M_i)P(K_{ij})}. \tag{12}$$

Відповідно до розглянутого вище співвідношення (9) умовою безумовної стійкості є $H(M)=H(M/C)$. Стосовно до ймовірності появи повідомлення $P(M_i)$ та апостеріорної ймовірності $P(M_i/C_j)$ можливо записати, що в безумовно стійких системах ймовірність $P(M_i/C_j)$ під час криптоаналізу не повинна змінюватися відносно $P(M_i)$, тобто

$$P(M_i/C_j)=P(M_i). \tag{13}$$

Інакше, після криптоаналізу, криптоаналітик не отримує будь якої додаткової інформації і його апостеріорні знання не збільшуються відносно джерела інформації для $i=\overline{1,n_M}$ та $j=\overline{1,n_C}$. Розділимо ліву та праву частини співвідношення (12) на $P(M_i) \neq 0$. В результаті маємо:

$$\frac{P(M_i/C_i)}{P(M_i)}=\frac{P(C_j/M_i)}{P(C_j)}=1, \tag{14}$$

звідки $P(C_j/M_i) = P(C_j)$. Таким чином умова (11) є як необхідною, так і достатньою.

Таким чином в безумовно стійкій системі ймовірність появи криптограми на виході пристрою шифрування не повинна залежати ні від ймовірності появи повідомлень ні від ймовірності появи ключа. Крім того, кількість криптограм повинна бути не менша за кількість повідомлень M_i. Для однозначності дешифрування, це означає, що кількість ключів повинна бути не менш за кількість повідомлень. Тобто:

$$N_K \geq N_M. \tag{15}$$

З кута зору розглянутого вище інформаційного підходу це означає, що ентропія джерела ключа повинна бути більшою або рівною ентропії джерела повідомлень:

$$N(K) \geq N(M). \tag{16}$$

Для вихідних даних, наведених на рис. 1, кількість повідомлень N_M довжиною l_M при m_M алфавіті

$$N_M = m_M^{l_M}. \tag{17}$$

Для ключів з потужністю алфавіту m_K та довжиною l_M

$$N_K = m_K^{l_K}. \tag{18}$$

Якщо вважати, що всі повідомлення та ключі є равноіймовірні, маємо:

$$P(M_i)=\frac{1}{N_M}=m_M^{-l_M}, \tag{19}$$

$$P(K_j)=\frac{1}{N_K}=m_K^{-l_K}. \tag{20}$$

Після підстановки (19) та (20) в (16) отримаємо:

$$H(K)=-\sum_{i=1}^{n_K}P(K_j)\log_2 P(K_j)=\left(N_K\frac{1}{N_K}\log_2\frac{1}{N_K}\right)=\log_2 N_K=\log_2 m_K^{l_K}. \tag{21}$$

За аналогією –

$$H(M)=\log_2 m_M^{l_M}. \tag{22}$$

Після підстановки (21) та (22) в (16), отримаємо:

$$\log_2 m_K^{l_K} \geq \log_2 m_M^{l_M},$$

або

$$l_K \log_2 m_K \geq l_M \log_2 m_M$$

Якщо потужність алфавіту джерела повідомлень та джерела ключів однакова ($m_K=m_M$), а це майже завжди так, то:

$$l_K \geq l_M. \tag{23}$$

Інакше:

$$l_K=\frac{\log_2 m_M}{\log_2 m_K}l_M \tag{24}$$

3. Методи реалізації безумовно стійкої криптосистеми

Проведений аналіз показав, що висунутим вимогам (вибір ключів здійснюється рівноймовірно, випадково та незалежно, а також виконується умова (23)) задовольняє криптосистема відома під назвою «Система Вернама» [3]. В ній зашифрування здійснюється методом потокового криптографічного перетворення за правилом:

$$C_i=(M_i+K_i^1)mod\ m. \tag{25}$$

де m – потужність алфавіту C_i.

Принципова вимога до цього перетворення – це $l_{K_i} \geq l_{M_i}$. Розшифрування в такій системі здійснюється за правилом:

$$M_i=(C_i-K_i^P)mod\ m. \tag{26}$$

Безпосередній аналіз співвідношень (2.25) та (2.26) означає, що для розшифрування повідомлення M_i необхідно забезпечити синхронізацію K_i^3 та K_i^P.

Оцінимо стійкість такої системи проти різноманітних криптоаналітичних атак. Оскільки така система безумовно стійка, то при додержанні усіх вищезазначених вимог найкраща атака – це атака типу "брудна сила".

З метою оцінки складності реалізації такої атаки, можна використати показник безпечного часу системи

$$t_б = P_p \frac{N_K}{\gamma K}. \tag{27}$$

де P_p – ймовірність успішного рішення задачі; N_K – кількість ключів; γ – продуктивність аналітичної системи (кількість переборів за секунду); K – коефіцієнт перерахунку, який дорівнює 3.1×10^7 с/рік для отримання значення $t_б$ в роках.

При умові (23) кількість ключів визначається $N_K = m^{l_k}$, а $t_б$ визначається:

$$t_б = P_p \frac{m^{l_k}}{\gamma K}. \tag{28}$$

Для m=2 (двійковий алфавіт)

$$t_б = P_p \frac{2^{l_k}}{\gamma K}. \tag{29}$$

Для m=256=2^8

$$t_б = P_p \frac{256^{l_k}}{\gamma K}. \tag{30}$$

В табл. 1 наведено значення $t_б$ для безумовно стійкої криптосистеми, в якій зашифрування та розшифрування здійсняються згідно з правилами (25) та (26). Розрахунки виконано при P_p=1 та $\gamma=10^{12}$ операцій за сек.

Таблиця 1

Значення $t_б$ для безумовно стійкої системи

довжина *байт*	безпечний час системи $t_б$ *років*
8	$1,34*10^{-1}$
16	$4,17*10^{18}$
32	$2,59*10^{57}$
64	$6,35*10^{134}$
128	$1,63*10^{289}$
256	$5,74*10^{597}$
512	$3,7*10^{1214}$
1024	$7,47*10^{2447}$

Розрахуємо також відстань рівнозначності l_0 для безумовно стійкої криптосистеми.

Відомо, що [1]:

$$H(M/C)=H(K)-l_C r log_2 m, \tag{31}$$

де $H(K)$ – ентропія джерела ключів; l_C – довжина криптограми; r – збитковість мови; m – потужність алфавіту.

Враховуючи, що криптоаналіз можливий лише за умов $H(M/C) = 0$, з (31) отримаємо:

$$H(K)-l_0 r log_2 m=0, \tag{32}$$

де l_0 – відстань рівнозначності.

Звідки:

$$l_0 = \frac{H(K)}{r \log_2 m}. \quad (33)$$

Для безумовно стійкого шифру (правила (25), (26)):

$$H(K) = \log_2 N_k = \log_2 2^{l_K} = l_K. \quad (34)$$

Таким чином:

$$l_0 = \frac{l_K}{r \log_2 m}. \quad (35)$$

Оскільки, як правило, $r < 1$ (тобто будь яка мова має збитковість) то:

$$l_0 > l_K. \quad (36)$$

Із (36) випливає, що для розкриття шифрограми необхідно, щоб криптоаналітик отримав криптограму довжиною, більшою за довжину ключа.

Таким чином, для реалізації безумовно стійкої системи шифрування необхідно, щоб довжина ключа була не менш за довжину повідомлення і ключі в системі вибирались би джерелом ключів рівноймовірно, випадково та незалежно.

4. Проблемні питання реалізації та області застосування безумовно стійких криптосистем

Вище показано, що безумовна стійкість може бути досягнута при умові, що довжина ключа не менша довжини повідомлення, а ключі формуються випадково з рівномірним законом розподілу та є незалежними. Тому першою проблемою, складність якої стримує впровадження безумовно стійких криптосистем, є проблема генерування, розповсюдження, установки та використання ключів. Сутність її полягає у виконанні вимоги появлення символів "1" та "0", на різних довжинах ключів l_k ймовірності повинні бути близькими до 0,5. Навіть невеликі відхилення ймовірностей від 0,5 не дозволяють реалізувати безумовну стійкість. Далі, якщо необхідно забезпечити шифрування значних об'ємів інформації, то необхідно розповсюджувати великі об'єми ключів з великою захищеністю від можливою компрометації. При використанні ключів, з однієї сторони необхідно здійснити узгоджене їх використання, в змісті побітової синхронізації, а з другої – їх узгодженого знищення після використання.

Разом з тим, сучасні досягнення у галузі створення та використання носіїв інформації, які можуть бути використані в якості носіїв ключів, роблять можливим розповсюдження та використання ключів. Наприклад, навіть звичайна дискета може бути використана в якості носія ключів для сотень коротких повідомлень. Тому безумовно стійкі засоби криптографічного захисту інформації можуть бути реалізовані з використанням навіть звичайних персональних комп'ютерів. Це підтверджено на практиці, що буде розглянуто в подальшому.

Важливим є забезпечення також цілісності та автентичності ключів, які використовуються. Сутність цієї задачі полягає в тому, що ключі та їх носії повинні бути захищені від порушення цілісності та викривлення. Крім того, навіть в безумовно стійкій системі необхідно забезпечити потенціально досягаєму автентичність захисту інформації. На наш погляд ця проблема потребує окремого розгляду.

Щодо застосування безумовно стійких систем, то вони можуть бути використані для захисту конфіденційної інформації, різного призначення ключів, наприклад, головних ключів (ключів сертифікації та транспортних ключів). При цьому реалізація процедур зашифрування та розшифрування є простою (правила (25) та (26)) і може виконуватись з великою швидкістю.

Метою цієї статі є бажання авторів звернути увагу на можливість реалізації та застосування криптосистем, які забезпечують безумовну стійкість. Наведені в табл. 1 значення безпечного часу показують, що повідомлення з довжиною 32 байти і більше можуть бути захищені з великою стійкістю.

Список літератури: 1. *Шеннон К.* Теория связи в секретных системах. Работы по теории информации и кибернетике. М.: Изд. иностр. лит., 1963. С. 333-402. 2. *Диффи У., Хеллмэн М.Э.* Новые направления в криптографии // ТИИЭР. 1976. 22. С. 644-654. 3. *Брикелл Э.Ф., Одлижко Э.М.* Криптоанализ: обзор новейших результатов // ТИИЭР: Малый тематический выпуск. Защита информации. 1988. 76(5). С. 75-94.

Харківський державний технічний університет радіоелектроніки

Надійшла до редколегії 27.03.2001