МЕТОДЫ АУТЕНТИФИКАЦИИ: ПРОБЛЕМЫ И ПРИНЦИПЫ РЕАЛИЗАЦИИ

УДК 681.3.06:519.248.681

О. А. ЗАМУЛА, канд. техн. наук, Г. М. ГУЛАК, Є. В. ПОПОВИЧ

МЕТОДИ АВТЕНТИФІКАЦІЇ В БЕЗУМОВНО СТІЙКИХ КРИПТОСИСТЕМАХ

Вступ

Згідно встановлених на сьогодні норм та вимог нормативних документів системи захисту інформації повинні надавати користувачу послуги спостереженості, доступності (управління доступом) та цілісності. Теоретичною основою побудови систем та засобів надання вказаних послуг є загальна теорія автентичності (справжності). На сьогодні ця теорія одержала значний розвиток, особливо в практичній площині. Але, на наш погляд, вона потребує подальшого узагальнення, класифікації, пояснення нових задач та проблемних питань, визначення методів та способів їх розв'язання. Метою статті є розгляд та аналіз методів та проблемних питань забезпечення автентичності в різноманітних інформаційних технологіях, включаючи телекомунікаційні системи. В даній статті ми розглянемо загальні питання теорії автентифікації та здійснення автентифікації в безумовно стійких системах. Справа в тому, що на сьогодні в більшості інформаційних технологій більш гостро стоять питання цілісності, автентичності та доступності. Вважаємо за необхідне запропонувати для обговорення та можливого використання наступні поняття та визначення.

Цілісність інформації – це властивість інформації, яка полягає в тому, що вона не може бути змінена випадково або навмисно неавторизованим користувачем і/або процесом і може бути використана за призначенням.

Доступність – властивість ресурсу системи або комп'ютерної системи (автоматизованої системи), яка полягає в тому, що авторизований користувач і/або процес, який володіє відповідними повноваженнями, може використати ресурс згідно з правилами і з визначеною якістю, в тому числі за рахунок використання криптографічних перетворень.

Спостереженість – властивість ресурсу системи (комп'ютерної системи, об'єкта комп'ютерної системи, інформації), що дозволяє реєструвати роботу користувачів та процесів, використання ресурсу системи, однозначно установлювати ідентифікатори (імена) причетних до певних подій користувачів та процесів, а також реагувати на ці події з метою мінімізації можливих втрат в системі, у тому числі за рахунок використання криптографічних перетворень.

Аналіз показує, що для забезпечення автентичності необхідно розглядати всі об'єкти та суб'єкти, що мають інформаційні співвідношення. В якості основи для побудови системи захисту повинна бути вибрана модель взаємної недовіри і взаємного захисту. Схематично така модель подана на рис. 1.

В даній моделі, з точки зору інформаційних співвідношень, приймають участь джерело та приймач інформації, арбітр, криптоаналітик. Для такої моделі джерело інформації, приймач інформації та арбітр є сторонами, що не довіряють один одному та повинні бути захищені від обману. Автентичність, як показав аналіз, може досягатися за рахунок розв'язання наступних задач:

1. Встановлення справжності користувача, що намагається вступити в інформаційні співвідношення (доступ до інформації, що захищається до ресурсу системи і т.п.).

2. Автентифікація системи - процедура встановлення справжності мережі, системи, до якої отримано доступ.

3. Автентифікація програмного забезпечення та даних - процедура встановлення цілісності програмного забезпечення та даних, які протягом деякого часу могли знаходитись за межами контролю володаря, а також підтвердження їх справжності (авторства).

4. Автентифікація повідомлень - процедура перевірки цілісності повідомлень та підтвердження авторства.

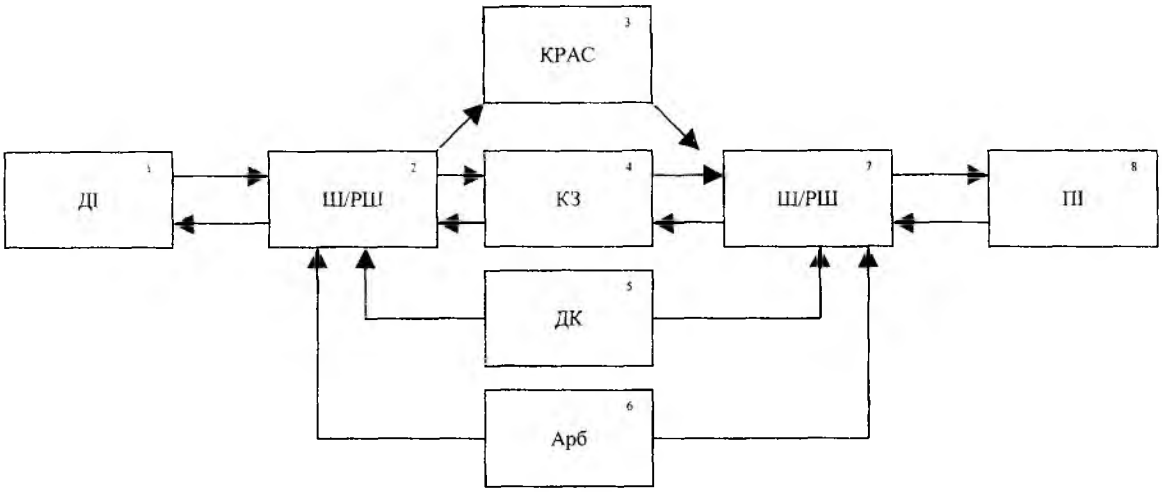

Рис. 1

Введені позначення:
1, 8 – джерело (приймач) інформації (ДІ, ПІ);
2, 7 – пристрої зашифрування/розшифрування (ЗШ/РШ);
3 – криптоаналітична система (КРАС);
4 – канал зв'язку та телекомунікаційна система, носій інформації;
5 – джерело ключа (ДК); 6 – арбітр (Арб);
8 – приймач (джерело) інформації.

2. Основні загрози порушення автентичності

Проведений аналіз показав, що в розглянутій моделі можуть бути реалізовано ряд загроз порушення автентичності [1-2].

Зі сторони об'єкта або суб'єкта А:

А1: абонент А формує повідомлення M_i та надсилає його абоненту В, а потім відмовляється від факту надсилання повідомлення M_i.

А2: абонент не формував і не передавав повідомлення M_i, але стверджує, що передавав.

А3: абонент А передав повідомлення M_j, а стверджує, що передав M_i.

А4: абонент передав повідомлення M_i у момент часу t_v, а стверджує, що передав повідомлення у $t_v \pm \Delta t$.

Під час реалізації загроз абонент А буде прагнути максимізувати обсяг втрати користувача В.

Зі сторони об'єкта або суб'єкта В:

В1: абонент В отримує від абонента А повідомлення M_i, а потім відмовляється від факту його отримання.

В2: абонент В отримує повідомлення M_i, а потім змінює його на M_i і стверджує, що отримав саме його.

В3: абонент А надсилає повідомлення у момент часу t_v, абонент В отримує це повідомлення у $t_v + \Delta t_1$, а стверджує, що отримав його у $t_v + \Delta t_2$.

В4: абонент В створює повідомлення M_i, а стверджує, що отримав його від абонента А.

Зі сторони арбітра:

АР1: арбітр може видати неправильне рішення відносно аналізу вищезазначених загроз Аі або Ві.

АР2: арбітр може прийняти неправильне рішення по відношенню до обох абонентів з метою збільшення свого виграшу.

АР3: арбітр приймає сторону зловмисника та компрометує систему (розголошує її)

КРАС1: імітація неправдивої криптограми з ймовірністю $P_i(C')$.

КРАС2: заміна істинної криптограми C неправдивою C' з ймовірністю $P_n(C')$.

КРАС3: повторна передача повідомлення, яке було передано раніше з ймовірністю $P_{pn}(C)$.

КРАС4: дезорганізація системи за рахунок передавання неправдивих команд управління.

КРАС5: модифікація повідомлення з ймовірністю $P_м(C)$.

У вірно спроектованій системі захисту, відповідно до політики безпеки, повинні бути перекриті основні загрози та мінімізовані втрати відповідно з вимогами до системи. Наприклад, під час вибору

стратегії подій криптоаналітик буде намагатися максимально збільшити ступінь втрат, тобто максимізувати ймовірність обману $P_{обм}$ [1]:

$$P_{обм}=max\{P_i,P_n,P_{рп},P_M,...\}, \quad (1)$$

де $P_i,P_n,P_{рп},P_M,...$ відповідні ймовірності, задані в наведеній вище моделі загроз. В якості загроз криптоаналітику необхідно вибирати одну або декілька, але таких, які мають найбільшу ймовірність успіху.

Покладемо, що на виході джерела повідомлень формується повідомлення M_i, де $i = \overline{l..n_M}$. Під час відображення повідомлення M_i, в криптограму C_i кількість станів джерела криптограм змінюється в межах $j = \overline{l..n_C}$. Якщо відомі розміри множини повідомлень n_M та множини криптограм n_C, то ймовірність обману в загальному випадку для моделі, що визначена на рисунку 1 $P_{обм}$, можна визначити як:

$$P_{обм} = \frac{n_M}{n_C}. \quad (2)$$

Аналіз співвідношення (2) показує, що:

1. Неможливо досягнути ймовірності $P_{обм}= 0$ тому, що для цього потрібно, щоб $n_C \to \infty$, а $n_M \to 0$.
2. З метою зменшення ймовірності $P_{обм}$ необхідно, щоб $n_M << n_C$.
3. Множина станів джерела криптограм може бути збільшена за рахунок внесення надлишковості, перш за все за допомогою збільшення довжини криптограм ($l_C >> l_M$), і, як наслідок, за рахунок збільшення кількості можливих криптограм.
4. Якщо $n_C = n_M$, то $P_{обм}= 1$.

3. Основні положення теорії автентичності Сімонсона

Аналіз джерел [1-3] показав, що на нинішній час з використанням інформаційного підходу розроблена тільки теорія оцінок ймовірності обману, яка одержала назву теорії Сімонсона [2].

В моделі, що розглядає Сімонсон, існує три учасника інформаційних співвідношень - джерело, одержувач та криптоаналітик. Водночас вважалося, що з метою автентифікації використовується, як і в схемі Шеннона, одноразовий ключ, а криптоаналітик знаходиться між джерелом та одержувачем (рис. 2).

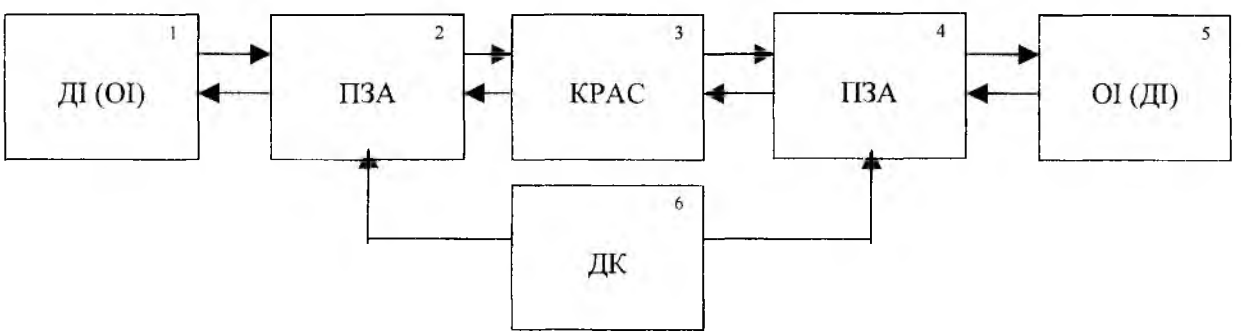

Рис. 2

Введені позначення:
1 – джерело інформації;
2, 4 – пристрої забезпечення автентифікації (ПЗА);
3 - криптоаналітична система (КРАС);
5 - одержувач (джерело) інформації; 6 - джерело ключів.

Сімонсон показав, що ймовірність обману в сенсі імітації P_i можна визначити, як [2]:

$$log_2 P_{обм} \geq -I(C,K), \quad (3)$$

де $I(C,K)$ - надлишковість (інформація), що вводиться з метою рішення задачі автентіфікації, наприклад ключа автентіфікації K_a.

В цьому випадку ключ автентифікації використовується з метою рішення завдання автентифікації, а ключ шифрування - для забезпечення конфіденційності. Тобто з теорії Сімонсона витікає, що з

метою забезпечення послуги конфіденційності повинен використовуватись ключ шифрування $K_ш$, а з метою забезпечення послуги автентифікації (цілісності та справжності) повинен використовуватися ключ автентифікації K_a.

Якщо $I(C,K)$ – взаємна інформація між джерелом криптограм та ключів, то [1, 2]

$$I(C,K)=H(C)-H(C/K). \tag{4}$$

$$H(C)=\sum_{i=1}^{n_C} P(C_i)\log P(C_i). \tag{5}$$

Розв'язуючи (3) отримаємо, що

$$P_{обм} \geq 2^{-I(C,K)}. \tag{6}$$

У випадку m - ічного алфавіту

$$P_{обм} \geq m^{-I(C,K)}. \tag{7}$$

Співвідношення (6) та (7) дозволяють отримати нижню оцінку для ймовірності обману, але наскільки реальна ймовірність буде близькою до неї, визначити неможливо. Сімонсон визначив ідеальну систему автентифікації, як криптографічну систему, в якій досягнута нижня межа ймовірності обману, тобто

$$P_{обм} = m^{-I(C,K)}. \tag{9}$$

Для випадку, коли в якості $I(C,K)$ можлива надлишковість, яка вводиться з метою забезпечення автентифікації у вигляді ключа автентифікації K_a довжиною $l_н$ коду автентіфікації повідомлень (КАП) та покласти

$$I(C,K) = l_н. \tag{10}$$

де індекс $н$ означає надлишковість. Тоді співвідношення (10) приймає вигляд:

$$P_{обм} \geq 2^{-l_н}. \tag{11}$$

З даного співвідношення випливає, що з метою зменшення ймовірності обману необхідно збільшувати надлишковість.

4. Аналіз методів забезпечення автентичності в безумовно стійких криптосистемах

Розглянемо загальні умови та методи забезпечення автентичності в безумовно стійких криптосистемах. Для них є вірними наступні ствердження про умови та стійкість в сенсі автентичності, яка може бути досягнена:

Ствердження 1. Нехай в системі Вернама здійснюється зашифрування інформації за правилом $C_i=(M_i+K_i) mod\ m$, а розшифрування – за правилом $M_i=(C_i-K_i) mod\ m$, тобто реалізується поточний метод шифрування. Тоді застосування поточного шифру Вернама [2] є необхідною, але недостатньою умовою забезпечення автентичності. Розглянемо простий випадок, коли $m=2$. В цьому випадку $C_i=(M_i \oplus K_i)$. Нехай в системі присутній криптоаналітик (відповідно до рисунку 2) та який перетворює C_i шляхом складання її з випадковою або спеціальною послідовністю символів R_i. Тоді на виході криптоаналітичної системи криптограма має вигляд:

$$C_i' = C_i \oplus R_i = M_i \oplus K_i \oplus R_i. \tag{11}$$

Одержувач здійснює розшифрування за правилом:

$$M_i' = C_i' \oplus K_i = M_i \oplus K_i \oplus R_i \oplus K_i = M_i \oplus R_i. \tag{12}$$

Аналіз (12) показує, що, якщо $R_i \neq 0$, то $M_i' \neq M_i$. За результатами криптоаналітичної атаки M_i відтворилося в M_i', де M_i (залежно від R_i) може бути як випадковим, так і повідомленням, яке має певний зміст та дозволене в даній системі, наприклад, «ТАК» може бути змінено на «НІ». Таким чином, в класичній системі Вернама завжди існує можливість заміни змісту повідомлень, тобто порушення автентичності.

Для довільної потужності алфавіту m:

$$C_i' = (C_i+R_i) mod\ m = (M_i+K_i+R_i) mod\ m, \tag{13}$$

а при розшифруванні:

$$M_i^{'}=(C_i^{'}-K_i)mod\ m=(M_i+K_i+R_i-K_i)mod\ m=(M_i+R_i)mod\ m. \quad (14)$$

Таким чином, для довільної потужності алфавіту в поточній системі Вернама застосування поточного шифрування є необхідною, але недостатньою умовою забезпечення автентичності. Твердження 1 доведено.

Розглянемо приклад, який підтверджує висновок загальної теорії Сімонсона про те, що з метою забезпечення автентичності необхідно внесення до криптограми надлишковості, а в класичній системі Вернама надлишковість відсутня.

Покладемо, що в системі Вернама, з метою виявлення втручань криптоаналітика, застосовуються групові лінійні коди, тобто використовується попереднє кодування інформації. Для цього випадку справедливе ствердження 2.

Ствердження 2. Якщо в системі Вернама повідомлення створюється за результатами кодування блоків M_{ij}, де j - кодова комбінація систематичного коду (групового коду визначення помилок), які створюються з повідомлення M_i додаванням $M_{ij}^{надл}$:

$$M_j = M_{ij} \mid M_{ij}^{надл}, \quad (15)$$

тобто перетворюємо повідомлення M_i з довжиною l_m в повідомлення M_j з довжиною $l_m + l_{надл}$:

$$M_i^{l_m} \Rightarrow M_i^{l_m} l_m^{надл} = M_j, \quad (16)$$

де $j = \overline{1, l_m + l_{надл}}$, тоді застосування системи Вернама є необхідною але недостатньою умовою аутентифікації.

Доказ.

Дійсно, нехай джерело повідомлень після здійснення групового системного кодування здійснює зашифрування відповідно з правилом:

$$C_j=(M_j+K_j)mod\ m \quad j = \overline{1, l_m + l_{надл}}. \quad (17)$$

За аналогією з (13) виконаємо перетворення C_j та отримаємо $C_j^{'}$:

$$C_j^{'} = (C_j+R_j)mod\ m = (M_j+K_j+R_j)mod\ m. \quad (18)$$

Після розшифрування отримаємо:

$$M_j^{'} = (C_j^{'}-K_j)mod\ m = (M_j+K_j+R_j-K_j)mod\ m = (M_j+R_j)mod\ m. \quad (19)$$

Якщо R_j випадкова або псевдовипадкова послідовність, то значення (19) буде послідовністю змінених кодових комбінацій, оскільки приймач не знає R_j послідовності, і декодер не зможе виправити помилки, і M_j+R_j буде являти собою повідомлення, яке не можливо прочитати (декодувати).

У цьому випадку декодер визначить помилки, а система може автоматично відмовитись від викривленого повідомлення яке нав'язується.

Таким чином, застосування групового систематичного коду є необхідною та достатньою умовою, коли R_j випадкова або псевдовипадкова.

В випадку, коли криптоаналітик формує R_j у вигляді послідовності комбінацій цього ж групового систематичного коду, причому йому відомі початок та кінець комбінацій коду, співвідношення (18) буде мати вигляд:

$$C_j^{'} = (C_j+R_j^k)mod\ m = (M_j+K_j+R_j^k)mod\ m = ((M_j+K_j)+R_j^k)mod\ m. \quad (20)$$

У випадку, коли R_j^k є послідовністю комбінацій групового систематичного коду, то враховуючи його замкнутість, $M_j+R_j^k$ являє собою кодову комбінацію з цього коду M_j^{ξ}, і тоді співвідношення (20) має вигляд:

$$C_j^{'}=(M_j^{\xi}+K_j)mod\ m. \quad (21)$$

На прийомному боці, відповідно до (19), розрахуємо $M_j^{'}$

$$M_j^{'} = (M_j^{\xi}+K_j-K_j)mod\ m = M_j^{\xi}. \quad (22)$$

Оскільки M_j^{ξ} є послідовністю комбінацій групового систематичного коду, то під час декодування факт модифікації повідомлення не буде визначений, і таким чином ствердження 2 підтверджується.

Розглянемо ствердження 3, в якому доводяться необхідні та достатні умови забезпечення автентичності та визначення навмисного впливу криптоаналітика.

Ствердження 3. Нехай в системі Вернама використовується поточне шифрування, тоді необхідними та достатніми умовами забезпечення аутентичності є:

1. Використання поточного шифрування.
2. Використання групового коду з визначенням помилок.
3. Формування ключової послідовності з використанням нелінійних алгоритмів перетворення відкритої інформації та криптограми.

Дійсно, нехай як і раніше

$$C_j = (M_j + K_j) mod\ m, \tag{23}$$

де M_j - послідовність комбінацій групового коду. На відміну від (23)

$$C_j = (M_j + K_j^{'}) mod\ m, \tag{24}$$

де:
$$K_j^{'} = \Psi[K_j, M_{j-\nu} \cup (\cap) C_{j-\nu}]. \tag{25}$$

Нехай функція Ψ в даному випадку реалізується схемою наведеною, на рис. 3.

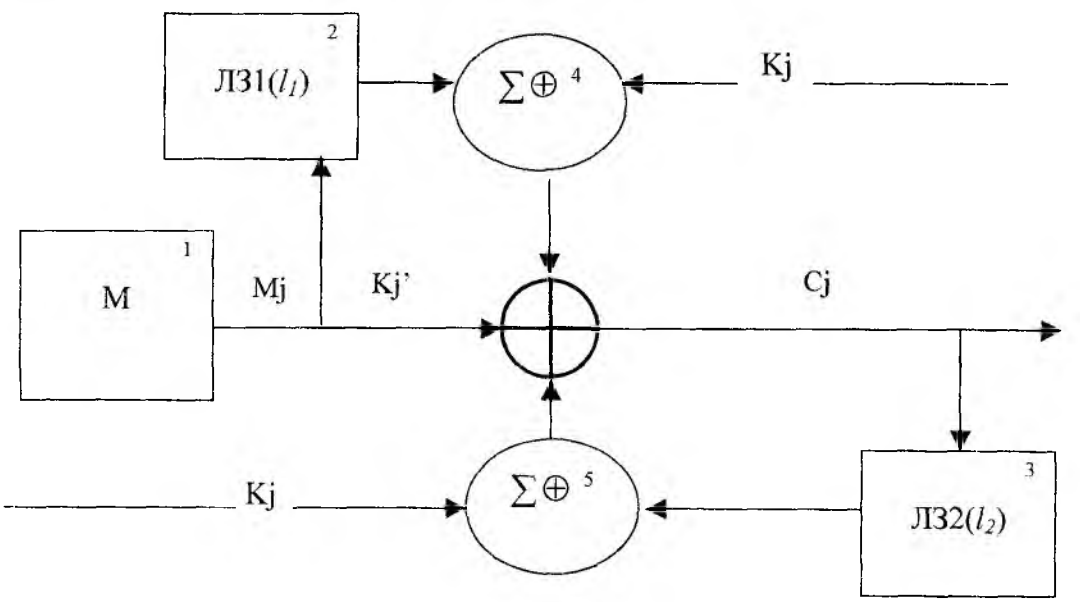

Рис. 3

Введені позначення: l_1 l_2 – довжина ліній затримки ЛЗ1 та ЛЗ2 відповідно;
$\sum\oplus$ - суматор за модулем два.

У вигляді співвідношення цю схему можна описати таким чином

$$K_j^{'} = \Psi[\ldots] = K_j \oplus \sum_{i=1}^{l_1} \oplus M_{j-i} \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i}. \tag{25}$$

Враховуючи співвідношення (25), маємо:

$$C_j = M_j \oplus K_j \oplus \sum_{i=1}^{l_1} \oplus M_{j-i} \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i},\ j = \overline{1, l_M}. \tag{26}$$

Нехай криптоаналітик, як і раніше здійснює криптоперетворення C_j криптограми

$$C_j^{'} = \varphi(C_j, R_j). \tag{27}$$

Тобто

$$C_j' = \varphi(C_j, R_j) = C_j \oplus R_j = M_j \oplus K_j \oplus \sum_{i=1}^{l_1} \oplus M_{j-i} \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i} \oplus R_j. \quad (28)$$

На прийомному боці реалізована наступна схема розшифрування (рис. 4).

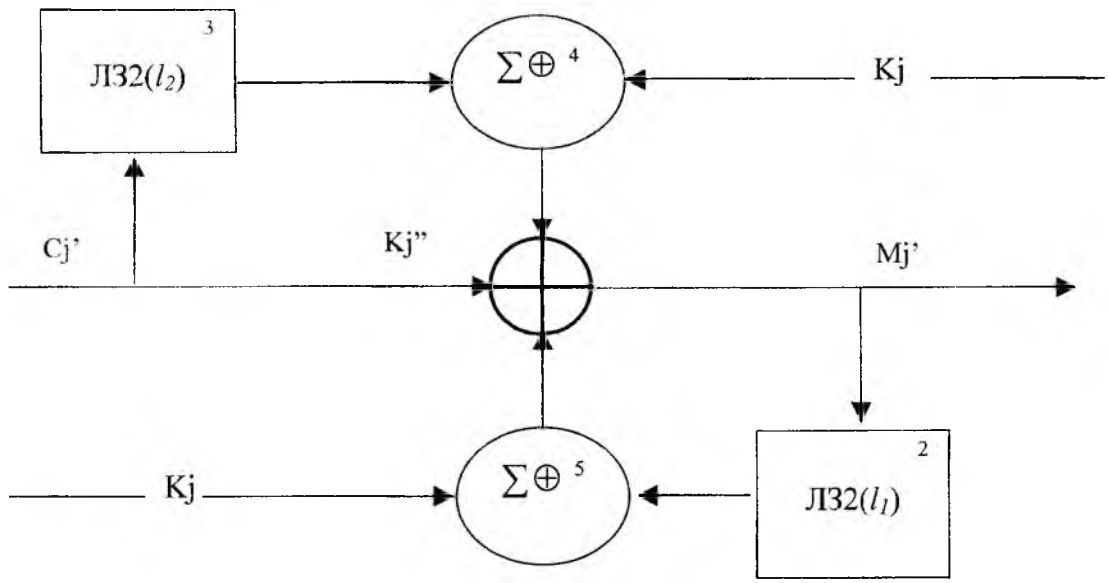

Рис. 4

У вигляді співвідношення цю схему можна описати наступним чином

$$M_j' = C_j' \oplus K_j''. \quad (29)$$

$$K_j'' = K_j \oplus \sum_{i=1}^{l_1} \oplus M_{j-i}' \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i}'. \quad (30)$$

Підставимо співвідношення 28 та 30 у співвідношення (29)

$$M_j' = M_j \oplus \underline{K_j} \oplus \sum_{i=1}^{l_1} \oplus M_{j-i} \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i} \oplus R_j \oplus$$

$$\oplus \underline{K_j} \oplus \sum_{i=1}^{l_1} \oplus M_{j-i}' \cup (\cap) \oplus \sum_{i=1}^{l_2} \oplus C_{j-i}' =$$

$$= M_j \oplus R_j \oplus (\sum_{i=1}^{l_1} \oplus M_{j-i} \oplus \sum_{i=1}^{l_1} \oplus M_{j-i}') \cup (\cap) \oplus (\sum_{i=1}^{l_2} \oplus C_{j-i} \oplus \sum_{i=1}^{l_2} \oplus C_{j-i}'). \quad (31)$$

Ми отримали співвідношення для розшифрування відповідно до схеми, зображеної на рис. 4. Спочатку для аналізу візьмемо лише частину із зворотним зв'язком за криптограмою.

$$M_j' = M_j \oplus (\sum_{i=1}^{l_2} \oplus C_{j-i} \oplus \sum_{i=1}^{l_2} \oplus C_{j-i}') \oplus R_j. \quad (32)$$

Аналіз співвідношення 32 показує, що у випадку, коли $R_j = 0$ (тобто R_j – відсутнє), а C_j' не містить помилок, тоді:

$$M_j' = M_j. \quad (33)$$

Іншими словами, реалізована безпомилкова передача. У випадку коли $R_j = 0$ (R_j – відсутнє), а C_j' містить помилки, тоді:

$$\sum_{i=1}^{l_2} \oplus C_{j-i} \oplus \sum_{i=1}^{l_2} \oplus C'_{j-i} \neq 0, \tag{34}$$

$$M'_j \neq M_j, \tag{35}$$

та декодер групового коду визначить помилку.

Таким чином, система визначає помилки природного походження. У випадку, коли $R_j \neq 0$, сума:

$$(\sum_{i=1}^{l_2} \oplus C_{j-i} \oplus \sum_{i=1}^{l_2} \oplus C'_{j-i}) \oplus R_j \neq 0, \tag{36}$$

незалежно від наявності помилки в каналі зв'язку. Якщо R_j випадкове, то схема працює, як і раніше, та визначає помилки, і декодер автоматично може відмовитись від повідомлення. Якщо R_j - груповий код, то він створить помилки в ключі K_j''. Тобто будь-який символ R_j викривить хоча б один символ криптограми C_j, та цей символ затримується в лінії затримки l_2 разів та в середньому скривдить $l_2/2$ символів, що призведе до появи пакету помилок, які визначать груповий код з визначенням помилок. Очевидно, що підібрати R_j криптоаналітик не може у зв'язку з тим, що він не знає ключа та повідомлення.

Розглянемо випадок, коли використовується лише зворотній зв'язок за повідомленням.

$$M_j' = M_j \oplus (\sum_{i=1}^{l_1} \oplus M_{j-i} \oplus \sum_{i=1}^{l_1} \oplus M'_{j-i}) \oplus R_j. \tag{37}$$

В цьому випадку криптоаналітик також не знає повідомлення та не в змозі підібрати відповідне R_j, тоді:

$$\oplus (\sum_{i=1}^{l_1} \oplus M_{j-i} \oplus \sum_{i=1}^{l_1} \oplus M'_{j-i}) \oplus R_j \neq 0. \tag{39}$$

Таким чином, ствердження 3 доведене.

Висновок

Основним засобом забезпечення послуг цілісності, доступності та спостереженності є застосування методів автентифікації. Методи автентифікації можуть застосовуватись для встановлення справжності користувача, системи, повідомлень, програмного забезпечення.

На сьогоднішній день немає навіть прикладної теорії автентифікації. Застосування елементів теорії Сімонсона дозволяє одержати граничні оцінки ймовірностей обману, які може досягти зловмисник.

Основним методом забезпечення автентичності є внесення в повідомлення надлишковості, яка може формуватись у вигляді контрольних сум, збиткових символів кодів, які визначають помилки, криптографічних контрольних сум (кодів автентифікації, імітовкладок) та хеш-функцій, а також цифрових підписів.

В потокових системах цілісність повідомлень може забезпечуватись за рахунок модифікації ключової послідовності (в безумовно стійких системах) або потокових гам (в обчислювально стійких системах) з використанням символів повідомлень та криптограм.

Список літератури: 1. *Boca Raton.* Authentication codes that parmit arbitration presented at the 18-th Southeastern conf., on Combinatories, Grapt Theory Computing, 1987. Feb. 23-27. 2. *Г.Дж. Симмонс.* Обзор методов аутентификации информации // ТИИЭР. 1988. 76 (5). С.105-125 (Малый тематический выпуск. Защита информации). 3. *Neuman B.C., Ts'o T.* Kerberos: An Authentication Service for Computer Networks//IEEE Comm. Magazine. 1994. Vol. 32. № 9. P. 33-38.

Харківський державний технічний університет радіоелектроніки

Надійшла до редколегії 29.03.2001