Выводы. По результатам анализа и обработки данных артикуляционных испытаний предложена описательная модель процесса возникновения ошибок аудитора при распознавании им искаженных маскирующей помехой слов артикуляционных таблиц. Модель позволяет на качественном уровне интерпретировать особенности и характеристики ошибок аудитора, объяснить форму закона распределения погрешностей оценок разборчивости и в ряде случаев может быть использована для построения аппроксимативной математической модели этого распределения.

ЛИТЕРАТУРА

1. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации / С.В. Дворянкин, Ю.К. Макаров, А.А. Хорев // Защита информации. Инсайд. – М.: 2007. - №2. – С.39-45.
2. Архипова О.О., Журавльов В.М., Кумейко В.М. Артикуляційні таблиці слів української мови / О.О. Архипова, В.М. Журавльов, В.М. Кумейко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2009. – № 2/19. – С. 13-17.
3. Архипова О.О., Журавльов В.М., Доровських А.В. Таблиці слів української мови для артикуляційних випробувань розбірливості інформації, що передається трактами зв'язку / О.О. Архипова, В.М. Журавльов, А.В. Доровських // Зв'язок. – К., 2010. – № 1 (89). – С. 9-11.
4. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки / А.А. Хорев // Специальная техника. – М.: 2009.– № 4. – С. 49– 63.
5. Архипов О.Є., Архипова С.А. Модель ошибок экспертных оценок / О.Є. Архипов, С.А. Архипова // "Сучасні проблеми управління", Матеріали IV Міжнародної наук.-практичної конференції (28-30 листопада 2007р., м.Київ). – ІВЦ Видавництво "Політехніка"– К.: 2007. – С. 65-66.
6. Мудров В.И., Кушко В.Л. Методы обработки ошибок измерений / В.И. Мудров, В.Л. Кушко – М., Советское радио, 1976. – 192 с.
7. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и её инженерные приложения / Е.С. Вентцель, Л.А. Овчаров – М.: Наука, 1988. – 480 с.
8. Пугачев В.С. Теория вероятностей и математическая статистика / В.С. Пугачев – М.: Наука, 1979. – 496 с.
9. Градштейн И.С., Рыжик И.М. Таблицы интегралов, сумм, рядов и произведений / И.С. Градштейн, И.М. Рыжик – М.: ГИФМЛ, 1971. – с.
10. Архипов А.Е. О моделировании некоторых типов случайных последовательностей / А.Е. Архипов // Вестник Киев. политехн. ин-та – Вып. 12. – К.:1988 – С. 39-44.

Надійшла: 14.11.2012 р.

Рецензент: д.т.н., професор Кваснiков В.П.

УДК 004.056.2

Василенко В.С., Дубчак О.В., Василенко М.Ю.

МАТРИЧНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ В ЗАДАЧАХ ЗАХИСТУ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

У статті запропоновано використання одного із видів матричних криптографічних перетворень на базі коду умовних лишків у задачах захисту цілісності інформації, що дозволяє одночасно з контролем і відновленням цілісності інформаційних об‘єктів забезпечити високий рівень їх імітостійкості.

Ключові слова: конфіденційність, цілісність інформації, криптографічні перетворення, імітостійкість.

Вступ. Система технічного захисту інформації (ТЗІ) забезпечує у разі збереження, передавання або оброблення інформації її цілісність достовірною, повною і захищеною від ненавмисних і навмисних спотворень. Одним з основних способів забезпечення цілісності інформації в автоматизованих системах є застосування засобів контролю цілісності програмних засобів та оброблюваної інформації, включаючи в деяких випадках і її відновлення.

Не зупиняючись на причинах порушення цілісності [1], слід підкреслити, що частина загроз цілісності, зокрема з боку авторизованих користувачів і випадкового впливу природних і технічних факторів, може бути виявленою, а, отже, і усуненою лише за рахунок застосування ефективних механізмів контролю і відновлення цілісності, в яких використовуються процедури захищених від підробок перетворень інформації. Це пов’язане з тим, що основним завданням засобів контролю цілісності інформаційних ресурсів є

забезпечення такого стану системи, коли неможливо приховування факту будь-якої несанкціонованої модифікації захищеної інформації (вставки, вилучення, підміна і т.п.). З цією метою до складу інформації, яка захищається, включають надлишкову інформацію - образ, відображення цієї інформації, процедура формування якого відома лише власнику інформації та авторизованим користувачам. Тобто образи, які формуються, повинні мати певну стійкість до підробок – імітостійкість. До механізмів контролю цілісності відносяться відомі механізми захисту [1] з використанням:

1. Сигнатур важливих об’єктів (у тому числі хеш-функцій);
2. Цифрового підпису;
3. Процедур завадостійкого кодування при забезпеченні цілісності архівної інформації, у тому числі й резервних копій програмних засобів і баз даних.

При цьому відомі механізми захисту з використанням сигнатур або цифрових підписів важливих об’єктів базуються на застосуванні процедур виявлення порушень цілісності і на наступному відновленні спотвореної інформації за рахунок повторної передачі неспотвореної інформації або повторного записування неспотвореної інформації з резервної копії. Обидві ці операції вимагають значних витрат часу.

З викладеного можна зробити висновок про те, що підвищення оперативності процесів забезпечення цілісності можливо за рахунок розробки і застосування узгоджених між собою швидкодіючих процедур як виявлення порушення цілісності інформації, так і її відновлення. Такими процедурами є процедури, які ґрунтуються на застосуванні корегуючих завадостійких кодів. Однак відомі завадостійкі коди не здатні забезпечити головну з необхідних при цьому властивостей - імітостійкість, внаслідок чого їх використання в механізмах контролю цілісності унеможливлено.

Це пов’язано з тим, що механізми формування контрольних ознак, які можна було б використовувати в якості відповідних образів (сигнатур, хеш-функцій і т.п.) не забезпечують прихованості їх формування, оскільки константи цих кодів (елементи кодувальних таблиць, див. нижче) є, як правило, загальновідомими. В окремих випадках, коли таку прихованість можна було б забезпечити (приклад - коди Ріда-Соломона), кількість елементів перетворення (підматриць кодувальної матриці) є обмеженим настільки, що важко говорити про необхідну імітостійкість відповідних контрольних ознак.

У статті пропонується використання завадостійкого коду, який є придатним як для контролю, так і для відновлення цілісності інформаційних об’єктів і по сукупності своїх властивостей, на думку авторів, перевершує відомі. Цей код легко вписується у стандартні процедури на базі матричних кодових перетворень.

Короткі відомості про матричні кодові перетворення. Під матричними кодовими перетвореннями будемо розуміти процедуру множення вихідного коду A довжиною в m символів (слова певного алфавіту, числа у деякій системі числення і т.п.), розглянутого як матриця розмірності $(1\times m)$, де m - число символів цього вихідного коду, на кодувальну матрицю G розмірності $(m\times m)$, елементами якої є деякі числа або підматриці. Найбільш загальні вимоги до побудови кодувальних матриць розглянуто нижче. Операції множення і додавання при обчисленні елементів закодованого слова (при множенні матриць) можуть бути або звичайними, або модульними - виконуються (всі або окремі з них) по модулю (залежно від типу коду - малої чи великої величини), або логічними, в тому числі у вигляді порозрядних логічних додавань і множень.

В результаті такого множення отримують перетворений код - матрицю $B = A\times G$ розмірності $(1\times m)$. Ясно, що для зворотного перетворення, тобто для отримання вихідного коду A з B достатньо виконати множення B на матрицю G^{-1}, зворотну до G:

$$A = B\times G^{-1} = A\times G\times G^{-1}.$$

Матриця G^{-1} носить назву декодувальної. Розмірність кодувальної матриці G (рис. 1), правила вибору, використання або формування її елементів (підматриць) визначаються видом перетворення, а також можливостями побудови зворотних матриць G^{-1}. Для визначеності будемо вважати, що умови існування зворотної матриці G^{-1} виконуються.

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ g_{n1} & g_{n2} & \cdots & g_{n2} \end{pmatrix}$$

Рис. 1 Загальний вигляд кодувальної матриці

Перший варіант - криптоперетворення. При використанні вихідного коду довжиною в *m* символів матриці *G* (рис. 1), яка в цьому випадку носить назву шифрувальної, із *m* рядків і *m* стовпців і певних правилах вибору або формування її елементів можна отримати матриці для криптографічних перетворень (шифрування) вихідного тексту.

Код, отриманий в результаті множення вихідного коду на кодувальну матрицю, є деяким криптографічним перетворенням вихідного коду. Якщо механізм формування елементів кодувальної матриці є секретним, або механізм формування елементів кодувальної матриці є загальновідомим, але при їх формуванні використовуються певний секретний параметр - ключ, то зашифрований код має визначену криптографічну стійкість, тобто стійкість до спроб криптоаналітиків отримати з зашифрованого коду вихідний.

Така криптографічна стійкість є основною властивістю даних перетворень і досить часто визначається кількістю варіантів ключів.

Зворотне перетворення (дешифрування) здійснюється шляхом множення вектора-рядка зашифрованого тексту *B* на дешифрувальну матрицю G^{-1}, зворотну до *G*.

Другий варіант - завадостійке кодування. Описані вище перетворення забезпечують надзвичайно важливу властивість захищеності інформації - конфіденційність, однак не дозволяють вирішувати проблему контролю, а тим більше, відновлення цілісності інформації. (Єдиним, мабуть, винятком є випадок, коли факт неможливості дешифрування зашифрованого слова можна тлумачити як факт наявності в ньому спотворення). Це пов'язано з тим, що операція обчислення нової матриці $B = A \times G$ не призводить до збільшення в закодованому слові кількості інформації (появи в ньому нової інформації), необхідної для подальшого виявлення факту спотворення, місця спотворення і його величини.

Необхідною умовою введення потрібної нової інформації є введення надлишковості в процедури перетворень, в тому числі, − у результат перетворення. Із цією метою необхідно забезпечити збільшення (розширення) розмірності, в загальному випадку, як початкового так і результуючого векторів-рядків на *k* символів, тобто до $n = m + k$ символів. Зрозуміло, що із цією метою необхідним є і розширення як кодувальної, так і декодувальної матриць. Найбільш простою процедурою перетворення вихідного коду довжиною в *m* символів у вихідне слово для кодування довжиною в *n* символів є додавання (вставка) $k = (n–m)$ додаткових символів, наприклад, в кінець вихідного коду (у деяких кодах, наприклад, в кодах Хеммінга, така вставка може здійснюватися і між символами вихідного коду). Отже, для перетворень, що дозволяють здійснювати контроль цілісності (можливо з подальшим її відновленням) необхідно ввести потрібну для цього додаткову інформацію, тобто використовувати матриці розмірності $n>m$ і, як наслідок цього, вихідні слова для кодування довжиною *n* символів. Тоді вихідне слово з *m* символів перетворюється в закодоване слово, як варіант - в завадостійкий код, довжиною в *n* символів.

Отже і кодувальна і перевірочна матриці, з причин, викладених вище, мають розмірність $(n \times n)$. Оскільки розмірність *n* перевищує довжину вихідного коду *m*, то можливі варіанти використання елементів матриці *G* або доведення довжини вихідного коду до *n*.

Звернемо увагу на те, що в такому випадку у складі кодувальної матриці G підматриці розмірності $(n \times n)$ можна відокремити підматрицю g розмірністю $(m \times m)$ (рис. 2) для перетворень інформаційної частини та власне кодувальну підматрицю k для розрахунку надлишкових символів розмірністю $(k \times n)$.

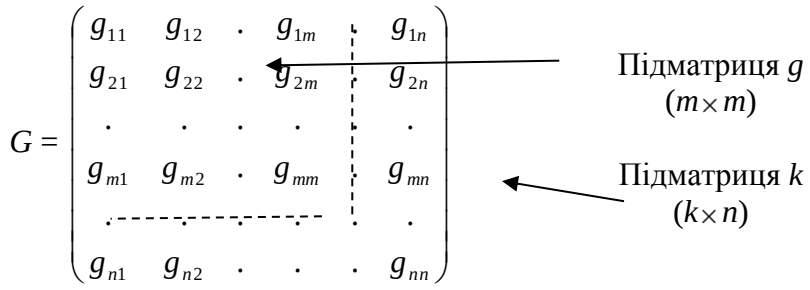

Рис. 2 Загальний вигляд матриці при завадостійкому кодуванні

Ці підматриці визначають можливості таких матричних перетворень. Якщо, наприклад, використовувати кодувальну матрицю, в якій п1ідматриця g є одиничною (рис. 3), то залежно від складу та порядку формування підматриці k можна одержати сукупність завадостійких кодів із різними можливостями щодо виявлення чи виявлення та виправлення спотворень у відповідних інформаційних об'єктах.

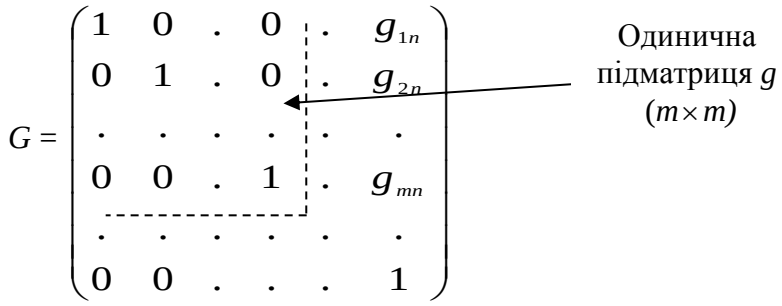

Рис. 3 Вид кодувальної матриці для завадостійких кодів

Тоді у результаті множення вихідного слова для кодування на кодувальну матрицю отримують n - символьний код, в якому перші m елементів співпадають з відповідними елементами вихідного коду, а інформація, яка формується в додаткових, надлишкових k символах закодованого слова в теорії завадостійкого кодування носить назву контрольної ознаки.

Як приклад, при $n - m = 1$, коли усі елементи n - го стовпця дорівнюють одиниці, отримаємо завадостійкий код (рис. 4), що виявляє спотворення і в якому контрольна ознака обраховується шляхом додавання всіх n елементів вихідного коду (еквівалент контрольного додавання). Таке додавання може бути, наприклад, порозрядним логічним або за модулем 2^b, де b - двійкова довжина символів вихідного коду, тобто його довжина в бітах.

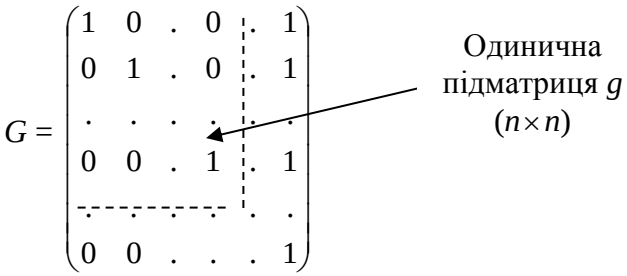

Рис. 4 Загальний вид кодувальної матриці для часткового випадку коду,
що виявляє спотворення (контрольне додавання)

При множенні закодованого слова на перевірочну матрицю G^{-1} отримують вектор - рядок помилок, елементи якого при виборі надмірності, достатньої для вирішення завдань виправлення помилок (коригувальні коди), несуть інформацію про наявність, місце і величину спотворень в коді, що перевіряється. При недостатній надмірності ці елементи несуть інформацію про місце або, просто, про наявність спотворень (коди, що виявляють спотворення). Надалі йдеться про завадостійкість коду, що належить, залежно від допустимої надмірності, до класу коригувальних або виявляючих. Такий код дозволяє при цьому вирішувати завдання контролю або контролю і відновлення цілісності контрольованих слів.

Третій варіант - завадостійка криптографія. Попередньо слід відзначити той факт, що найчастіше задачі забезпечення конфіденційності та цілісності інформації доводиться вирішувати одночасно по відношенню до одних і тих же інформаційних об'єктів. При цьому найчастіше процедура такого захисту полягає в послідовному застосуванні криптографічного перетворення і завадостійкого кодування зашифрованого тексту. На приймальній стороні спочатку перевіряється і відновлюється цілісність, а потім здійснюється дешифрування тексту. Тобто мова йде про двофазність процедур перетворення на обох сторонах і, як наслідок цього, про зниження загальної швидкодії засобів, що реалізують ці процеси.

Відзначимо [5], що використання кодувальної матриці виду, що надано на рис. 2, дозволяє використовувати однофазні процедури перетворення, що, на думку авторів, може підвищити загальну швидкодію засобів перетворення. В такому варіанті підматриця g розмірності $(m \times m)$ є матрицею криптографічного перетворення, а підматриця k розмірності $(n \times k)$ є матрицею завадостійкого кодування.

Код умовних лишків в задачах контролю цілісності. Нагадаємо, що під цілісністю інформації в комп'ютерних системах розуміють властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [2, 3]. Зрозуміло, що з цією метою потрібно або виключити можливість несанкціонованого доступу до цієї інформації неавторизованих користувачів, або здійснювати контроль (а в необхідних випадках контроль та поновлення цілісності) із використанням згаданих вище механізмів. Наразі прийнято вважати, що процедури завадостійкого кодування можна застосовувати лише при забезпеченні цілісності архівної інформації, у тому числі і резервних копій програмних засобів і баз даних. Це пов'язано із тим, що ці процедури не мають, або мають досить обмежену кількість варіантів параметрів, які можна було б вважати ключовими наборами і які можна зберегти в таємниці від неавторизованих користувачів. У зв'язку із цим зловмисник може легко зробити будь-яку модифікацію інформаційного об'єкту, обчислити нове значення ознаки цілісності (контрольної ознаки), що унеможливить виявлення такої модифікації. Отже, формування ознаки цілісності (контрольної ознаки) слід здійснювати із параметрами, які є невідомими неавторизованим користувачам і мають достатню кількість варіантів.

На думку авторів, для здійснення всіх описаних вище перетворень можна використовувати код умовних лишків (лишків умовних код - ЛУ-код). Це пов'язано з двома аспектами. Перший обумовлений тим, що на базі цього коду можна будувати алгоритми контролю цілісності, контролю і відновлення цілісності, криптографічних перетворень з контролем цілісності і, нарешті, криптографічних перетворень з контролем і відновленням цілісності.

Другий з них полягає в тому, що даний код одночасно з контролем і відновленням цілісності забезпечує і потрібний рівень імітостійкості. В рамках даної статті розглядаються можливості коду з контролю, контролю і відновленню цілісності.

У цьому коді, як і в інших, для контролю наявності спотворень - контролю цілісності, а в подальшому і відновлення цілісності базових кодових слів потрібно мати k додаткових (надлишкових) символів, які зберігають у собі в специфічному виді - у вигляді або контрольної ознаки (в термінах завадостійкого кодування), або хеш-функції (в термінах криптографічних перетворень) образ - деяке відображення інформації базових кодових слів,

яка контролюється, за її станом на час формування цього образу (а не після порушення цілісності!).

У загальному випадку базовим кодовим словом називається частина узагальненого кодового слова $A = \alpha_1, ..., a_n$, довжина якої визначена в символах (α_i), наприклад в байтах, задовольняє рівності

$$N = n \cdot \lambda,$$

де: N− кількість символів у блоці інформації(узагальненому кодовому слові);

λ − кількість базових кодових слів (глибина перемежування) в узагальненому кодовому слові;

n− кількість символів у базовому кодовому слові (довжина базового кодового слова).

У свою чергу, під узагальненим кодовим словом розуміється деяка частина файлу або послідовного набору даних − блок інформації довжиною N символів.

Контрольна ознака H будь-якого з базових кодових слів при застосуванні процедур ЛУ-коду формується з використанням кодувальної матриці, представленого на рис. 3 виду, елементами k-го ($k = m + 1$) стовпця якої є величини $g_{ki} = m_i/p_i$ ($i = 1,\ldots, n$), а операції множення при обчисленні контрольної ознаки виконуються за модулем $p_к$, де $p_к$− так звана контрольна ознака. Нагадаємо, що для використання операцій матричних перетворень необхідно забезпечити збільшення (розширення) розмірності початкового m – символьного вектора-рядка на k символів, тобто до $n = m + k$ символів. Таке розширення в найпростішому випадку можна здійснити дописуванням до початкового символьного вектора-рядка k нульових символів. Обчислення скалярного добутку базового кодового слова (вектора-рядка) на k-тий стовпець кодувальної матриці є еквівалентним обчисленню контрольної ознаки H відповідно до виразу

$$H = \alpha_k = \{p_k - \{[z \cdot p_k] \cdot R_k\}_{p_k}\}_{p_k}, \qquad (1)$$

де змінна z, у свою чергу, обчислюється заформулою:

$$z = \sum_{i=1}^{i=n} \frac{\alpha_i \cdot m_i}{p_i} - \left[\sum_{i=1}^{i=n} \frac{\alpha_i \cdot m_i}{p_i}\right].$$

В цих виразах:

- позначка $\{X\}_y$ означає операцію за модулем y (обчислення залишку від ділення X на y), а позначка $[X]$ - обчислення цілої частини змінної X;
- змінна m_i - константа ЛУ - коду, - "вага" так званого ортогонального базису системи числення ($i = 1,\ldots, n$);
- змінна R_k - константа ЛУ - коду, така, що дорівнює величині робочого діапазону системи числення – добутку основ, які утворюють цей робочий діапазон: $R_k = \prod_{i=1}^{m} p_i$;
- змінна n ($n = m+ k$), де m− кількість інформаційних символів у базовому кодовому слові, k − кількість додаткових (надлишкових) символів, необхідних для вирішення задачі виявлення факту наявності, місця і величини викривлень. Змінна k визначає при цьому потрібну кількість контрольних основ і, через це, - довжину контрольної ознаки $H = \alpha_k$;
- i - номер основи ($i = 1, 2, ..., n$);
- змінна α_i - числовий (двійковий) еквівалент i-го інформаційного символу частини файлу, що контролюється (базового кодового слова);
- p_i – i – та ($i = 1, ..., n$) основа (елемент криптографічного ключа, за допомогою якого забезпечується потрібна імітостійкість (див.далі). Ці основи вибираються як сукупність з n взаємно простих чисел.

При цьому як змінна p_k позначена контрольна (надлишкова) основа, така, що $p_k = p_n > p_m$ при вирішенні задачі контролю цілісності, та $p_k \geq p_m \cdot p_{m-1}$ при вирішенні задачі контролю та поновлення цілісності. В останніх виразах p_m та p_{m-1} − найбільші із основ, які утворюють робочий діапазон системи числення.

При цьому, оскільки величини p_i, з умови забезпечення технологічності механізмів формування контрольних ознак можна вибирати наприклад, восьмибітовими, то величини p_{n1} повинні бути, як мінімум, дев'ятибітовими, а тоді − змінна p_k, відповідно, повинна мати не менше 18 розрядів. Останнє, знову-таки з умови забезпечення технологічності, призводить до необхідності мати змінну p_k розрядністю не менше 3 байтів.

Змінні m_i і p_i є базовими константами ЛУ - коду. Розрахунок базових констант (вагових коефіцієнтів) m_i здійснюється, виходячи зі стандартних процедур, і потому не наводиться, а величини p_i є при цьому елементами конфіденційного ключа (секретним елементом при відомому алгоритмі перетворення) і вибираються користувачем (власником інформації).

Після формування контрольної ознаки її значення для будь-якого з базових кодових слів записується або після інформаційних наборів, або в іншому місці файлу, який контролюється, або в окремому файлі і зберігається для наступного контролю цілісності цих же базових кодових слів.

Контрольна ознака узагальнених кодових слів формується як конкатенація контрольних ознак всіх базових кодових слів.

Примітка 1. Під конкатенацією двох символів розуміється слово, довжина якого в бітах (байтах) дорівнює сумі числа біт (байтів) будь-якого з символів. При цьому ліва половина цього нового слова є першим словом, а права - другим словом.

Результуюча контрольна ознака тексту (файлу) формується як конкатенація контрольних ознак всіх блоків інформації − узагальнених кодових слів і зберігається (записується) в кінці файлу або після всіх файлів носія інформації.

Для останнього з узагальнених кодових слів, у разі, якщо кількість базових кодових слів в ньому є величиною не цілою, меншою ніж λ або, якщо довжина файлу є невеликою, як контрольні ознаки відсутніх базових кодових слів приймаються нульові контрольні ознаки, тобто контрольні ознаки, в яких кожен з k байтів, які входять до їх складу, є арифметичним нулем.

При організації контролю і відновлення цілісності шляхом використання властивостей ЛУ - коду, відповідно до алгоритму обчислення контрольних ознак базових кодових слів, здійснюється обчислення величини Z відповідно до виразу (1), в якому n_1 змінна приймає значення $n = n+k$.

Таким чином, при обчисленні величин Z для будь-якого з базових кодових слів на етапі контролю цілісності використовуються не тільки символи інформаційної частини файлу (носія), яка контролюється,− базового кодового слова, але і символи контрольної ознаки цього базового кодового слова.

Отримане при цьому значення величини Z порівнюється з константою ЛУ – коду $Z<1/p_k$, де змінна p_k, як і раніше, - контрольна основа ЛУ - коду.

Якщо ця нерівність задовольняється, то це є критерієм того, що цілісність цього базового кодового слова не порушено, і здійснюється контроль цілісності наступного базового кодового слова, доти, поки не здійсниться контроль усього носія.

Якщо ця нерівність не задовольняється, то це є критерієм того, що цілісність цього базового кодового слова порушено, і здійснюється його відновлення відповідно з нижче

викладеним Z - алгоритмом відновлення цілісності. Після цього здійснюються контроль цілісності наступного базового кодового слова доти, поки не закінчиться контроль всього носія.

Відновлення інформації при контролі цілісності з використанням властивостей ЛУ - коду не вимагає використання резервних копій, а є суто розрахунковим з повним використанням інформації, яка зосереджена в надлишкових символах - в контрольних ознаках будь-якого з базових кодових слів.

Відповідно до Z - алгоритму корекція спотвореної змінної, тобто обчислення неспотвореного значення цієї ж змінної, відбувається відповідно до виразу

$$\alpha_i = \{ \tilde{\alpha}_i - \{[Z \cdot p_i] \cdot R_i\}_{pi}\}_{pi},$$

в якому зміст усіх змінних співпадає з раніше визначеними, а змінна $R_i = (\prod_{j=1}^{n} p_j) / p_i$.

В останньому виразі не визначеним є лише значення i - номера спотвореного символу. Це значення знаходиться з системи нерівностей:

$$Z \cdot p_i - [Z \cdot p_i] < p_i / p_k, \ (i = 1, 2, ..., n).$$

За шукане значення i приймається номер тої нерівності (того p_i), для якого ця умова задовольняється.

Звернемо увагу на те, що значення основ p_i можуть бути відомими лише авторизованим користувачам. Отже, процес обчислення контрольних ознак за відомими алгоритмами, але за невідомими ключами або невідомими ключовими наборами є по суті криптографічним перетворенням при обчисленні контрольної ознаки інформації, цілісність якої повинна контролюватися. При цьому неавторизований користувач, не знаючи ключового набору, не має можливості замаскувати порушення цілісності інформації шляхом формування такої контрольної ознаки, яка б приховувала це порушення. Тобто запропонований підхід цілком задовольняє вимогам щодо контролю чи контролю та поновлення цілісності інформаційних об'єктів.

Імітостійкість запропонованих механізмів контролю цілісності

Під імітостійкістю запропонованих механізмів контролю цілісності інформації розуміється здатність бути нерозкритими використовуваних ключових наборів (наборів p_i), а також здатність не допускати приховування навмисних порушень цілісності інформації (імітацію відсутності порушень) з боку неавторизованих користувачів (зловмисників).

При цьому стійкість механізмів контролю цілісності інформації визначається стійкістю обчислень контрольних ознак, яка залежить від довжини вибраних ключів криптозахисту (кількості основ), а також від статистичної залежності початкового тексту (інформаційного блоку) з його криптографічним відображенням.

Під ключем криптозахисту в запропонованих механізмах контролю цілісності інформації розуміється набір чисел, які є чи то номерами основ (i), чи то власне основами (p_i). Основи в першому випадку вибираються за їх номерами з набору простих чисел. При цьому формується ключовий набір, інакше, таким ключовим набором є набір, який заданий у вигляді сукупності основ (p_i). Кількість цих основ визначає згадану вище довжину ключового набору.

Процес обчислення контрольних ознак за відомими алгоритмами, але за невідомими ключами або ключовими наборами ***є по суті криптографічним перетворенням*** в контрольну ознаку інформації, цілісність якої повинна контролюватися. При цьому неавторизований користувач, не знаючи ключового набору, не має можливості замаскувати порушення цілісності інформації шляхом формування такої контрольної ознаки, яка б приховувала це порушення.

Примітка. Звернемо увагу на те, що в запропонованих механізмах контролю цілісності інформації доступною для аналізу неавторизованими користувачами є лише

частина закритої інформації - контрольна ознака і відповідна частина (при n = 32, k = 3, це близько 8%) ключового набору для їх формування (основ для формування надлишкової інформації - контрольних ознак). Основна ж частина (для тих же умов - близько 92%) ключового набору є недоступною для аналізу, оскільки не є представленою в явному вигляді, а лише в контрольних ознаках в результаті перетворення інформації. Цим самим забезпечується прихованість ключа або результатів перетворення інформації відповідно до цього ключа. Це пов'язано з тим, що контрольні ознаки, які формуються, навіть найпростіші, є відображенням результатів перетворення інформації лише за незначною кількістю елементів ключа. Така властивість є не чим іншим, як додатковою можливістю підвищення імітостійкості запропонованих механізмів контролю цілісності інформації за рахунок відсутності безпосереднього статистичного зв'язку між первинним текстом і його контрольною ознакою, і дає можливість говорити про відсутність можливості або значному утрудненні з'ясування такої статистичної залежності початкового тексту (інформаційного блоку) з його криптографічним відображенням - контрольною ознакою. Останнє, у свою чергу, дозволяє говорити про можливість визначення ключа тільки шляхом прямого перебору і визначати стійкість запропонованого механізму контролю цілісності інформації лише через кількість варіантів ключів.

Якщо при контролі і відновленні цілісності використовується n= 195 робочих і k= 29 контрольних основ, то загальна кількість варіантів ключів $N_{вк}$ визначається як добуток кількості перестановок (розміщень) з 195 елементів по n на кількість перестановок (розміщень) з 29 елементів по k:

$$N_{вк} = A_{195}^{n} \cdot A_{29}^{k}.$$

При застосуванні цього механізму для контролю цілісності останнє обмеження на величини робочих основ знімається, тому їх кількість обмежена лише можливостями процесорів по обробці мультибайтових чисел і є значно більшим. Наприклад, лише кількість простих чисел, яке є більшими ніж 256 і меншими 6000 перевищує 650. Тому й кількість варіантів є значною.

ЛІТЕРАТУРА

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НДТЗІ 1.1-003-99.
2. Василенко В.С. Целостность информации в автоматизированных системах. / В.С.Василенко, М.П. Короленко // Корпоративные системы. 1999.–№ 3.–с. 52–57.
3. Василенко В.С. Методика оцінки захищеності інформації в ЛОМ. Графічні моделі взаємодії загроз функціональним властивостям захищеності інформаційних ресурсів ЛОМіз елементами системи захисту. / В.С. Василенко, О.В. Дубчак, М.Ю. Василенко // Безпека інформації/ – 2012. – № 1 (17).– С. 49 – 54.

Надійшла: 15.10.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.5

Недайбида Ю.П., Котова Ю.В., Хлапонин Ю.И.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ СОЗДАНИЯ СЛОЖНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

В статті розглянуті проблеми створення складних інформаційно-управляючих систем реального часу з урахуванням психічних особливостей людини як суб'єкту управління. Наданий в статті підхід дає можливість ситуаційної оцінки виникнення конфліктів та біфуркацій в складних інформаційно-управляючих системах, чіткого розподілення функцій управління, дій і прийняття рішень між оператором і технічними пристроями в реальному часі.

Ключові слова**:** інформаційно-управляючі системи (ІУС), ергономіка, ергопрофіка, людино-машинна система.