УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03056 Київ, Україна

Стійкість контрольних ознак коду умовних лишків в умовах загроз цілісності інформаційних об'єктів

Розглянуто можливості застосування колізій контрольних ознак у коді умовних лишків в умовах загроз цілісності інформаційних об'єктів.

Ключові слова: *кодування, колізії, інформаційні об'єкти, стійкість, цілісність.*

Вступ

Для забезпечення контролю цілісності інформаційних об'єктів, включаючи і можливе відновлення зруйнованої інформації, до складу інформації, яка захищається, включають надлишкову інформацію — хеш-функцію, ознаку цілісності або контрольну ознаку — своєрідний образ відображення цієї інформації, процедура формування якого відома, і який з дуже високою ймовірністю відповідає інформації, що захищається [1–3]. Механізми забезпечення цілісності істотно залежать від умов їхнього застосування, а саме: в умовах впливу випадкових або зловмисних спотворень. Характерною особливістю випадкових спотворень є те, що вони, через відсутність навмисності, з високою ймовірністю порушують регулярний (функціональний) односторонній зв'язок між інформацією й ознаками цілісності. Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких спотворень, а за певних умов, і їхнього місця та величини. За відсутності порушення цього зв'язку встановлюється факт відсутності спотворень.

Характерною ж особливістю навмисних спотворень є те, що зловмисник прагне забезпечити, зімітувати наявність регулярного зв'язку між модифікованою ним початковою інформацією і ознаками цілісності. З цією метою порушник може, використовуючи знання процедур формування контрольних ознак чи знання їхніх вразливостей, після необхідної для його цілей модифікації початкової інформації перед передачею одержувачу забезпечити формування відповідних ознак.

Постановка задачі

Украй важливим моментом при виборі засобів контролю цілісності є врахування характеру загроз інформаційним об'єктам, наслідком яких є відповідні спотворення. Йдеться, перш за все, про штучні впливи, коли відповідні порушники здійснюють заходи із маскування своєї шкідницької діяльності. Можливими шляхами цього є, по-перше, формування нових ознак цілісності, використовуючи знання процедур їхнього первинного формування. В цих умовах при застосуванні кодів із повністю відомими алгоритмами чи константами кодування, а, відповідно й декодування, порушник має нагоду ввести будь-яке спотворення та обчислити нове значення контрольної ознаки. Зрозуміло, що після цього спроби виявити такі спотворення є марними. Враховуючи очевидність можливостей такого шляху, за відповідних умов, розглядати його в подальшому не будемо.

По-друге, можна скористатися можливою вразливістю відповідних контрольних ознак (хеш-функцій), наприклад, наявністю їхніх колізій. Для цього порушник здійснює таку модифікацію, за якої ознака цілісності збігається з початковою (використати колізії хеш-функцій).

При успішному формуванні вказаних ознак, чи використанні їхніх колізій, розкрити наявність модифікації неможливо. Для боротьби з цим користувачу необхідно використовувати або секретні процедури формування контрольних ознак (що дуже складно забезпечити), або вводити в загальновідомі процедури формування контрольних ознак секретні параметри (ключі перетворення). Не знаючи цих ключів, порушник не зуміє зімітувати наявність регулярного зв'язку між модифікованою ним початковою інформацією і ознаками цілісності.

Таким чином, при вирішенні задач контролю чи контролю та поновленню цілісності інформаційних об'єктів в умовах захисту від умисних порушень слід або здійснювати криптографічний захист контрольних ознак, обчислених із застосуванням криптографічно не стійких завадостійких кодів, або ж застосовувати завадостійкі коди, стійкість яких забезпечена іншим шляхом, наприклад застосуванням таємних констант чи параметрів. Отже, слід застосовувати коди з високою стійкістю щодо маскування порушень цілісності відповідних інформаційних об'єктів. Одним із таких можливих кодів є *код умовних лишків* [1]. Тому в статті ставиться задача аналізу можливостей використання та оцінки стійкості алгоритмів кодування-декодування інформаційних об'єктів на основі *коду умовних лишків* [1].

Характеристика коду умовних лишків

При кодуванні для обчислення ознаки цілісності інформаційний об'єкт розглядається як деяке умовне число, представлене в системі лишкових класів $A_{СЛК}$, тобто у вигляді конкатенації умовних лишків α_i по сукупності основ p_i (i = 1, 2, …, n). Таке число спочатку за відповідними правилами переводиться в позиційну систему числення:

$$A_{ПСЧ} = (\sum_{i=1}^{i=n} \alpha_i b_i) \bmod P = \sum_{i=1}^{i=n} \alpha_i b_i - [(1/P)\sum \alpha_i b_i] \times P, \qquad (1)$$

де n — кількість умовних основ, які забезпечують потрібний діапазон представлення чисел у системі числення лишкових класів; $P=\prod_{i=1}^{n} p_i$ — діапазон представлення чисел у системі числення лишкових класів; b_i — константа системи числення, її ортогональний базис, такий, що: $b_i = P \cdot m_i / p_i$, (i = 1, 2, …, n); m_i — ціле позитивне число («вага» ортогонального базису b_i), таке що

$$b_i \pmod{p_i} = m_i b_i \pmod{p_i} = 1,$$

де позначка [X] означає обчислення цілої частки від X.

Обчислена таким чином величина $A_{ПСЧ}$, *по-перше*, не перевищує величини робочого діапазону, а, *по-друге*, надає змогу обчислення лишку числа $A_{ПСЧ}$ і по будь-якій іншій основі, наприклад — по надлишковій, контрольній основі p_{n+1}:

$$\alpha_{n+1} = (A_{ПСЧ}) \bmod p_{n+1} =$$

$$= \{(\sum_{i=1}^{i=n} \alpha_i b_i) \bmod P\} \bmod p_{n+1} = \{\sum_{i\ 1}^{i\ n} \alpha_i b_i - [(1/P) \sum_{i\ 1}^{i\ n} \alpha_i b_i] \times P\} \bmod p_{n+1},$$

яка і є *шуканою ознакою цілісності, що є метою процедури кодування*.

Криптографічні властивості ознак цілісності коду умовних лишків

У роботі [5] показано, що перетворення (1) є криптографічними, а отже ознака цілісності (хеш-функція), як результат криптографічних перетворень, має певні криптографічні властивості, зокрема, криптографічну стійкість. Для підтвердження цього звернемо увагу на те, що обчислення ознак цілісності α_{n+1} здійснюється, *по-перше*, з використанням відомостей про конкатенацію числових значень груп, на які умовно розбивається інформаційний об'єкт α_i (i = 1, 2, …, n). *По-друге*, з використанням невідомих, не наданих у явному вигляді констант коду умовних лишків — умовних основ системи числення p_i (i = 1, 2, …, n), де n — кількість умовних основ та інших змінних, які є функціями цих умовних основ: поточних змінних b_i — констант системи числення, її ортогональних базисів m_i, що мають назву «вага» ортогонального базису.

Тобто, серед цих змінних і констант відкритими є лише вихідний інформаційний об'єкт — конкатенація числових значень груп, на які розбивається інформаційний об'єкт. Решта інформації про використані константи, включаючи кількість груп умовних лишків, є закритою. Тоді, за цими ознаками перетворення, які надають у результаті ознаку цілісності інформаційного об'єкта, слід вважати криптографічними, а сама ознака цілісності має певну криптографічну стійкість.

З урахуванням того, що більшість згаданих констант є функціями умовних основ, до низки закритих слід віднести набір умовних основ системи числення p_i (i = 1, 2, …, n), їхню кількість, взаємне розташування та правила розподілу вихід-

ного інформаційного об'єкта на умовні лишки. Полегшимо задачу оцінки та порівняння криптографічної стійкості ознак цілісності коду умовних лишків, заздалегідь зменшивши її за рахунок виключення з розгляду таких закритих відомостей як кількість і правила розподілу вихідного інформаційного об'єкта на умовні лишки. Тоді набір p_i слід розглядати як ключовий.

Нагадаємо, одним із підходів оцінки стійкості певних криптографічних перетворень є визначення кількості комбінацій відповідних ключових наборів, що використовується в такому криптографічному перетворенні. Використаємо цей показник для порівняння криптографічної стійкості перетворень із застосуванням коду умовних лишків та алгоритмами формування цифрового підпису (за стандартом ГОСТ Р 34.10-94), і криптографічного перетворення (за стандартом ГОСТ 28147-89 із довжиною ключа в 256 біт та байтовою структурою відповідних даних і констант).

Нехай символами вихідного тексту є байт, а в якості контрольних основ (з умови технологічності програмної реалізації) необхідно використовувати складну контрольну основу із s взаємно простих чисел з проміжку [131, …, 251], оскільки їхня розрядність також повинна бути рівною 8 бітам (по 1 байту кожен). Неважко переконатися, що кількість таких чисел одно 29. Робочі основи, виходячи з умови забезпечення восьмибітових умовних лишків, як і символів вихідного тексту, слід вибирати розрядністю більшою, ніж 8. Тобто такими основами можуть бути взаємно прості числа, величина яких перевищує 257.

Кількість варіантів ключових наборів, як і надійність рішень також залежить від використаної надмірності, зокрема від кількості елементарних основ s в складній контрольній основі. Простежимо цю залежність. Як уже зазначено, основи, які утворюють робочий діапазон, в свою чергу, слід вибирати з діапазону, лівою межею якого є число 257. Права межа (основа p_n) при відомому значенні контрольної основи вибирається з умови, щоб добуток цього числа на найближче, менше, взаємно просте число (p_{n-1}), тобто добуток двох найбільших робочих основ, не перевищував би добутку s менших основ з числа контрольних:

$$p_{n+1} > p_n \cdot p_{n-1} \le \prod_{i=1}^{s} p_i \ .$$

Наприклад, при s = 3, мінімальне значення контрольної основи становить $p_{n+1} = \prod_{i=1}^{3} p_i = 131 \cdot 137 \cdot 139.$

Це значення повинно бути більшим ніж подвійний добуток максимальних основ, що утворюють робочий діапазон. Неважко показати, що ця умова задовольняється при максимальних основах p_n = 1117 та p_{n-1} = 1109, тобто при

$$131 \cdot 137 \cdot 139 = 2494633 > 2 \cdot 1117 \cdot 1109 = 2477506.$$

Це, в свою чергу, означає, що робочі основи слід вибирати з діапазону 257, …, 1117. При цьому кількість взаємно простих чисел у діапазоні 257, …, 1117 налічує 182. Якщо при контролі цілісності використовується n із 182-х робочих і s з 29-ти

контрольних основ, то загальна кількість варіантів ключів $N_{вк}$ визначається як добуток кількості розміщень зі 195-ти елементів по n на кількість розміщень з 29-ти елементів по s і при $n = 32$, $s = 3$ дорівнює:

$$N_{вк} = A_{182}^{n} \cdot A_{29}^{s} = A_{182}^{29} \cdot A_{29}^{3} > 3 \cdot 10^{76},$$

а ймовірність, що довільно обраний порушником ключ є правильним, дорівнює $p_{ВК} = 1 / N_{ВК}$

Якщо ж взяти $s = 4$, то основи, що утворюють робочий діапазон, у свою чергу, слід вибирати з діапазону 257, …, 13632, і кількість варіантів ключових наборів стає значно більшим і задовольняє будь-яким вимогам щодо стійкості засобів контролю цілісності щодо спроб їхнього подолання.

У таблиці для порівняння наведено кількість варіантів ключів для відомих механізмів формування цифрового підпису (за стандартом ГОСТ Р 34.10-94), і криптографічного перетворення (за стандартом ГОСТ 28147-89), а також запропонованого механізму.

Порівняння механізмів контролю цілісності інформації за кількістю варіантів ключових наборів

Довжина ключа (байти)	**Механізми формування ознак цілісності (хеш-функцій) для контролю цілісності інформації**				
	ГОСТ Р 34.10-94	ГОСТ 28147-89	ВУ-код		
			$n = 28$, $s = 4$	$n = 29$, $s = 3$	$n = 32$, $s = 4$
1	2	3	4	5	6
32	–	10^{76}	$>3 \cdot 10^{76}$	$>>10^{76}$	$>>10^{76}$
64	$9 \cdot 10^{8}$	–	$>10^{135}$	$>10^{136}$	$>10^{136}$
128	$9 \cdot 10^{25}$	–	$>>10^{260}$	$>>10^{260}$	$>>10^{260}$

Примітка. *У шостій колонці наведено дані для довжини інформаційної частини базового кодового слова в 32 байти і довжині надлишкової частини базового кодового слова в 4 байти.*

Як видно з таблиці, цей механізм забезпечує кількість варіантів ключів, яка істотно перевищує кількість варіантів ключів відомих механізмів, і має, відповідно, значно вищу імітостійкість. У наведених прикладах кількість варіантів ключів задовольняє вимогам навіть гарантованого криптозахисту.

Таким чином, аналіз криптографічного стійкості механізмів перетворень дає можливість стверджувати, що кількість варіантів ключових наборів при використанні коду умовних лишків є не меншою, ніж для інших відомих механізмів формування контрольних ознак.

Код умовних лишків і маскування порушень цілісності інформаційних об'єктів в умовах впливу навмисних загроз

Із викладеного вище витікає, що потенційному порушнику для маскування спотворень інформаційного об'єкта досить змінити числове значення цього об'єк-

та на величину $\pm l \cdot p_{n+1}$. Зрозуміло, що сформульована можливість маскування порушення цілісності притаманна інформаційним об'єктам, які розглядаються як деякі числа позиційної системи числення, та спотворенням і операціям з їхнього «впровадження в інформаційний об'єкт» у вигляді арифметичного додавання чи віднімання «величин» спотворень. Ці спотворення повинні бути величиною $\pm l \cdot p_{n+1}$ (одним числом чи їхньою такою сукупністю, яка в сумі дорівнює $l \cdot p_{n+1}$). Такі спотворення легко реалізуються, наприклад, у кодах з контрольним додаванням (CRC). Не важко зрозуміти, що при застосуванні в завадостійких кодах логічних операцій типу порозрядне додавання по модулю 2 (наприклад, циклічні коди, коди Хеммінга) можливість маскування порушення цілісності легко реалізується парними спотвореннями відповідних біт інформаційного об'єкта. У випадку таких спотворень ніякі засоби захисту (наприклад, криптографічні перетворення) відповідних контрольних ознак чи хеш-функцій не в змозі допомогти у виявленні замаскованих порушень цілісності. Отже, за таких умов, коли відомими є як алгоритм, так і змінні та константи для обрахування контрольних ознак, задача приховування (маскування) навмисного порушення цілісності є досить тривіальною і може здійснюватися з імовірністю, близькою до одиниці.

Зовсім інша ситуація утворюється при застосуванні запропонованого авторами коду умовних лишків. Згадаємо, що в цьому коді первинний інформаційний об'єкт уявляється як сукупність (конкатенація) числових значень груп, на які умовно розбивається інформаційний об'єкт α_i (i = 1, 2, …, n). При цьому ці групи вважаються лишками від розподілу деякого умовного числа $A_{ПСЧ}$ на сукупність основ p_i (i = 1, 2, …, n). Тепер слід згадати також, що для порушення цілісності, яке не виявляється (маскування порушення цілісності), коли ознака цілісності при модифікаціях первинного об'єкта не змінюється, необхідно здійснити зміну (в позиційній системі числення) первинного об'єкта на величину $\pm l \cdot p_{n+1}$. Але вихідне число, за умовою, є числом у системі лишкових класів, що потребує і введення змін цій же системі числення. А в системі лишкових класів порушення цілісності величиною $\Delta A_{ПСЧ} = l \cdot p_{n+1}$ трансформується в набір відповідних лишків

$$\Delta A_{СЛК} = \Delta\alpha_1, \Delta\alpha_2, \Delta\alpha_3, ..., \Delta\alpha_n,$$

де $\Delta\alpha_i = \Delta A_{СЛК} \bmod p_i$ (i = 1, 2, …, n). Отже, для маскування порушення цілісності слід модифікувати кожен з умовних лишків вихідного інформаційного об'єкта та одержати:

$$\begin{gathered}\tilde{A}_{СЛК} = (\alpha_1 + \Delta\alpha_1) \bmod p_1, (\alpha_2 + \Delta\alpha_2) \bmod p_2, (\alpha_3 + \Delta\alpha_3) \bmod p_3, ..., \\ (\alpha_n + \Delta\alpha_n) \bmod p_n = \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3, ..., \tilde{\alpha}_n.\end{gathered} \tag{2}$$

Тільки за такої умови буде забезпечено маскування порушення цілісності, тобто буде забезпечено незмінність ознаки цілісності:

$$\{\widetilde{A}_{СЛК}\} \bmod p_{n+1} = \{A_{СЛК}\} \bmod p_{n+1} = \alpha_n.$$

Але для виконання маскування згідно з виразом (2) слід мати інформацію про: сукупність умовних основ p_i (i = 1, 2, …, n), їхнє взаємне розташування, межі кожної з умовних лишків, тобто мати варіант ключа криптографічного перетворення, застосованого при обрахуванні ознаки цілісності. Але, як витікає із викладеного вище, ймовірність правильності довільно обраного ключового набору є суттєво меншою ніж імовірність того, що введене навмання порушення цілісності не буде виявленим застосованим алгоритмом контролю. Слід звернути увагу на ще один запобіжник проти порушення та маскування цілісності інформаційних об'єктів, який надає застосування коду умовних лишків. Цей запобіжник полягає в наступному. Нагадаємо, що в коді умовних лишків умовні основи p_i вибираються так, що $p_i > \alpha_i < 2^{m_i}$, де m_i — розрядність відповідного умовного лишку. Виконання операцій з маскування порушення цілісності із застосуванням сукупності виразів (2) по кожній з умовних основ p_i дає значення $\widetilde{\alpha}_i = (\alpha_i + \Delta\alpha_i) \bmod p_i$, яке завжди є меншим відповідної основи p_i: $\widetilde{\alpha}_i < p_i$, але може не забезпечити умови $p_i > \widetilde{\alpha}_i < 2^{m_i}$. Наприклад, використовується байтова структура умовних лишків $m_i = 8$ (тоді максимальне значення умовних лишків не може перевищувати величини $\alpha_i \le 255$), а умовна основа дорівнює $p_i = 491$. Нехай маємо випадок $\alpha_i = 255$, а значення $\Delta\alpha_i = 100$. Тоді, $491 > \widetilde{\alpha}_i = 255 + 100 = 355 > 255$. Це призведе до того, що для розміщення такого модифікованого лишку потрібно більше, ніж один байт 355 > 255, а отже загальна довжина інформаційного об'єкта збільшиться, що, по-перше, легко виявляється, наприклад в протоколах транспортного рівня TCP. По-друге досвідчений порушник, у силу цього, вимушено відмовиться від такого порушення цілісності.

Таким чином, у статті здійснено аналіз стійкості контрольних ознак інформаційних об'єктів у коді умовних лишків. Найбільш досконалим, на погляд авторів, є алгоритм з використанням процедури переведення із системи лишкових класів у позиційну систему числення.

1. *Василенко В.С.* Код условных вычетов: монографія / В.С. Василенко. — LAMBERT Academic Publishing, Saarbrucn+1en, Deutschland. — 2011. — 107 с. — ISBN 776-3-657-46203-6.

2. *Матов О.А.* Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об'єктів. Код умовних лишків / О.А. Матов, В.С. Василенко // Реєстрація, зберігання і обробка даних. — 2006. — Т. 6, № 3. — С. 46–66.

3. *Акушский И.Я.* Машинная арифметика в остаточных классах / И.Я. Акушский, Юдицкий Д.И. — М.: Сов. радио, 1766. — 421 с.

4. *Матов О.А.* Хеш-функції та цілісність інформаційних об'єктів / Матов О.А., В.С. Василенко // Реєстрація, зберігання і оброб. даних. — 2014. — Т. 16, № 4. — С. 12–17.

5. *Василенко В.С.* Геш-функції та цілісність інформаційних об'єктів / Василенко В.С. // Матеріали X міжнар. наук.-практ. конф. «Vědecký průmysl evropského kontinentu – 2014» 27 листопада – 05 грудня 2014 р. — Прага: Publishing House «Education and Science» s.r.o. — 2014. — Т. 19. — С. 8–12. — ISBN 978-966-8736-05-6; ISBN 978-966-8736-05-6,

6. *Василенко В.С.* Алгоритми кодування інформаційних об’єктів у коді умовних лишків / Василенко В.С., О.А. Матов // Реєстрація, зберігання і оброб. даних. — 2015. — Т. 17, № 1. — С. 99–107.

7. *Василенко В.С.* Блокові криптографічні перетворення з використанням лишкових класів / В.С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2005. — Вип. 10. — С. 99−105.

Надійшла до редакції 10.06.2015