УДК 621.391.037

В.Я. Пєвнєв, М.В. Цуранов

Харківський національний університет внутрішніх справ, Харків

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДУ ВІДНОВЛЕННЯ ПОВІДОМЛЕННЯ, ПРИЙНЯТОГО З ПОМИЛКАМИ

В статті теоретично доведено можливість гарантованого відновлення повідомлення за наявності однієї помилки. Теоретично доведено відсутність колізій у разі зміни двох з чотирьох біт повідомлення при успішному здійсненні перевірки на парність.

Ключові слова: *завадостійке кодування, біт, контрольна сума, відновлення повідомлення, колізія, метод перебору.*

Вступ

У наш час до ужитку увійшло поняття інформаційної безпеки (ІБ). Існує велика кількість визначень цього терміну [1 – 6], усі вони базуються на забезпеченні цілісності інформації. Ця властивість може бути досягнута декількома шляхами, один з них застосування завадостійкого кодування. Розроблена велика кількість завадостійких кодів [7]. За своєю структурою їх можна поділити на два великих класи: лінійні і нелінійні коди. У [8, 9] представлений підхід до побудови завадостійких кодів, де кожна четвірка біт перевіряється на парність, а у кінці повідомлення розміщується контрольна сума, за допомогою якої методом перебору відновлюється повідомлення.

Мета пропонованої роботи: теоретичне обґрунтування запропонованого методу і визначення меж можливого його застосування.

Виклад основного матеріалу

Відновлення повідомлення при одній помилці. Розглянемо систему зв'язку, в каналах якої є присутніми помилки. Абсолютно очевидно, що кількість помилок визначатиметься якістю каналу, розміром повідомлення що передається і типом помилок, що виникають в каналі. У [10] показано, що використовуючи запропонований метод, можна з достатньою достовірністю представити усі помилки як поодинокі і незалежні. Для доказу можливості використання запропонованого методу сформулюємо і доведемо таку теорему.

Теорема 1. Для гарантованого відновлення початкового повідомлення за наявності однієї помилки в повідомленні що передається досить послідовно змінити чотири біта в спотвореній четвірці.

Доведення теореми. Як відомо з [8, 9]

$$a_{i+3} = a_i \oplus a_{i+1} \oplus a_{i+2} ,$$

тобто

$$\sum_{p=i}^{i+3} a_p \bmod 2 = 0 .$$

Спотворена четвірка визначається, як один з чотирьох варіантів :

I варіант - $\overline{a}_i ; a_{i+1}; a_{i+2}; a_{i+3};$

II варіант - $a_i ; \overline{a}_{i+1}; a_{i+2}; a_{i+3};$

III варіант - $a_i ; a_{i+1}; \overline{a}_{i+2}; a_{i+3};$

IV варіант - $a_i ; a_{i+1}; a_{i+2}; \overline{a}_{i+3}$

При цьому $\sum_{p=i}^{i+3} a_p \bmod 2 = 1 .$

Послідовно змінюючи значення одного елементу, отримуємо початкову послідовність. Розглянемо випадок, коли був спотворений останній символ в послідовності:

$$\overline{a}_i ; a_{i+1}; a_{i+2}; \overline{a}_{i+3};$$

$$a_i ; \overline{a}_{i+1}; a_{i+2}; \overline{a}_{i+3};$$

$$a_i ; a_{i+1}; \overline{a}_{i+2}; \overline{a}_{i+3};$$

$$a_i ; a_{i+1}; a_{i+2}; a_{i+3} .$$

Тобто на четвертому кроці отримана початкова послідовність.

Виходячи з викладеного, можна стверджувати, що при послідовній зміні чотирьох біт, буде відновлена початкова послідовність., тобто теорема 1 доведена.

Якщо в повідомленні було спотворено дві і більше послідовності з чотирьох біт, то кількість можливих варіантів оцінюється як 4n, де n - кількість спотворених четвірок. Виходячи з вищевикладеного, можна сформулювати наступне слідство.

Наслідок теореми 1. Для відновлення початкового сполучення з n помилками досить змінити 4n біта з максимальною кількістю змін 4^n.

Можливість колізії при однієї помилки. В результаті застосування способу відновлення інформації, представленого в [8,9], при досить великій кількості помилок можливі колізії - події, коли два різні повідомлення мають однакову контрольну суму. У пропонованому методі в якості контрольної суми обирають залишки від ділення на 15, 14, 13, 11.

Отримана контрольна сума при цьому має розмір рівний двом байтам. Розглянемо наступну теорему.

Теорема 2. Зміна двох будь-яких елементів в послідовності з чотирьох біт, що задовольняє перевірці на парність, не призводить до колізії.

Доведення теореми. Для доведення запропонованої теореми необхідно розглянути усі можливі комбінації побудови відновлюваних послідовностей в загальному вигляді. Таких послідовностей буде 16.

При спотвореному першому елементі послідовності матимуть такий вигляд:

$a_i;\ a_{i+1};\ a_{i+2};a_{i+3};\ \ \overline{a}_i;\ \overline{a}_{i+1};\ a_{i+2};a_{i+3};$

$\overline{a}_i;\ a_{i+1};\ \overline{a}_{i+2};a_{i+3};\ \ \overline{a}_i;\ a_{i+1};\ a_{i+2};\overline{a}_{i+3}.$

При спотвореному другому елементі:

$\overline{a}_i;\ \overline{a}_{i+1};\ a_{i+2};a_{i+3};\ \ a_i;\ a_{i+1};\ a_{i+2};a_{i+3};$

$a_i;\ \overline{a}_{i+1};\ \overline{a}_{i+2};a_{i+3};\ \ a_i;\ \overline{a}_{i+1};\ a_{i+2};\overline{a}_{i+3}.$

При спотвореному третьому елементі:

$\overline{a}_i;\ a_{i+1};\ \overline{a}_{i+2};a_{i+3};\ \ a_i;\ \overline{a}_{i+1};\ \overline{a}_{i+2};a_{i+3}$

$a_i;\ a_{i+1};\ a_{i+2};a_{i+3};\ \ a_i;\ a_{i+1};\ \overline{a}_{i+2};\overline{a}_{i+3}.$

При спотвореному четвертому елементі:

$\overline{a}_i;\ a_{i+1};\ a_{i+2};\overline{a}_{i+3};\ \ a_i;\ \overline{a}_{i+1};\ a_{i+2};\overline{a}_{i+3};$

$a_i;\ a_{i+1};\ \overline{a}_{i+2};\overline{a}_{i+3};\ \ a_i;\ a_{i+1};\ a_{i+2};a_{i+3}.$

При розгляді множини послідовностей представлених вище, можна побачити, що деякі повторюються. Якщо прибрати послідовності, що повторюються, то з 16 залишиться 7 послідовностей:

$a_i;\ a_{i+1};\ a_{i+2};a_{i+3};\ \ \overline{a}_i;\ \overline{a}_{i+1};\ a_{i+2};a_{i+3};$

$\overline{a}_i;\ a_{i+1};\ \overline{a}_{i+2};a_{i+3};\ \ \overline{a}_i;\ a_{i+1};\ a_{i+2};\overline{a}_{i+3};$

$a_i;\ \overline{a}_{i+1};\ \overline{a}_{i+2};a_{i+3};\ \ a_i;\ \overline{a}_{i+1};\ a_{i+2};\overline{a}_{i+3};$

$a_i;\ a_{i+1};\ \overline{a}_{i+2};\overline{a}_{i+3}.$

Усі елементи цих множин є прямими і інвертованими значеннями чотирьох біт, що входять у відновлювану послідовність. Очевидно, що усі вони можуть набувати значень рівні одиниці і нулю. Виходячи з алгоритму відновлення повідомлення [8], необхідно порівняти передані і відновлені контрольні суми. Для наявності колізії необхідно довести, що сума двох переданих біт дорівнюватиме сумі їх інверсії

$$\left(a_{i+k}\times 2^{i+k}+a_{i+n}\times 2^{i+n}\right)\bmod z=$$
$$=\left(\overline{a}_{i+k}\times 2^{i+k}+\overline{a}_{i+n}\times 2^{i+n}\right)\bmod z. \quad (1)$$

де k= 0, 1, 2; n = 1, 2, 3; k < n, z=11, 13, 14, 15.

Для прозорості доказу зведемо усі можливі стани біт в табл. 1.

Таблиця 1

Можливі стани бітової послідовності

	a_{i+k}	a_{i+n}	$\overline{a}_{i+k}$	$\overline{a}_{i+n}$
1 варіант	1	1	0	0
2 варіант	1	0	0	1
3 варіант	0	1	1	0
4 варіант	0	0	1	1

Розглянемо послідовність, в якій k= 0, n = 1.

1 варіант

$$\left(2^i+2^{i+1}\right)\bmod 11=0;$$
$$3\times 2^i \bmod 11=0;$$
$$2^i \bmod 11=0.$$

У цього рівняння немає рішення.

2 варіант

$$2^i \bmod 11=2^{i+1}\bmod 11;$$
$$2^i \bmod 11=0.$$

У цього рівняння немає рішення.

Два інші рівняння для цього варіанту k і n дзеркально повторюють нами розглянуті.

Розглянемо послідовність, в якій k= 0, n = 2.

1 варіант

$$\left(2^i+2^{i+2}\right)\bmod 11=0;$$
$$5\times 2^i \bmod 11=0;$$
$$2^i \bmod 11=0.$$

У цього рівняння немає рішення.

2 варіант

$$2^i \bmod 11=2^{i+2}\bmod 11;$$
$$3\times 2^i \bmod 11=0;$$
$$2^i \bmod 11=0.$$

У цього рівняння немає рішення.

Два інші рівняння для цього варіанту k і n дзеркально повторюють нами розглянуті.

При розгляді наступних варіантів слід зазначити той факт, що відбувається збільшення початкового стану і на одиницю, і усі наші вищевикладені математичні викладення повторюються для k= 0, 1; n = 1, 2.

Тобто нами доведено неможливість виникнення колізії при відновленні повідомлення у разі спотворення одного символу в послідовності що передається.

Можливість колізії при двох помилках в повідомленні. При передачі даних можливе виникнення двох і більше помилок в повідомленні що передається. Для відновлення повідомлення при виникненні двох помилок, виходячи з наслідку **теореми 1**, досить змінити 8 біт з максимальною кількістю змін рівним 16. Для першої змінюваної четвірки стан змінюваних біт представлений в табл. 1. Аналогічну таблицю будуємо для другої четвірки.

Таблиця 2

Друга четвірка біт що змінюється

	a_{i+k+4p}	a_{i+n+4p}	$\overline{a}_{i+k+4p}$	$\overline{a}_{i+n+4p}$
1 варіант	1	1	0	0
2 варіант	1	0	0	1
3 варіант	0	1	1	0
4 варіант	0	0	1	1

Для знаходження колізій необхідно вирішити систему з двох рівнянь. Для варіанту 1-1, виходячи з (1), отримуємо:

$$\begin{cases} \left(2^{i} + 2^{i+1}\right) \bmod z = 0; \\ \left(2^{i+4p} + 2^{i+1+4p}\right) \bmod z = 0. \end{cases} \quad (2)$$

Після складання двох рівнянь, отримуємо:

$$\left(2^{i} + 2^{i+1} + 2^{i+4p} + 2^{i+1+4p}\right) \bmod z = 0.$$

Після невеликих математичних перетворень отримуємо:

$$\left(3 \times 2^{i}\left(1 + 2^{4p}\right)\right) \bmod z = 0$$

Для знаходження колізій необхідно знайти рішення для усіх значень z, іншими словами необхідно вирішити таку систему рівнянь :

$$\begin{cases} \left(1 + 2^{4p}\right) \bmod 11 = 0; \quad \left(1 + 2^{4p}\right) \bmod 13 = 0; \\ \left(1 + 2^{4p}\right) \bmod 14 = 0; \quad \left(1 + 2^{4p}\right) \bmod 15 = 0. \end{cases} \quad (3)$$

Читач, знайомий з модулярною арифметикою, може переконатися, що при z=14, це рівняння не має рішення. Отже, не має рішення і уся система.

Для варіантів 1-2, 1-3, 1-4 можна побудувати системи рівнянь аналогічні (2), які після незначного перетворення набирають вигляду:

$$\left(2^{i} + 2^{i+1} + 2^{i+4p} - 2^{i+1+4p}\right) \bmod z = 0;$$

$$\left(2^{i} + 2^{i+1} - 2^{i+4p} + 2^{i+1+4p}\right) \bmod z = 0;$$

$$\left(2^{i} + 2^{i+1} - 2^{i+4p} - 2^{i+1+4p}\right) \bmod z = 0.$$

Для кожного з рівнянь будуємо систему рівнянь, аналогічну системі (3), вирішуючи які, переконуємося у відсутності рішення.

Головним висновком, який витікає з цих досліджень, є доказ відсутності колізій при перегляді комбінацій 1 варіанту (таблиця.1) з усіма можливими станами біт, представлених в табл. 2.

Аналогічним чином розглядаємо інші складові табл. 1, 2 приходимо до висновку про неможливість колізій при розмірі посилки до 2048 біт.

Висновки

В представленій роботі показано теоретичне обґрунтування можливості застосування запропонованого коду, який відновлює помилки, в повідомленнях за наявності одного чи двох спотворених символів.

Список літератури

1. Доктрина інформаційної безпеки України. ЗАТВЕРДЖЕНО Указом Президента України від 8 липня 2009 року № 514/2009. – Режим доступу до тексту: http://www.president.gov.ua/documents/9570.html.

2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи / Б.А. Кормич. – К.:Кондор, 2004. – 384 с.

3. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдин. – К.: МК-Прес, 2005. – 432 с.

4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов / А.А. Матюк .– М.: Горячая линия-Телеком, 2004. – 280 с.

5. Інформаційна безпека України: сутність та проблеми. Матеріали круглого столу. – Режим доступу до тексту: www/nirr.gov.ua/ukr/publishing/panorama3_4.

6. Певнев В.Я. Математическая модель информационной безопасности / В.Я. Певнев, М.В. Цуранов // Системи обробки інформації. Збірник наукових праць. – Х.: ХУПС, 2010, – Вип. 3(84). – С. 27-30.

7. Хэмминг Р.В. Коды с обнаружением и исправлением ошибок Р.В. Хэмминг .– М.:ИЛ, 1956. – С. 7-22.

8. Патент Украины № 26778. Спосіб відновлення інформації при обміні даними у телекомунікаційних системах// Логвиненко М.Ф., Серков О.А., Пєвнєв В.Я. Чурюмов Г.І.,Яценко І.Л., БИ № 16 от 10.10.07.

9. Певнев В.Я. Сравнительный анализ скорости работы помехоустойчивых кодов / В.Я. Певнев, М.В. Цуранов // Теоретические и прикладные проблемы информационной безопасности : тез. докл. Межд. науч.-практ. конф. (Минск, 21 июня 2012 г.) / М-во внутр. дел Респ. Беларусь, учреждение образ. «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2012. – С. 153-156.

10. Певнев В.Я., Цуранов М.В. Экспериментальные исследования моделей групповых ошибок в каналах святи / В.Я. Певнев, М.В. Цуранов // Вісник НТУ „ХПІ”. Збірник наукових праць. – Х.:НТУ”ХПІ”, 2011. –№49. – С.115-121.

Надійшла до редколегії 18.01.2013

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ МЕТОДА ВОССТАНОВЛЕНИЯ СООБЩЕНИЯ, ПРИНЯТОГО С ОШИБКАМИ

В.Я. Певнєв, М.В. Цуранов

В статье теоретически доказана возможность гарантированного восстановления сообщения при наличии одной ошибки. Теоретически доказано отсутствие коллизий в случае изменения двух из четырех бит сообщения при успешном проведении проверки на четность.

Ключевые слова: *помехоустойчивое кодирование, бит, контрольная сумма, восстановления сообщения, коллизия, метод перебора.*

THE THEORETICAL FOUNDATION OF THE METHOD RECOVERY MESSAGES RECEIVED WITH ERRORS

V.Ya.. Pevnev, M.V. Tsuranov

This article theoretically demonstrates the possibility of a guaranteed renewal of a message in the presence of a single error. Theoretically, it also shows that, if the parity check is successful, there will be no collision when changing two of four bits in a message.

Keywords*: Antinoise encoding bit checksum, recovery message collision method of enumeration.*