Выводы

1. При использовании кольцевых кодов предыскажению с одинаковым результатом может подвергаться либо исходный вектор, либо любая строка.

2. Смещение исходного вектора кольцевого кода позволяет кроме основного ВПС получить $N - 1$ дополнительных векторов особых частных показателей сдвигов с новыми свойствами.

3. Применением особых кольцевых кодов обеспечивается получение широкого спектра различных спецификаторов.

4. Для предыскажений удобно иметь банк предыскажающих двоичных последовательностей-фильтров.

5. Один и тот же фильтр посредством XOR-преобразования служит и для внесения предыскажения в кодовое слово, и для его удаления.

6. Глубина предыскажения может быть любой и диктоваться требованиями защиты данных от несанкционированного доступа.

7. Для защиты информации от несанкционированного доступа одновременно с предыскажением можно использовать принципы криптографии.

Литература

1. ***Дикарев, А. В.*** *Коды на основе двоичных колец / А. В. Дикарев // Системи управління, навігації та зв'язку.— 2014.— Вип. 1(29).— С. 50–53.*

2. ***Дикарев, А. В.*** *Постулаты кольцевых кодов / А. В. Дикарев // Зв'язок.— 2013.— Вип. №5(105).— С. 53–56.*

3. ***Дикарев, А. В.*** *Идентификация семейств кольцевых кодов // А. В. Дикарев // Телекомунікаційні та інформаційні технології.— 2015.— №2.— С. 52–57.*

4. ***Дикарев, А. В.*** *Некоторые закономерности кольцевых кодов // А. В. Дикарев / Системи управління, навігації та зв'язку.— 2014.— Вип. 3(31).— С. 51–55.*

Рецензент: доктор техн. наук, профессор **Б. Ю. Жураковский**, Государственный университет телекоммуникаций, Киев.

О. В. Дікарев

ОСОБЛИВІ КІЛЬЦЕВІ КОДИ — ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

Доведено, що завдяки внесенню попередніх спотворень у кільцеві коди останні набувають нових корисних властивостей і можуть кваліфікуватись як особливі кільцеві коди, котрі з вихідними класичними кодами пов'язані певною функціональною залежністю. Надаючи особливим кодам деяких властивостей криптографії, маємо змогу використовувати їх не тільки для виявлення та виправлення канальних помилок, а й для захисту інформації від несанкціонованого доступу.

Ключові слова: кільцевий код; ідентифікатор; кодове слово; вектор; фільтр.

A. V. Dikarev

THE SPECIAL RING CODES — AVERTING A DANGER OF NOT AUTORISED ACCESS

It is shown, that as a result of entering of predistortions into ring codes the last get new useful properties owing to what they can be qualified as special ring codes. Initial "classical" and special ring codes are connected by functional dependence.

Giving to special codes certain properties of cryptography, begins possible to use them not only for detection and correction of errors, but also for protection of data against not authorised access.

Keywords: a ring code; the identifier; a code word; a vector; the filter.

УДК 381.3.004

М. М. БРАЇЛОВСЬКИЙ, канд. техн. наук, доцент;
С. В. КОЗЕЛКОВ, доктор техн. наук, професор, заслужений винахідник України,
лауреат Державної премії України в галузі науки і техніки;
Н. В. КОРШУН, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

ОПТИМІЗАЦІЯ ВИБОРУ ПАРАМЕТРІВ ЯКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КАНАЛАХ ЗВ'ЯЗКУ

Запропоновано критерій вибору параметрів якості складної системи, який дозволяє давати узагальнену оцінку якості такої системи в діапазоні можливих відхилень значень частинних критеріїв від екстремальних і завдяки цьому враховувати ступінь погіршення одних параметрів за рахунок поліпшення інших.

Ключові слова: оптимізація; система захисту інформації; параметри якості; канали зв'язку.

Вступ

Коли та чи інша природна система (організм) протягом тривалого часу залишається цілісною, не руйнуючись під впливом зовнішніх чинників, то її вважають життєздатною. Адже, як відомо, функціонування в природних умовах відсіює нежиттєздатні організми. Для того щоб вижити, організм має адаптуватись до навколишніх умов. Те саме стосується й технічних систем. Тому при їх проектуванні, розробці та модернізації доводиться

насамперед дбати про забезпечення здатності системи зберігати рівновагу, незважаючи на зовнішні та внутрішні впливи. Це завдання особливо ускладнюється в разі сучасних великих систем, де існують надзвичайно різноманітні механізми взаємодії між їхніми підсистемами.

Ідеться передусім про космічні системи зв'язку (КСЗ), функціонування яких потребує дедалі надійніших систем захисту інформації (СЗІ). Створення СЗІ для КСЗ з якомога точнішим оцінюванням їхньої роботоздатності передбачає розв'язання широкого кола багатопланових завдань.

Здійснювати вибір параметрів якості СЗІ є сенс на базі критерію, який має охоплювати застосування однієї і тієї самої системи в різних умовах, а також різних систем при розв'язуванні однопланових завдань.

Мета статті полягає у виборі такого критерію щодо СЗІ в каналах зв'язку.

Основна частина

Намагання поліпшити в процесі проектування СЗІ один із параметрів якості функціонування цієї системи неминуче призводить до зміни певної кількості інших її параметрів. Тому й не вдається строго обґрунтувати вигляд результуючої цільової функції (визначити узагальнений показник якості) об'єктивним шляхом. У таких випадках одна з можливостей полягає в застосуванні лінійного критерію [1].

Припустимо, що якість функціонування СЗІ описується сукупністю $\vec{K} = < K_1, K_2, ..., K_m >$ частинних критеріїв, які необхідно мінімізувати.

Знайдемо відносні відхилення частинних критеріїв від екстремальних (мінімального і максимального) значень:

$$K^i_{\max} = \frac{K_i(\text{СЗІ}) - K_i^{\min}(\text{СЗІ})}{K_i^{\max}(\text{СЗІ})}, \quad i = \overline{1, m}. \qquad (1)$$

Тоді вибрана СЗІ буде оптимальною за сукупністю частинних критеріїв, якщо вони характеризуються множиною відносних відхилень, які мають найменші значення.

Позначивши оптимальний варіант СЗІ як C_0, запишемо цю задачу у формалізованому вигляді:

$$K'_{\max}(C_0) < K_{\max}(C); \;\; C, C_0 \in C_{\text{СД}}, \qquad (2)$$

де $K'_{\max} = \max\{K'_i\}$; $i = \overline{1, m}$ — найбільше з відносних відхилень, розраховуваних за формулою (1); $C_{\text{СД}}$ — множина строго допустимих систем, що задовольняють умови застосовності системи та обмеження на структуру і значення основних її параметрів.

До умов застосовності СЗІ належать, наприклад, діапазон робочих температур, глибина захисту і т. ін.

Пропонований критерій відрізняється від наведених у [1; 2] тим, що дозволяє давати оцінку СЗІ в діапазоні можливих відхилень частинних критеріїв і завдяки цьому додатково враховує ступінь погіршення одних параметрів СЗІ за рахунок поліпшення інших. Однак при використанні критерію $K_i^{\min} << K_i^{\max}$ перевага може бути надана такій СЗІ з пари існуючих, яка при незначно кращому (меншому) значенні одного параметра якості має значно гірші порівняно з рештою СЗІ інші параметри. У такому разі даний критерій має той самий недолік, що й згадувані вже критерії в [1; 2]. З огляду на це при виборі оптимального варіанта із сукупності СЗІ однакового технологічного виконання доцільно використати модифікований мінімаксний критерій (2), подавши його у вигляді:

$$K_{\text{р}} = f_{\text{р}}(K_1, ..., K_i, ..., K_m) = \min_{C \in C_{\text{СД}}}, \qquad (3)$$

де

$$f_{\text{р}}(K_1, ..., K_i, ..., K_m) =$$

$$= \max\left(\frac{K_1 - K_1^{\min}}{K_1^{\max}}, ..., \frac{K_i - K_i^{\min}}{K_i^{\max}}, ..., \frac{K_m - K_m^{\min}}{K_m^{\max}}\right). \qquad (4)$$

Система захисту інформації C_0, що її визначає розв'язок задачі (3), (4), і буде оптимальною. Із формули (3) впливає, що мінімаксний критерій можна вважати різновидом критерію на базі мінімізації результуючої цільової функції, вигляд якої відповідає виразу (4).

Залежності (3) і (4) показують, що мінімаксний критерій забезпечує найкраще (найменше) значення із сукупності найгірших (найбільших) нормованих показників якості. Тому всі частинні показники якості СЗІ слід звести до стандартного вигляду. Показник якості K_i вважатиметься стандартним, якщо він задовольнятиме умову $K_i \geq 0$, де $i = \overline{1, m}$.

При цьому чим менше значення K_i, тим кращий вибраний варіант СЗІ. Якщо деякий показник якості K_i^* не стандартний, то його завжди можна звести до вигляду K_i.

Нехай, наприклад, невід'ємний показник якості K_i^* задовольняє нерівності $K_{i\min}^* \leq K_i^* \leq K_{i\max}^*$ і при цьому чим більше значення K_i^*, тим краща відповідна СЗІ. Тоді як еквівалентний йому стандартний показник якості слід вибрати

$$K_i = K_{i\max}^* - K_i^*,$$

а коли $K_{i\max} \to \infty$, то $K_i = \frac{1}{K_i^*}$.

Отже, K_i^* — стандартний показник якості, який дає змогу здійснювати порівняння СЗІ у різних умовах експлуатації або зіставляти між собою різні системи, які працюють на одному й тому самому об'єкті.

Припустимо, що СЗІ (типорозмір) параметричного ряду характеризується m-вимірним вектором:

$$\overrightarrow{K_j} = \left\langle K_{j1}, ..., K_{ji}, ..., K_{jm} \right\rangle; \; j = \overline{1, n},$$

де j — порядковий номер типорозміру; K_{ji} — частинний критерій якості j-го типорозміру, зведений до стандартного вигляду.

Потреби в кожному типорозмірі параметричного ряду задаються однією з координат вектора $\overrightarrow{K_j}$, з урахуванням меж $K_j^{\min}$ і $K_j^{\max}$ можливих значень критеріїв, де $K_j^{\min}$ — найменше, а $K_j^{\max}$ — найбільше значення j-ї координати вектора за всіма значеннями j. Типорозміри вхідного змінного ряду впорядковано за найбільш значущим частинним критерієм, якому відповідає порядковий номер координати $i = 1$. Таким чином, можна записати:

$$K_{11}^{\max} \geq K_{21} \geq K_{j1} \geq K_{(n-1)1} \geq K_{n1}^{\max}; \; j = \overline{1, n}.$$

Будемо також вважати заданим набір опорних векторів $K_r^0\left(r = \overline{1, R}\right)$, кожний з яких характеризує якість СЗІ, виконаної в рамках однієї схемотехнічної реалізації. Основні параметри цих СЗІ можуть бути оцінені за результатами аналізу моделей і тенденцій розвитку систем охорони і повинні на час реалізації вимог параметричного ряду відповідати досягнутому рівню розвитку зазначених систем. Тоді шляхом установлен-

ня відповідності опорного і вхідного наборів векторів із координатами, які задовольняють значущий критерій якості СЗІ, інтервал $\left[K_{11}^{\max}, K_{n1}^{\min}\right]$ можна розбити на дрібніші інтервали $\left[K_{11}^{\max}, K_{11}^{0}\right], \left[K_{11}^{0}, K_{21}^{0}\right], \ldots, \left[K_{(R-1)1}^{0}, K_{R1}^{0n}\right]$, де $K_{R1}^{0} \le K_{n1}^{\min}$.

Таким чином, можливе повне покриття інтервалу $\left[K_{11}^{\max}, K_{n1}^{\min}\right]$ і задоволення всіх вимог до СЗІ.

Системи захисту інформації з опорними критеріями якості утворюють опорний параметричний ряд, у загальному випадку не оптимальний. Це пов'язано з тим, що один або кілька параметрів системи можуть перевищувати необхідні значення. Утім для забезпечення високого технічного рівня розробок необхідно створити СЗІ, параметри яких максимально відповідали б новітнім досягненням у сфері захисту інформації.

Компромісне вирішення при цьому дозволяє оптимізувати параметричний ряд на основі мінімаксного критерію. Для інтервалу $\left(K_{(r-1)1}^{0}, K_{r1}^{0}\right)$, де $r = \overline{1, R}$, розв'язуємо таку задачу математичного програмування:

$$\min_{K_{j\in\Omega_r^s}} r K^{!}\left(\frac{r}{K_j}\right) = \min_{K_{j\in\Omega_r^s}} r \max\left(\frac{K_{ji} - K_i^{\max}}{K_i^{\max}}\right); \quad (5)$$

$$i = \overline{1, m},$$

де $K^{!}\left(\frac{r}{K_j}\right)$ — найбільше з відношень частинних критеріїв, що є координатами вектора $\overrightarrow{K_j}$ від екстремальних значень; Ω_r^s — множина векторів вхідного параметричного ряду, яка задовольняє умову $K_{ji}^{s} \ge K_{j1} \ge K_r^0$. Тут K_{ji}^{s} — найбільш значущий частинний критерій оптимальної (у розумінні мінімаксного критерію) СЗІ.

Механізм утворення множин Ω_r^s можна подати таким чином. Спочатку розв'язують задачу (5) на інтервалі $\left[K_{(r-1)1}^{0}, K_{r1}^{0}\right]$, визначаючи першу мінімаксну систему і найбільш значущий критерій, який має значення $K_{j1}^{1}(S=1)$. Відповідна СЗІ (із ряду розглянутих) характеризується мінімаксним відносним відхиленням і щодо сукупності частинних критеріїв. Проте жорсткі обмеження, які накладаються на найбільш значущий параметр СЗІ, у загальному випадку не дозволяють розглядати його як єдиний типорозмір, що задовольняє всі вхідні вимоги. Тому задачу розв'язують повторно на інтервалі $\left[K_{(r-1)1}^{0}, K_{r1}^{0}\right]$ і визначають другу СЗІ, найбільш значущий критерій якої має значення $K_{j1}^{2}(S=2)$. Процес розв'язання задачі (5) триває доти, доки опорний типорозмір не виявиться серед мінімаксних СЗІ або не буде єдиним елементом множини Ω_r^s.

Зрозуміло, що найбільшому значенню змінної S відповідає така кількість типорозмірів, які утворюють на інтервалі $\left(K_{(r-1)1}^{0}, K_{r1}^{0}\right)$ оптимальний параметричний ряд СЗІ. Для формування ряду, що задовольнить увесь діапазон вимог, задачу (5) розв'язують окремо на кожному інтервалі $\left[K_{(r-1)1}^{0}, K_{r1}^{0}\right]$, де $r = \overline{1, R}$.

Висновки

Особливість пропонованої оптимізації полягає в наявності мішаних обмежень на область застосування кожного типорозміру: жорсткі обмеження у вигляді нерівностей накладаються на найбільш значущий параметр СЗІ; на інші параметри накладаються жорсткі обмеження у вигляді відносних втрат, що в процесі оптимізації мінімізуються.

Для створення та експлуатації інтегрованих систем безпеки об'єктів, побудованих на поєднанні перспективних промислових пристроїв і сучасних інформаційних технологій, потрібен збалансований підхід до вибору показників якості всієї системи і окремих її елементів, який дозволить підвищити безпеку використовуваних каналів зв'язку.

Література

1. ***Мамиконов, А. Г.*** *Достоверность, защита и резервирование информации в АСУ / А. Г. Мамиконов, В. В. Кульба, А. Б. Шилков.— М.: Энергоатомиздат, 1986.— 386 с.*

2. ***Сигорский, В. П.*** *Математичний апарат інженера / В. П. Сигорский.— К.: Техніка, 1975.— 768 с.*

Рецензент: доктор техн. наук, професор ***Л. Н. Беркман***, Державний університет телекомунікацій, Київ.

Н. Н. Браиловский, С. В. Козелков, Н. В. Коршун

ОПТИМИЗАЦИЯ ВЫБОРА ПАРАМЕТРОВ КАЧЕСТВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

Предложен критерий выбора параметров качества сложной системы, позволяющий давать обобщенную оценку качества такой системы в диапазоне возможных отклонений значений частных критериев от экстремальных и благодаря этому учитывать степень ухудшения одних параметров за счет улучшения других.

Ключевые слова: оптимизация; система защиты информации; параметры качества; каналы связи.

M. M. Brailovskyi, S. V. Kozelkov, N. V. Korshun

THE CHOICE OPTIMIZATION OF AN INFORMATION PROTECTION SYSTEM QUALITY PARAMETERS IN COMMUNICATION CHANNEL

The selection criterion of compound system quality parameter considering the degree of some parameters worsening owing to improving other is proposed.

Keywords: optimization; information protection system; quality parameters; communication chennel.

ЗВ'ЯЗОК

Наукове видання

Редакційна обробка та коректура
О. П. Бондаренко, Т. В. Ількевич

Комп'ютерна верстка да дизайн
Г. С. Тимченко, О. Ю. Апухтіна

Підписано до друку 25.04.2016 р.
Формат 60×84/8. Папір друкарський.
Гарнітура SchoolBookC, EuropeCond. Наклад 100 прим.

РВЦ Державного університету телекомунікацій
03110, м. Київ, вул. Солом'янська, 7. Тел. 249-25-75
E-mail: *zviaz-ok@ukr.net*