L. Rivest – 1990

12. Sleator, D. D., D. Temperlay, “Parsing English with a Link Grammar”, Technical report CMU-91-196, Carnegie Mellon University, School of Computer Science, October 1991.

Надійшла 19.9.2011 р.

УДК 004.056.5: 518

А.А. КОБОЗЄВА, В.А. МОКРИЦЬКИЙ
Одеський національний політехнічний університет
Р.Г.МЕЛКУМЯН
Київський національний університет

# ОСНОВИ МЕХАНІЧНОЇ МОДЕЛІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

*В роботі запропоновано основи принципово нової моделі захищеної інформаційної системи, заснованої на механічній інтерпретації системи лінійних алгебраїчних рівнянь із залученням теорії збурень, що ніколи не робилося раніше.*

*The paper presents fundamentals of a new model of secure information system based on the interpretation of the mechanical system of linear algebraic equations involving the perturbation that has never been done before.*

Ключові слова: модель системи, захист інформації, система лінійних алгебраїчних рівнянь, теорія збурень.

**Вступ.** Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, перехід до безпаперової технології, збільшення об’ємів оброблюваної інформації й розширення кола користувачів сьогодні призводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем, що спричиняє підвищення актуальності вимоги захищеності будь-якої інформаційної системи.

Проблеми побудови систем захисту інформації (СЗІ) дуже широко обговорюються в сучасних відкритих джерелах [1– 5]. Висновок про необхідність створення системного комплексного підходу до захисту інформації на основі єдиного наукового базису [1, 2] ні в кого не викликає сумнівів. Побудова такого наукового базису неможлива без наявності адекватної математичної моделі СЗІ. Існуючі проблеми при створенні таких моделей добре відомі [1– 8]. Основні з них – це складність і різнорідність інформаційних систем, більшість із яких погано формалізуються, вимагають адаптації безпосередньо в процесі функціонування й управління.

*Метою* роботи є створення основ принципово нової механічної моделі захищеної інформаційної системи.

Як основні математичні інструменти виступають обчислювальна лінійна алгебра, теорія матриць, теорія збурень.

Для досягнення поставленої мети необхідно розв’язати наступні *задачі*:

- обрати механічну інтерпретацію для СЗІ; встановити відповідність між елементами інформаційної системи й параметрами її механічної моделі;
- провести математичну формалізацію механічної моделі;
- формалізувати вимогу стійкості СЗІ стосовно передбачуваних атак у рамках механічної моделі;
- отримати формальні умови стійкості СЗІ до передбачуваного супротивника.

**Формалізація системи захисту інформації.** Як механічну модель захищеної інформаційної системи завдяки аналогіям, що наведені на рис. 1, логічно розглянути пружну статичну систему $S$, закріплену на краях [9], наприклад, стрижень.

Оберемо на пружному стрижні скінченну множину точок, кожна з яких буде відповідати конкретному засобу захисту, наявному в розпорядженні інформаційної системи, які для зручності занумеруємо в порядку зліва направо: $1,2,...,n$. Будемо розглядати прогини $b_1, b_2, ..., b_n$ точок $1,2,...,n$ системи $S$ під впливом сил $x_1, x_2, ..., x_n$, прикладених у цих точках. Тоді $x_1, x_2, ..., x_n$ інтерпретуються як атаки, спрямовані безпосередньо на засоби захисту $1,2,...,n$, а $b_1, b_2, ..., b_n$ – результати впливу атак на засоби захисту.

Припустимо, що

сили, що впливають на стрижень, і переміщення (прогини) його складових перпендикулярні вхідному (недеформованому) положенню стрижня, тобто паралельні між собою, а тому повністю визначаються своїми алгебраїчними величинами (рис. 2);

має місце принцип лінійного накладення сил [9].

Нехай $a_{ik}$ – прогин стрижня в точці $i$ під впливом одиничної сили, прикладеної в точці $k$, або коефіцієнт впливу точки $k$ на $i$, $i,k = \overline{1,n}$. При спільній дії довільних сил $x_1, x_2, ..., x_n$ на стрижень $S$

при зроблених вище припущеннях прогини будуть визначатися формулою:

$$\sum_{k=1}^{n} a_{ik} x_k = b_i, \quad i = \overline{1,n}. \tag{1}$$

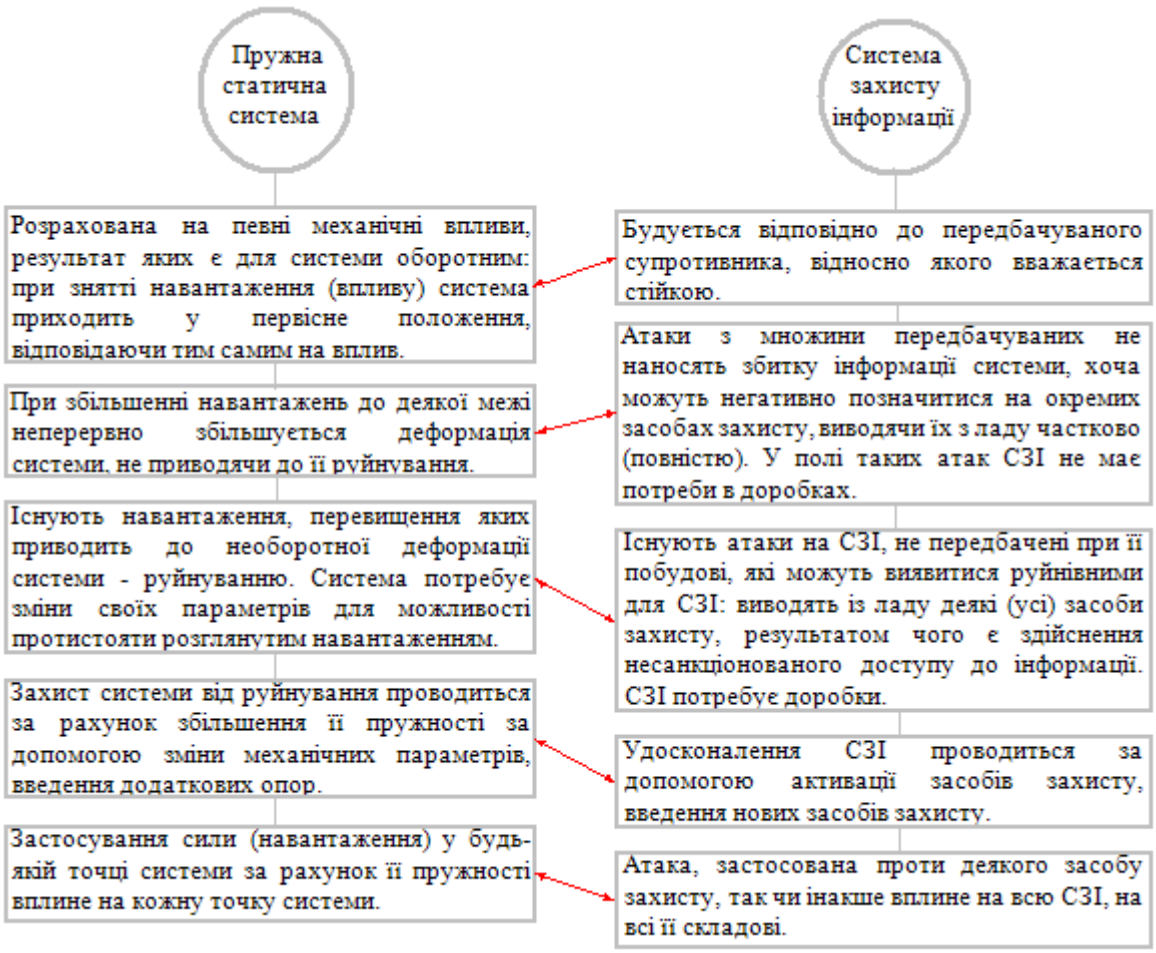


**Рис. 1. Аналогії між властивостями пружної статичної системи й системи захисту інформації**

Ці прогини $b_1, b_2, ..., b_n$ є формальною кількісною інтерпретацією підсумкового стану кожного засобу захисту після спільного проведення атак $x_1, x_2, ..., x_n$ на інформаційну систему.

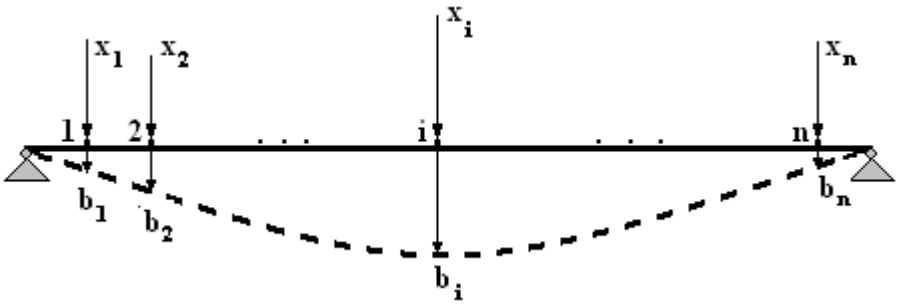


**Рис. 2. Деформація пружного стрижня під впливом зовнішніх сил**

Матричний вид співвідношення (1)

$$Ax = b, \tag{2}$$

де $A$ – $n \times n$ – матриця з елементами $a_{ik}, i,k = \overline{1,n}$, $x, b$ – вектори довжини $n$ з елементами $x_i, b_i, i = \overline{1,n}$ відповідно.

Співвідношення (2) представляє в загальному випадку неоднорідну систему лінійних алгебраїчних рівнянь (СЛАР) щодо невідомих сил, які впливають на стрижень $x_1, x_2, ..., x_n$ при відомих прогинах

$b_1, b_2, ..., b_n$. Припускаючи, що $\det(A) \neq 0$, маємо єдине рішення (2).

Система (2) є формальним представленням СЗІ при використанні пружного стрижня як її механічної інтерпретації. Мовою теорії інформаційного захисту задача про рішення СЛАР (2) може бути інтерпретована наступним чином: визначити кількісні характеристики прояву атак на захищену інформаційну систему, які призведуть до певного стану засобів захисту. В граничному варіанті: визначити максимально можливі прояви атак $x_1, x_2, ..., x_n$, які ще не призведуть до руйнування СЗІ й безпосереднього доступу до інформації, що для задачі про деформацію пружного стрижня зведеться до визначення максимальних впливів, які може витримати стрижень, щоб результат цих впливів був оборотним.

**Умови стійкості системи захисту інформації.** СЗІ будемо називати стійкою стосовно проведеної атаки, якщо в результаті атаки несанкціонований доступ до збереженої інформації не відбувся.

Назвемо задачу, що визначається системою (2), прямою.

Механічною інтерпретацією стійкості СЗІ природно вважати малі пружні зміни в деформації стрижня при порівняно великому збільшенні значень зовнішніх сил, що впливають на стрижень, інакше кажучи, великі збурення $x_1, x_2, ..., x_n$ можуть виникати в результаті малих збурень вхідних даних $b_1, b_2, ..., b_n$. Таким чином, формально вимога стійкості СЗІ буде відповідати вимозі чутливості [10] прямої задачі до збурних дій.

Мірою чутливості будь-якої задачі є її число обумовленості [11]. У випадку задачі про рішення СЛАР це число обумовленості може визначатися як

$$cond(A) = \|A\|\|A^{-1}\|. \tag{3}$$

Дійсно [12], нехай $x$ – точне, $\bar{x}$ – реально отримане, тобто наближене рішення СЛАР (2),

$dx = \bar{x} - x$, $dA, db$

- збурення матриці $A$ і вектора $b$ відповідно. СЛАР (2) представляється у вигляді:

$$(A + dA)(x + dx) = b + db. \tag{4}$$

Враховуючи, що $b = Ax$ і $\det(A) \neq 0$, з (4) випливає:

$$dx = A^{-1}(db - dA\bar{x}),$$

звідки отримуємо:

$$\|dx\| \leq \|A^{-1}\|\left(\|db\| + \|dA\|\|\bar{x}\|\right) = \|A^{-1}\|\|A\|\left(\frac{\|db\|}{\|A\|} + \frac{\|dA\|\|\bar{x}\|}{\|A\|}\right).$$

Оскільки $\bar{x}$ – це рішення неоднорідної системи, то $\|\bar{x}\| \neq 0$. Розділивши останню нерівність на $\|\bar{x}\|$, отримаємо:

$$\frac{\|dx\|}{\|\bar{x}\|} \leq \|A^{-1}\|\|A\|\left(\frac{\|dA\|}{\|A\|} + \frac{\|db\|}{\|A\|\|\bar{x}\|}\right). \tag{5}$$

Тут відносна похибка результату порівнюється з відносною зміною вхідних даних через величину $cond(A)$, яка визначається відповідно до (3).

У силу специфіки отриманої СЛАР (2) будемо вважати, що $dA = 0$, а збурена система (4), для якої $\bar{x}$ є точним рішенням, отримана лише завдяки збуренню вектора правої частини. Дійсно, коефіцієнти матриці $A$ ніяк не залежать від змін в $x, b$, вони визначаються лише коефіцієнтом пружності стрижня (мірою пружності стрижня). Тоді співвідношення (5) стане:

$$\frac{\|dx\|}{\|\bar{x}\|} \leq cond(A)\frac{\|db\|}{\|A\|\|\bar{x}\|},$$

звідки випливає, що малі зміни у векторі прогинів $b$ можуть відповідати великим збуренням у векторі сил $x$ у випадку значної величини $cond(A)$, що для моделюємої СЗІ буде говорити про її стійкість.

При побудові механічної моделі захищеної інформаційної системи природно вважати, що СЗІ буде тим більше стійкою до передбачуваних атак, чим менше будуть коефіцієнти впливу точок відповідного їй пружного стрижня одна на одну, тобто чим менше будуть коефіцієнти матриці системи, чим більше буде коефіцієнт пружності стрижня. Очевидно, при побудові механічної моделі гіпотетично ідеальним з погляду стійкості СЗІ буде варіант, коли $a_{ik} = 0,\ i,k = \overline{1,n}$, тоді всі прогини $b_1, b_2, ..., b_n$ будуть нульовими

незалежно від конкретного прояву сил. У цьому випадку $cond(A) = \infty$. Однак на практиці це очевидно є нереальним.

Якщо $A \neq 0$, але $\det(A) = 0$ ($cond(A) = \infty$), то нульовий вектор $b$ у прямій задачі (2) може відповідати ненульовому вектору сил, які впливають на стрижень $x$, що говоре на користь адекватності запропонованої моделі СЗІ. Дійсно, згаданий випадок є інтерпретацією існування для СЗІ таких атак, вплив яких ніяк не позначиться на засобах захисту й, як наслідок, на самій інформації.

Однак у реальних умовах для стійкої СЗІ логічно припустити, що

$$a_{ik} \approx 0,\ i,k = \overline{1,n}. \qquad (6)$$

З великою ймовірністю при виконанні умов (6) елементи $A$ будуть мало відрізнятися за значеннями. Тоді навіть, якщо $\det(A) \neq 0$, значення визначника може виявитися близьким до нуля. Дійсно, малі відмінності $a_{ik}$ між собою приведуть до малої міри лінійної незалежності між векторами-стовпцями (векторами-рядками) матриці $A$ – малим кутам між ними. Близькість визначника матриці до нуля призведе до великого значення числа обумовленості $cond(A)$, а тому до чутливості прямої задачі до збурних дій..

***Твердження.*** Нехай СЗІ є стійкою до передбачуваних атак, тоді з великою ймовірністю відповідна їй СЛАР (2) буде чутливої до збурних дій.

З врахуванням вищесказаного має місце наступна теорема.

***Теорема.*** Для того, щоб СЗІ при її формальному представленні у вигляді СЛАР (2) була стійкою до передбачуваних атак необхідно й достатньо, щоб пряма задача була чутливою до збурних дій, тобто щоб матриця СЛАР (2) була погано обумовлена: $cond(A) >> 1$.

**Висновки.** Розгляд пружного стрижня як механічної моделі захищеної інформаційної системи є першим кроком на шляху побудови механічної моделі. Більш привабливим щодо цього є розгляд пружної пластини, для якої відповідна система рівнянь може бути отримана, наприклад, з залученням методу скінченних елементів, різних схем змішаного методу скінченних елементів.

На підставі проробленої роботи можна стверджувати, що запропонований новий підхід до питання моделювання СЗІ, заснований на аналогіях між пружною статичною системою й системою інформаційної безпеки, що використовує в якості математичних інструментів матричний аналіз, обчислювальну лінійну алгебру, теорію збурень, є надзвичайно перспективним.

**Література**

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 с.

2. Ленков С.В. Методы и средства защиты информации : в 2 т. / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К. : Арий, 2008.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В.В. – Изд-во : ТИД «ДС», 2001. – 688 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход / Домарев В.В. – Изд-во : ТИД «ДС», 2004. – 992 с.

5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А.А. — М. : Горячая линия – Телеком, 2004. – 280 с.

6. Кобозева А.А. Модель системы защиты информации, основанная на принципах естественной системы управления / А.А. Кобозева, В.А. Хорошко // Захист інформації. – 2007. – С. 56–62.

7. Кобозева А.А. Методика оценки адекватности системы защиты информации / А.А. Кобозева, В.А. Хорошко // Вісник ДУІКТ. – 2007. – № 5 (3). – С. 328–334.

8. Кобозева А.А. Векторная sign-чувствительность как основа геометрической модели системы защиты информации / А.А. Кобозева, В.А. Хорошко // Захист інформації. – 2008. – № 3 – С. 49–57.

9. Гантмахер Ф.Р. Теория матриц / Гантмахер Ф.Р. – М. : Наука, 1988. – 552 с.

10. Деммель Дж. Вычислительная линейная алгебра / Дж. Деммель ; [пер. с англ. Х.Д. Икрамова]. – М. : Мир, 2001. – 430 с.

11. Кобозева А.А. Общий подход к анализу состояния информационных объектов, основанный на теории возмущений / А.А. Кобозева // Вісник Східноукраїнського національного університету ім. В. Даля. – 2008. – № 8 (126), Ч. 1. – С. 72–81.

12. Кобозева А.А. Стеганографический метод, основанный на решении системы линейных алгебраических уравнений / А.А. Кобозева, А.В. Коломийчук // Праці УНДІРТ. – 2006. – № 1 (45)–2 (46). – С. 104–109.

Надійшла 5.9.2011 р.