УДК 681.322 Н.Б. Дахно, Т.В. Майсак, Г.В. Шевченко

АНАЛІЗ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ, ЩО МОДЕЛЮЮТЬСЯ ІНТЕГРО-ДИФЕРЕНЦІЙНИМИ РІВНЯННЯМИ З МАЛОЮ НЕЛІНІЙСТЮ НА ОСНОВІ МОДИФІКОВАНИХ ГРАДІЄНТНИХ МЕТОДІВ

Стаття присвячена актуальному питанню: застосуванню градієнтних методів до розв’язання інтегро-диференціальних рівнянь з малою нелінійністю, за допомогою яких моделюється і аналізується стан захищеності інформаційно-комунікаційних систем і мереж. На основі проведеного аналізу зроблено висновки про достатню ефективність і перспективність застосування модифікованих градієнтних методів до аналізу моделей захисту інформації в нелінійних випадках .

Ключові слова: інформаційно-комунікаційні системи і мережі, варіаційно-градієнтні методи, градієнтні методи, захист інформації, математичні моделі.

Вступ

Цінність інформації в інформаційно-комунікаційних системах і мережах є головним критерієм при прийнятті рішень про її захист. Хоча було зроблено багато різних спроб формалізувати цей процес з використанням методів теорії інформації і аналізу рішень, процес оцінки досі залишається дуже суб'єктивним.

Практика показала, що захищати необхідно не тільки секретну інформацію. Несекретна інформація, піддана несанкціонованим змінам в інформаційно-комунікаційних системах і мережах (наприклад, модифікації команд управління), може привести до витоку або втрати пов’язаної з нею секретної інформації, а також до невиконання системою заданих функцій через отримання помилкових даних, які можуть бути не виявлені користувачем системи.

Процес захисту інформації характеризується великою кількістю і різноманітністю факторів, що впливають на його результат, вплив яких часто описується інтегро-диференціальними рівняннями, що дозволяє розглядати це завдання, як безперервний у часі процес.

Аналіз моделей захисту інформації дозволяє зробити висновки про ефективність опису таких моделей з використанням інтегро-диференціальних рівнянь. Але при описі складних систем з урахуванням багатьох параметрів дуже часто виникають нелінійні системи інтегро-диференціальних рівнянь.

Теорія варіаційно-градієнтних методів добре розроблена для лінійних рівнянь в гільбертовому просторі з позитивно визначеними симетричними операторами [1,2]. Для рівнянь, які не мають такої властивості, теорія варіаційно-градієнтних методів знаходиться на стадії становлення.

В роботах [3,4] обґрунтовано градієнтний метод для нелінійних рівнянь, згідно з яким для побудови наближеного розв’язку необхідно здійснити ітерацію. Для цього необхідно розв’язати нелінійне алгебраїчне або трансцендентне рівняння, що не завжди можливо.

Тому є актуальним розроблення і застосування методів, що дозволять уникнути отримання нелінійних рівнянь та систем для побудови наближень при розгляді та аналізі нелінійних моделей.

Основна частина

1.Застосування модифікованого градієнтного методу до моделей, що характеризуються інтегральними рівняннями з малою нелінійністю для аналізу захищеності інформаційно-комунікаційних систем і мереж.

Будемо розглядати системи захисту інформації в інформаційно-комунікаційних системах і мережах, що описуються математичною моделлю, що породжена виразом з параметром λ :

$$u(x)+\int_a^b A(x,t)u(t)dt+\lambda\int_a^b Q(x,t)F(t,u(t))dt = f(x), \qquad (1)$$

де $f \in L_2([a,b])$.

Інтегральні оператори

$$(Au)(x) = \int_a^b A(x,t)u(t)dt,$$
$$(Fu)(x) = \int_a^b C(x,t)F(t,u(t))dt. \qquad (2)$$

відображають $L_2([a,b])$ в себе. Ядра $A(x,t)$ і $C(x,t)$ є лінійними і симетричними. Оператор A задовольняє умови:

$$\exists \gamma, \delta \in \Re \quad : \quad 0 < \gamma < \delta < \infty \quad \forall u \in L_2([a,b])$$
$$(\gamma - 1)\int_a^b u^2(t)dt \le \int_a^b (Au)(t)u(t)dt \le (\delta - 1)\int_a^b u^2(t)dt. \qquad (3)$$

Дійсна функція $F(x,z)$ задовольняє умову Ліпшиця, тобто

$$\exists L(t) \in L_2([a,b]) \quad : \quad \forall t \in [a,b] \quad y, z \in L_2([a,b])$$
$$\left|F(t,y) - F(t,z)\right| \le L(t)\left|y - z\right| \qquad (4)$$

і виконується умова

$$\exists \beta > 0 \quad : \quad \int_a^b \int_a^b C^2(x,t)L^2(t)dtdx = \beta^2 < \infty, \qquad (5)$$

$$\exists \alpha > 0 \quad : \quad \forall u, v \in L_2([a,b])$$
$$\int_a^b (u(x) - v(x))\int_a^b C(x,t)(F(t,u(t) - F(t,v(t))dtdx \ge \alpha \int_a^b (u(t) - v(t))^2 dt. \qquad (6)$$

При виконанні умов (2) – (6) і $\left|\lambda\right| < \dfrac{2\gamma^{\frac{5}{2}}}{\beta\sqrt{\delta}(\gamma + \delta)}$ рівняння (1) має єдиний розв'язок і виконуються всі умови теореми про збіжність модифікованого градієнтного [5].

Розглядаємо задачу (1). Припустимо, що виконані умови (2) – (6).

Нехай $u_0 \in L_2([a,b])$ довільне початкове наближення, і припустимо, що $(k-1)$-е наближення знайдено. Тоді k - те шукаємо за формулою:

$$u_k(t) = u_{k-1}(t) + \tau_k r_k(t), \quad t \in [a,b], \quad k \ge 1, \qquad (7)$$

де τ_k деякий коефіцієнт, а $r_k(t) = f(t) - u_{k-1}(t) - (Au_{k-1})(t) - \lambda(Fu_{k-1})(t)$ – нев'язка.

Невідомий коефіцієнт τ_k шукаємо з умови мінімуму функціоналу

$$\Phi(u_k) = \int_a^b u_k^2(t)dt + \int_a^b (Au_k)(t)u_k(t)dt -$$
$$-2\int_a^b f(t)u_k(t)dt + 2\lambda\int_a^b (Fu_{k-1})(t)u_k(t)dt. \qquad (8)$$

Після перетворень отримаємо співвідношення для τ_k:

$$\tau_k = \frac{\int_a^b r_k^2(t)dt}{\int_a^b r_k^2(t)dt + \int_a^b (Ar_k)(t)r_k(t)dt}. \qquad (9)$$

Зауважимо, що коли $\lambda = 0$, то градієнтний метод для рівнянь з малою нелінійністю (7) – (9) вироджується в звичайний градієнтний метод найскорішого спуску для лінійного випадку [6].

2. Застосування модифікованого градієнтного методу до моделей, що описуються інтегро-диференційними рівняннями з малою нелінійністю і з К-позитивно визначеним К-симетричним оператором для аналізу захищеності інформаційно-комунікаційних систем і мереж.

Введемо до розгляду інтегро-диференційні оператори

$$(Au)(t) = u^{(n)}(t) + a_1(t)u^{(n-1)}(t) + ... + a_{n-1}(t)u(t) + \\ + \sum_{i=1}^{n} \int_a^b A_i(x,\xi)u^{(i)}(\xi)d\xi, \tag{10}$$

$$(Fu)(t) = \sum_{i=1}^{n} \int_a^b C_i(t,\xi)F_i(\xi, u(\xi))d\xi, \tag{11}$$

визначені на щільній в $L_2([a,b])$ множині $D(A) = \{u : u^{(n)} \in L_2([a,b]),\quad U_l = \sigma_l,\quad l = \overline{1,n-1}\}$, де $a_i \in C([a,b])$, $i = \overline{1,n-1}$ і

$$U_l(u) = \sum_{i=1}^{n-1} (\alpha_{li}u^{(i)}(a) + \beta_{li}u^{(i)}(b)), \qquad l = \overline{0,n-1}, \tag{12}$$

де α_{li}, β_{li} сталі числа.

Будемо розглядати модель захищеності інформації в інформаційно-комунікаційних мережах, що описується крайовою задачею, яка породжена інтегро-диференційним виразом з параметром λ:

$$(Au)(t) + \lambda(Fu)(t) = f(t), \quad f \in L_2([a,b]), \tag{13}$$

$$U_l(u) = 0, \qquad l = \overline{0,n-1}. \tag{14}$$

Вважаємо, що оператор *A* є *K*-позитивно визначеним *K*-симетричним, тобто існує оператор $K : D(K) \to L_2([a,b])$ вигляду:

$$(Ku)(t) = u^{(m)}(t) + k_1(t)u^{(m-1)}(t) + ... + k_{m-1}u(t) + \\ + \sum_{i=1}^{m-1} \int_a^b K_i(t,\xi)u^{(i)}(\xi)d\xi, \quad t \in [a,b],\ m \le n, \tag{15}$$

$$U_l(u) = \sigma_l, \qquad l = \overline{0,m-1}.$$

такий, що виконуються умови

$$\exists \mu, \nu > 0 \ : \ \int_a^b (Au)(t)(Ku)(t)dt \ge \mu \int_a^b u^2(t)dt, \quad \forall u \in D(A), \tag{16}$$

$$\int_a^b (Ku)^2(t)dt \le \nu \int_a^b (Au)(t)(Ku)(t)dt, \quad \forall u \in D(A), \tag{17}$$

$$\int_a^b (Au)(t)(Kv)(t)dt = \int_a^b (Av)(t)(Ku)(t)dt, \quad \forall u, v \in D(A). \tag{18}$$

Нехай існує лінійний оператор $B : D(B) \to L_2([a,b])$ і $D(B) = D(A)$:

$$(Bu)(t) = u^{(n)}(t) + b_1(t)u^{(n-1)}(t) + ... + b_{n-1}u(t) + \sum_{i=1}^{n-1} \int_a^b B_i(t,\xi)u^{(i)}(\xi)d\xi, \tag{19}$$

де b_i сталі числа.

Оператор *B* є *K*-позитивно визначеним і *K*-симетричним.

Вважаємо, що справедлива нерівність:

$$\exists \gamma, \delta > 0 \ : \ \gamma < \delta < \infty, \quad \forall u \in D(A)$$

$$(\gamma - 1)\int_a^b (Bu)(t)(Ku)(t)dt \le \int_a^b (Au)(t)(Ku)(t)dt \le (\delta - 1)\int_a^b (Bu)(t)(Ku)(t)dt. \tag{20}$$

Оператор F – нелінійний і задовольняє умови:

$$\exists \alpha > 0 \ : \ \int_a^b ((Fu)(t) - (Fv)(t))K(u(t) - v(t))dt \ge$$
$$\ge \alpha \int_a^b (B(u(t) - v(t))K(u(t) - v(t))dt, \quad \forall u, v \in D(F), \tag{21}$$

$$\exists \beta > 0 \ : \ \int_a^b ((Fu)(t) - (Fv)(t))K(u(t) - v(t))dt \le$$
$$\le \beta \int_a^b (B(u(t) - v(t))K(u(t) - v(t))dt, \quad \forall u, v \in D(F). \tag{22}$$

При виконанні умов (16) – (22) і $|\lambda| < \dfrac{2\gamma^{5/2}}{\beta\sqrt{\delta}(\delta + \gamma)}$ модель (13) – (14) має єдиний розв'язок і виконуються всі умови теореми про збіжність модифікованого градієнтного методу для рівнянь з малою нелінійністю і з К-позитивно визначеним К-симетричним оператором [7].

Розглядаємо задачу (13) – (14). Припускаємо, що виконані умови (16) – (22) і $|\lambda| < \dfrac{2\gamma^{5/2}}{\beta\sqrt{\delta}(\delta + \gamma)}$. Застосуємо до задачі (13) – (14) модифікований градієнтний метод. Візьмемо $u_0 \in D(A)$ довільне початкове наближення, і припустимо, що $(k-1)$-е наближення знайдено. Тоді k-те шукаємо за формулою:

$$(Bu_k)(t) = (Bu_{k-1})(t) + \tau_k r_k(t), \quad t \in [a,b], \quad k \ge 1, \tag{23}$$

де $r_k(t) = f(t) - (Au_{k-1})(t) - \lambda(Fu_{k-1})(t)$ – нев'язка, а τ_k деякий параметр, який визначається з умови мінімуму функціоналу:

$$\Phi(u_k) = \int_a^b (Au_k)(t)(Ku_k)(t)dt - 2\int_a^b f(t)(Ku_k)(t)dt +$$
$$+2\lambda \int_a^b (Fu_{k-1})(t)(Ku_k)(t)dt. \tag{24}$$

Оскільки оператор B має обернений, існує функція Гріна для задачі:

$$\begin{gathered}(BR_k)(t) = r_k(t), \quad t \in [a,b], \\ U_l(R_k) = 0, \quad k \ge 1.\end{gathered} \tag{25}$$

Тобто

$$R_k(t) = \int_a^b G(t,\xi) r_k(\xi) d\xi \tag{26}$$

і вираз (23) можна переписати у вигляді

$$u_k(t) = u_{k-1}(t) + \tau_k R_k(t), \quad t \in [a,b]. \tag{27}$$

З умови мінімуму функціоналу (24) після перетворень з урахуванням (26) – (27) маємо співвідношення для визначення параметра τ_k :

$$\tau_k = \frac{\int_a^b R_k(t)(Kr_k)(t)dt}{\int_a^b (AR_k)(t)(KR_k)(t)dt}.$$

Висновки

Модифікований градієнтний метод застосовано до рівнянь з малою нелінійністю. Отриманий модифікований градієнтний метод поширено на рівняння з малою нелінійністю і *K*-позитивно визначеними *K*-симетричними операторами. При застосуванні зазначених методів до нелінійних рівнянь отримаємо співвідношення для визначення невідомого параметру за допомогою якого будується наближення. На основі проведеного аналізу можемо зробити висновки про достатню ефективність застосування модифікованих градієнтних методів до аналізу моделей захисту інформації в нелінійних випадках. Модифіковані градієнтні методи дають змогу розв'язувати більш широкий клас задач для захисту інформації в інформаційно-комунікаційних системах і мережах.

Література

1. Лучка А. Ю. Возникновение и развитие прямых методов математической физики / А. Ю. Лучка, Т. Ф. Лучка. – К.: Наукова думка, 1985. – 239 с.
2. Хорошко В.О. Аналіз математичних моделей інформаційно-комунікаційних систем і мереж щодо захисту інформації на основі теорії варіаційно-градієнтних методів / В.О. Хорошко, Т.В. Майсак, Н.Б. Дахно // Моделювання та інформаційні системи в економіці: зб. наук. пр. – К. : КНЕУ, 2015. – № 91. – С. 246 – 255.
3. Вайнберг М. М. Вариационные методы исследования нелинейных операторов / М. М. Вайнберг. – Москва: Гос. издат. технико-теоретической литературы, 1956. – 345 с.
4. Гаевский Х., Грёгер К., Захариас К. Нелинейные операторные уравнения и операторные дифференциальные уравнения. М., 1978.
5. Дахно Н. Б. Застосування модифікованого градієнтного методу до операторних рівнянь з малою нелінійністю для аналізу захищеності інформаційних структур / Н. Б. Дахно // Вісник ДУІКТ. – К. : ДУІКТ, 2009. – Том 7(4). – С. 323 – 327.
6. Канторович Л. В. Функциональный анализ / Л. В. Канторович, Г. П. Акилов. – 3-є изд., перераб. – Москва: Наука. Главная редакция физико-математической литературы, 1984. – 752 с.
7. Дахно Н. Б. Модифікований градієнтний метод для *K*-позитивно визначених *K*-симетричних операторів в системах підтримки прийняття рішень для управління безпілотними літальними апаратами / Н. Б. Дахно // Системи обробки інформації: збірник наукових праць. – Харків : Харківський університет Повітряних Сил імені Івана Кожедуба, 2015. – Вип. 11(136). – С. 23 – 28.

Надійшла 10.03.2017 р. Рецензент: д.т.н., проф. Дудикевич В.Б.