3. Економічний аналіз і діагностика стану сучасного підприємства : навч. посібник / Й. Д. Костено, Є. О. Пыдгора, В. С. Рижиков, В. А. Панков, А. А. Герасимов, В. В. Ровенська. — К., 2005. — 400 с.

4. *Манів З.О.* Економіка підприємства : нав. посібник / З. О. Манів, І. М. Луцький. — К. : Знання, 2004. — 580 с.

5. *Новак В.* Інформаційне забезпечення менеджменту : навч. посібник / В. Новак, Л. Макаренко, М. Луцький // Мін-во освіти і науки України ; Нац. авіаційний ун-т ; Ін-т економіки та менеджменту. — К. : Кондор, 2007. — 462 с.

Хорошко В. О., д.т.н., проф.,
Національний авіаційний університет
Майсак Т. В., к.т.н., доц.,
КНЕУ імені Вадима Гетьмана
Дахно Н. Б., ст. викл.,
ДУТ, Україна

МАТЕМАТИЧНІ МОДЕЛІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ТЕОРІЇ ВАРІАЦІЙНО-ГРАДІЄНТНИХ МЕТОДІВ

АНОТАЦІЯ. Стаття присвячена актуальному питанню: застосуванню варіаційно-градієнтного підходу до розв'язання систем інтегро-диференціальних рівнянь, за допомогою яких моделюється і аналізується стан захищеності інформаційно-комунікаційних систем і мереж. Результати досліджень показують достатньо високу швидкість збіжності цих методів.

КЛЮЧОВІ СЛОВА. інформаційно-комунікаційні системи і мережі, варіаційно-градієнтні методи, аналіз захисту інформації.

АННОТАЦИЯ. В статье рассматривается актуальный вопрос: применение вариационно-градиентного подхода к решению систем интегро-дифференциальных уравнений, с помощью которых моделируется и анализируется состояние защиты информационно-коммуникационных систем и сетей. Результаты исследований показывают достаточно хорошую скорость сходимости этих методов.

ABSTRACT. The article is devoted to the question: usage variation-gradient approach for solving systems of integro-differential equations, which is modeled and analyzed the state of security of ICT systems and networks. The results of the studies show a high rate of convergence of these methods.

Вступ. Бурхливий розвиток техніки, технологій і програмного забезпечення в останні десятиліття призвів до такої ситуації: при досить складних розробках і великих витратах на їх фінансування часто стає вигіднішим витратити певну суму для добування існуючої технології, ніж на розробку власної. Тому це викликало більш бурхливий розвиток технічних пристроїв і систем шпигування [2]. Відповідно зростає роль захисту інформації в інформаційно-комунікаційних структурах, зокрема, в телекомунікаційних системах і мережах: у відомчих системах зв'язку і передавання даних, у радіотехнічних і системах загального користування.

Для дослідження інформаційно-комунікаційної системи або мережі будь-якого складного об'єкта, або явища будують різноманітні математичні моделі. При цьому стан безпеки інформації в будь-яких системах і мережах давно став однією із найважливіших розглядуваних характеристик.

Розробка методів і засобів, що забезпечують ефективність захисту, пов'язана з реалізацією різного виду оцінок для аналізу захищеності інформації. Захист інформації в інформаційно-комунікаційних структурах може бути ефективним лише у випадку, якщо він буде здійснюватись як неперервний і керований процес. Для цього потрібні, з одного боку, механізми безпосереднього захисту інформації, а з другого — механізми управління механізмами безпосереднього захисту. Ці механізми описуються за допомогою інтегро-диференціальних рівнянь. 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 виникають великі системи інтегро-диференціальних рівнянь.

Тому в зв'язку з цим постає завдання швидкого та ефективного розв'язання інтегро-диференціальних рівнянь та їх систем. У класичному аналізі розроблено багато прийомів знаходження розв'язків таких рівнянь за допомогою елементарних (або спеціальних) функцій. Але часто при розв'язанні практичних задач ці методи виявляються або геть безпорадними, або надто витратними в часі. З цієї причини для розв'язання задач практики були створені методи наближеного розв'язку диференціальних рівнянь [1].

Серед великої кількості цих методів найчастіше на практиці застосовують варіаційні, проекційні, градієнтні та різницеві методи. Останнім часом усе частіше застосовуються підходи, які суттєво прискорюють швидкість збіжності градієнтних методів, мають більш широку область застосування і більш стійкі до збу-

рень. Ці підходи об'єднують ідеї як варіаційних, так і градієнтних методів, як, наприклад, варіаційно-градієнтний метод для лінійних рівнянь [3].

1. Застосування однокрокового варіаційно-градієнтного методу до лінійних рівнянь з *K*-позитивно визначеним *K*-симетричним оператором для аналізу захищеності інформаційно-комунікаційних систем і мереж

Будемо розглядати системи захисту інформації в інформаційно-комунікаційних системах і мережах, що описуються рівняннями або системами рівнянь вигляду

$$Au = f, \quad f \in H. \tag{1}$$

Оператор $A : D(A) \to H$ визначено на щільній в H множині $D(A)$, H деякий гільбертів простір і $H_0 \subset D(H) \subset H$ деякий підпростір. Оператор A є лінійним, K-позитивно визначеним і K-симетричним, тобто існує оператор $K : D(K) \to H$ і $D(K) \subset D(A)$, що допускає замикання, такий, що

$$\exists \alpha, \beta > 0 : (Au, Ku) \geq \alpha \|u\|^2, \ \forall u \in D(A); \tag{2}$$

$$\|Ku\|^2 \leq \beta (Au, Ku), \ \forall u \in D(A); \tag{3}$$

$$(Au, Kv) = (Ku, Av), \ \forall u, v \in D(A). \tag{4}$$

Припустимо, що існує лінійний K-позитивно визначений і K-симетричний оператор $B : D(B) \to H$ і $D(B) = D(A)$, для якого просто побудувати обернений.

Нехай виконується умова

$$\begin{aligned} &\exists \gamma, \delta > 0 : 0 < \gamma \leq \delta < \infty, \forall u \in D(A), \\ &\gamma (Bu, Ku) \leq (Au, Ku) \leq \delta (Bu, Ku). \end{aligned} \tag{5}$$

При виконанні умов (2) — (5) рівняння (1) має єдиний узагальнений розв'язок, що рівносильно знаходженню мінімуму функціоналу

$$F(u) = (Au, Ku) - 2(f, Ku). \tag{6}$$

Нехай $u_0 \in D(A)$ — довільне початкове наближення. Припустимо, що $(k-1)$-е наближення знайдено, тоді k-те шукаємо за схемою

$$u_k = x_k + w_k, \ w_k \in H_0, \tag{7}$$

в якій елемент x_k визначається з рівняння

$$Bx_k = Bu_{k-1} + \tau_k(f - Au_{k-1}), \tag{8}$$

де τ_k деякий параметр.

Невідомі τ_k і w_k знаходимо з умови мінімуму функціоналу (6).

Оскільки B має обернений, метод (7) — (8) можна переписати у вигляді

$$u_k = u_{k-1} + \tau_k B^{-1} r_k + w_k, \tag{9}$$

де $r_k = f - Au_{k-1}$ — нев'язка.

Після перетворень з урахуванням формул (7)–(9) матимемо співвідношення

$$(Au_k, KB^{-1}r_k) = (f, KB^{-1}r_k); \tag{10}$$

$$(r_k - \tau_k AB^{-1}r_k - Aw_k, Kv) = 0, \ \forall v \in H_0. \tag{11}$$

Формули (10)–(11) можна переписати у такому вигляді:

$$\tau_k(AB^{-1}r_k, KB^{-1}r_k) + (Aw_k, KB^{-1}r_k) = (r_k, KB^{-1}r_k);$$

$$\tau_k(AB^{-1}r_k, Kv) + (Aw_k, Kv) = (r_k, Kv), \ \forall v \in H_0.$$

Звертаємо увагу, що

$$(r_k, Kv) = 0, \ k \geq 2.$$

Це випливає з того, що $r_{k+1} = f - Au_k = f - A(u_{k-1} + \tau_k B^{-1} r_k + w_k) =$ $= r_k - \tau_k AB^{-1}r_k - Aw_k$ і з системи (11).

2. Застосування двокрокового варіаційно-градієнтного методу для лінійних рівнянь з *K*-позитивно визначеним *K*-симетричним оператором для аналізу захищеності інформаційно-комунікаційних систем і мереж.

Розглядаємо математичну модель захисту інформації в інформаційно-комунікаційних системах і мережах, що описується рівнянням вигляду

$$Au = f, \ f \in H. \tag{12}$$

Оператор $A : D(A) \to H$ визначено на щільній в H множині $D(A)$, є лінійним K-позитивно визначеним і K-симетричним, тобто існує оператор $K : D(K) \to H$ і $D(K) \subset D(A)$, який допускає замикання в H, і такий, що

$$\exists \alpha, \beta > 0 : (Au, Ku) \geq \alpha \|u\|^2, \ \forall u \in D(A); \tag{13}$$

$$\|Ku\|^2 \leq \beta(Au, Ku), \ \forall u \in D(A); \tag{14}$$

$$(Au, Kv) = (Ku, Av), \ \forall u, v \in D(A). \tag{15}$$

Припустимо, що існує лінійний K-позитивно визначений і K-симетричний оператор $B : D(B) \to H$ і $D(B) = D(A)$, для якого просто побудувати обернений B^{-1}

$$\exists \gamma, \delta > 0 : 0 < \gamma \le \delta < \infty, \forall u \in D(A),$$
$$\gamma(Bu, Ku) \le (Au, Ku) \le \delta(Bu, Ku). \tag{16}$$

При виконанні умов (13) — (16) рівняння (12) має єдиний узагальнений розв'язок і, як відомо, його розв'язання рівносильне знаходженню мінімуму функціоналу

$$F(u) = (Au, Ku) - 2(f, Ku).$$

Розглянемо рівняння (12) і припустимо виконання умов (13)–(16).

Нехай H_0 деякий гільбертів підпростір такий, що $H_0 \subset D(A) \subset H$ і $u_0 \in D(A)$ — довільне початкове наближення. Припустимо, що k-е наближення знайдено, тоді такі наближення знаходяться за схемою

$$u_k = x_k + w_k, \ \ w_k \in H_0, \tag{17}$$

в якій елемент x_k визначається з рівняння

$$Bx_k = Bu_k + \alpha_k B\delta_k + \beta_k r_k, \tag{18}$$
$$Bx_0 = Bu_0 + \beta_0 r_0, \tag{19}$$

де $\delta_k = u_k - u_{k-1}$, $r_k = f - Au_k$ — нев'язка.

Невідомі параметри α_k, β_k та елемент w_k знаходимо з умови мінімуму функціоналу

$$F(u_{k+1}) = (Au_{k+1}, Ku_{k+1}) - 2(f, Ku_{k+1}).$$

Оскільки B має обернений, метод (17)–(19) можна переписати у вигляді

$$u_{k+1} = u_k + \alpha_k \delta_k + \beta_k B^{-1} r_k + w_k; \tag{20}$$
$$u_1 = u_0 + \beta_0 B^{-1} r_0 + w_0. \tag{21}$$

Перше наближення шукається згідно з однокроковим варіаційно — градієнтним методом. Для наступних наближень, після перетворень з урахуванням формул (20)–(21), отримаємо співвідношення для визначення невідомих параметрів α_k, β_k та поправки w_k при $k \ge 1$:

$$\alpha_k(A\delta_k, K\delta_k) + \beta_k(AB^{-1}r_k, K\delta_k) + (Aw_k, K\delta_k) = (r_k, K\delta_k),$$
$$\alpha_k(A\delta_k, KB^{-1}r_k) + \beta_k(AB^{-1}r_k, KB^{-1}r_k) + (Aw_k, KB^{-1}r_k) = (r_k, KB^{-1}r_k),$$

$$\alpha_k(A\delta_k, Kv) + \beta_k(AB^{-1}r_k, Kv) + (Aw_k, Kv) = (r_k, Kv), \ \ \forall v \in H_0. \quad (22)$$

Побудуємо початкове наближення u_0 таким чином:

$$u_0 = u_{-1} + w_{-1},$$

де $u_{-1} \in D(A)$ довільний елемент , а $w_{-1} \in H_0$ знаходимо з умови

$$(f - Au_{-1}, Kv) = 0, \quad \forall v \in H_0. \quad (23)$$

Перепишемо (23) у вигляді

$$(f - Au_{-1}, Kv) = (Aw_{-1}, Kv), \quad \forall v \in H_0. \quad (24)$$

З рівняння (24) легко бачити, що при $u_{k-1} = 0$ за початкове наближення можна взяти елемент, побудований за методом Рітца.

Звертаємо увагу, що

$$(r_k, Kv) = 0, \ \ k \geq 0, \ \ \forall v \in H_0. \quad (25)$$

Для $k = 0$ це випливає з рівності (23). Для $k = 1$ з однокрокового варіаційно-градієнтного методу. При $k \geq 2$ з визначення r_k та (20) маємо

$$r_{k+1} = r_k - \alpha_k A\delta_k - \beta_k AB^{-1}r_k - Aw_k. \quad (26)$$

З формули (26) і системи (22) бачимо, що (25) виконується для всіх $k \geq 2$.

3. Застосування модифікованого градієнтного методу для операторних рівнянь з малою нелінійністю для аналізу захищеності інформаційно-комунікаційних систем і мереж.

Великий клас математичних моделей захисту інформації в інформаційно-комунікаційних системах і мережах описується нелінійними рівняннями. Однак розв'язання таких рівнянь пов'язане з багатьма складностями. Дуже часто для побудови ітерації потрібно розв'язати нелінійне алгебраїчне або трансцендентне рівняння, що не завжди можливо. Тому виникла задача побудови методів для розв'язання нелінійних рівнянь, які зводяться до побудови ітерації і розв'язання лінійних алгебраїчних рівнянь.

Будемо розглядати системи захисту інформації в інформаційно-комунікаційних системах і мережах, що описуються рівняннями або системами рівнянь вигляду:

$$Au + \lambda Fu = f, \ \ f \in H, \quad (27)$$

де λ — деякий параметр, H — гільбертів простір, оператор $A : H \to H$ є лінійним позитивно визначеним обмеженим і симетричним, тобто виконуються умови

$$\exists \gamma, \delta > 0 : \gamma < \delta < \infty, \quad \forall u \in H$$
$$\gamma \|u\|^2 \le (Au, u) \le \delta \|u\|^2, \tag{28}$$

$$\forall u, v \in H \quad (Au, v) = (u, Av). \tag{29}$$

Оператор $F : H \to H$ є нелінійний монотонний і Ліпшиць-неперервний, тобто

$$\exists \alpha, \beta > 0 : \forall u, v \in H$$
$$\|Fu - Fv\| \le \beta \|u - v\|, \tag{30}$$

$$(Fu - Fv, u - v) \ge \alpha \|u - v\|^2. \tag{31}$$

При виконанні умов (28)–(31) рівняння (27) має єдиний розв'язок [Грегер].

Розглянемо рівняння (27) і припустимо, що виконано умови (28)–(31).

Нехай $u_0 \in H$ довільне початкове наближення. Припустимо, що (k – 1)-е наближення знайдено. Тоді k-те шукаємо за схемою

$$u_k = u_{k-1} + \tau_k r_k, \tag{32}$$

де τ_k деякий параметр, а

$$r_k = f - Au_{k-1} - \lambda F u_{k-1}. \tag{33}$$

Невідомий параметр τ_k знаходимо з умови мінімуму функціоналу:

$$\Phi(u_k) = (Au_k, u_k) - 2(f, u_k) + 2\lambda (Fu_{k-1}, u_k). \tag{34}$$

Після перетворень з формул (32), (33) і (34), отримаємо співвідношення для τ_k:

$$\tau_k = \frac{(r_k, r_k)}{(Ar_k, r_k)}. \tag{35}$$

Теорема 1. Якщо в рівнянні (27) оператори A і F задовольняють умови (28)–(31), параметр $|\lambda| < \frac{2\gamma}{\gamma + \delta} \cdot \frac{\gamma}{\beta} \sqrt{\frac{\gamma}{\delta}}$, то наближення побудоване градієнтним методом (32)–(35) збігається до розв'язку рівняння (27) і швидкість збіжності характеризується оцінкою:

$$\|u^* - u_k\| \le \eta q^k \|u^* - u_0\|, \quad k \ge 1,$$

$$\eta = \frac{\delta + \lambda\beta}{\gamma + \lambda\alpha}, \quad q = \rho + |\lambda| \frac{\beta}{\gamma} \sqrt{\frac{\delta}{\gamma}}, \quad \rho = \frac{\delta - \gamma}{\delta + \gamma}.$$

4. Застосування градієнтного методу для операторних рівнянь з малою нелінійністю і *K*-позитивно визначеним *K*-симетричним оператором для аналізу захищеності інформаційно-комунікаційних систем і мереж.

Розглядаємо математичну модель захисту інформації в інформаційно-комунікаційних системах і мережах, що описується рівнянням вигляду

$$Au + \lambda Fu = f, \quad f \in H, \tag{36}$$

де λ — деякий параметр, H — гільбертів простір, оператор $A : D(A) \to H$ визначений на щільній в H множині є лінійним K-позитивно визначеним і K-симетричним. Тобто, існує оператор $K : D(K) \to H$, $D(K) \subset D(A)$, що допускає замикання, такий, що

$$\exists \mu, \upsilon > 0 : (Au, Ku) \geq \mu \|u\|^2, \ \forall u \in D(A), \tag{37}$$

$$\|Ku\|^2 \leq \upsilon (Au, Ku), \ \forall u \in D(A), \tag{38}$$

$$(Au, Kv) = (Av, Ku), \ \forall u, v \in D(A). \tag{39}$$

Припустимо, що існує лінійний K-позитивно визначений і K-симетричний оператор $B : D(B) \to H$ і $D(B) = D(A)$, для якого просто побудувати обернений.

Нехай виконується умова

$$\begin{aligned} &\exists \gamma, \delta > 0 : 0 < \gamma < \delta < \infty, \ \forall U \in D(A) \\ &\gamma (Bu, Ku) \leq (Au, Ku) \leq \delta (Bu, Ku). \end{aligned} \tag{40}$$

Оператор $F : D(F) \to H$ визначений на щільній в H множині, причому $D(A) \subset D(F)$ є нелінійний K-монотонний K-Ліпшиць-неперервний, тобто виконуються умови

$$\begin{aligned} &\exists \alpha, \beta > 0 : \forall u, v, h \in D(F) \\ &\left|(Fu - Fv, K(u - v))\right| \geq \alpha (B(u - v), K(u - v)), \end{aligned} \tag{41}$$

$$\left|(Fu - Fv, K(u - v))\right| \leq \beta (B(u - v), K(u - v)). \tag{42}$$

При виконанні умов (37)–(42) рівняння (36) має єдиний узагальнений розв'язок.

Розглядаємо рівняння (36) і припускаємо, що виконано (37)–(42).

Нехай $u_0 \in D(A)$ — довільне початкове наближення. Припустимо, що $(k-1)$-е наближення знайдено, тоді наступні шукаємо за схемою

$$Bu_k = Bu_{k-1} + \tau_k r_k, \tag{43}$$

де τ_k деякий параметр, а r_k — нев'язка

$$r_k = f - Au_{k-1} - \lambda F u_{k-1}. \tag{44}$$

Невідомий параметр τ_k знаходимо з умови мінімуму функціоналу

$$\Phi(u_k) = (Au_k, Ku_k) - 2(f, Ku_k) + 2\lambda(Fu_{k-1}, Ku_k). \tag{45}$$

Оскільки оператор B має обернений, то (43) можна переписати у вигляді

$$u_k = u_{k-1} + \tau_k B^{-1} r_k. \tag{46}$$

З умови мінімуму функціоналу (45), враховуючи (46) отримаємо співвідношення для визначення τ_k:

$$\tau_k = \frac{(B^{-1}r_k, Kr_k)}{(AB^{-1}r_k, KB^{-1}r_k)}. \tag{47}$$

Обґрунтування методу. На множині $D(B)$ задамо новий скалярний добуток

$$[u, v] = (Bu, Kv), \quad u, v \in D(B). \tag{48}$$

Тоді для (48) будуть виконуватись всі аксіоми скалярного добутку, і лінійну множину $D(B)$ можна розглядати, як дійсний гільбертів простір. Будемо називати замикання множини $D(B)$ в сенсі метрики (48) енергетичним простором H_B. Норму елементу u в просторі H_B будемо позначати через $|u|_2$, так, що

$$|u|_B^2 = [u, u], \ u \in D(B). \tag{49}$$

Теорема 2. Якщо в рівнянні (36) оператори A і F задовольняють умови (37)–(42), параметр $|\lambda| < \dfrac{2\gamma^{\frac{5}{2}}}{\beta\sqrt{\delta}(\gamma+\delta)}$, то градієнтний метод (43)–(47) збігається і швидкість збіжності характеризується оцінкою

$$|u^* - u_k|_B \le \eta q^k |u^* - u_0|_B, \ k \ge 1, \tag{50}$$

$$\eta = \frac{\delta + \lambda\beta}{\gamma + \lambda\alpha}, \ q = \rho + |\lambda| \frac{\beta\sqrt{\delta}}{\gamma^{\frac{3}{2}}}, \ \rho = \frac{\delta - \gamma}{\delta + \gamma}. \tag{51}$$

Висновки. Варіаційно-градієнтні методи збігаються краще, ніж відомі градієнтні методи (зокрема, метод найскорішого спуску) і не потребують знання меж спектра оператора. Тому застосування їх до задач захисту інформації в інформаційно-комунікаційних системах і мережах є актуальним і перспективним.

Література

1. *Гаевский Х.* Нелинейные операторные уравнения и операторные дифференциальные уравнения / Гаевский Х., Грёгер К., Захариас К. — М., 1978.
2. *Герасименко В.А.* Основы защиты информации / В. А. Герасименко, А. А. Малюк. — М.: МИФИ, 1997. — 537 с.
3. *Лучка А.Ю.* Вариационно-градиентный метод / Лучка А.Ю., Нощенко О.Э., Тухалевская Н.И. // Журнал вычислительной математики и математической физики. — 1984. — 24. — № 7. — С. 963-971.

УДК 517.9: 330.42

Неня О. І., к.ф.-м.н.,
доцент, кафедра вищої математики,
Київський національний економічний університет імені Вадима Гетьмана

ПРО РОЗВ'ЯЗОК ФУНКЦІОНАЛЬНО-ДИФЕРЕНЦІАЛЬНОГО РІВНЯННЯ ДИНАМІЧНОЇ МОДЕЛІ РОЗВИТКУ ПІДПРИЄМСТВА

АНОТАЦІЯ. У публікації досліджено проблему побудови динамічної моделі розвитку підприємства в умовах кредитування та короткотривалих зовнішніх впливів на виробництво, а також побудови розв'язку функіонально-диференціального рівняння зі змінними коефіцієнтами, несталим запізненням та імпульсною дією, яке описує дану модель.

КЛЮЧОВІ СЛОВА: динамічна система, імпульсне диференціальне рівняння, нелінійне запізнення, фундаментальна функція, спряжене рівняння, асимптотична стійкість, тривіальний розв'язок.

АННОТАЦИЯ. В публикации исследуются проблемы построения динамической модели развития предприятия в условиях кредитирования и коротковременных внешних воздействий на производство, а также построения решения функционально-дифференциального уравнения с переменными коефициентами та импульсным воздействием, которое описывает данную модель.

КЛЮЧЕВЫЕ СЛОВА: динамическая система, импульсное дифференциальное уравнение, нелинейное запаздывание, фундаментальная функция, сопряженное уравнение, асимптотическая устойчивость, тривиальное решение.