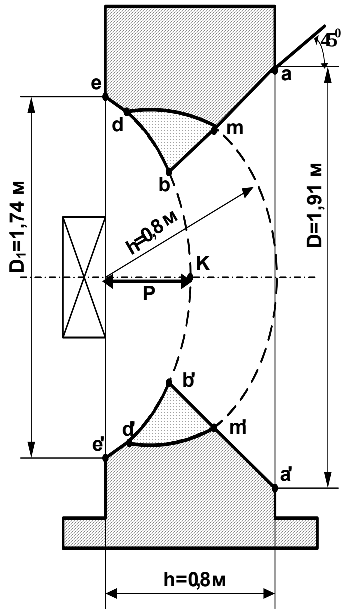


**Рис. 1. Пролом в цегляній стіні**
**abba – відкольна вирва; edbbde- вирва викиду;**
**dbm і dbm – зони руйнування цегли**

**Висновок.** Наведений у статті математичний апарат буде корисним фахівцям піротехнічних підрозділів під час запобігання або ліквідації наслідків надзвичайних ситуацій та надання допомоги комунальним службам при прокладанні мереж.

1. Саламахин Т.М. Основы моделирования и боевая эффективность зарядов разрушения [Текст]: учебное пособие для слушателей академии. Ч. 1 / Т.М. Саламахин – М.: ВИА им. Куйбышева, 1984. – 160 с.
2. Саламахин Т.М. Физические основы механического действия взрыва и методы определения взрывных нагрузок. [Текст]: учебник. / Т.М. Саламахин – М.: ВИА им. Куйбышева, 1974. – 256 с.

**Надійшла до редколегії 21.08.09р**

**УДК 681.3**

**С.В.Лєнков, д-р. техн. наук, проф., В.О. Хорошко, д-р. техн. наук, проф., Н.Б. Дахно, здобувач**

# ОДНОКРОКОВИЙ ВАРІАЦІЙНО-ГРІЄНТНИЙ МЕТОД ЩОДО МАТЕМАТИЧНИХ МОДЕЛЕЙ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ.

***Розглянуто однокроковий варіаційно-градієнтний метод щодо математичних моделей комплексних систем захисту інформації, що описуються інтегро-диференційними рівняннями з $K$ – позитивно визначеними $K$ -симетричними операторами. Велика увага приділена встановленню ознак збіжності, отриманню конструктивних оцінок погрішності, дослідженню швидкості збіжності для рівнянь в операторній формі.***

***Ключові слова: варіаційно-градієнтний метод, оцінка погрішності, захист інформації.***

***The single-step gradient method for a variation concerning mathematical models of complex protection systems of the information that are described by integro-partial differential equations from $K$ – positively defined $K$ -symmetrical operator is considered. The big attention is given an establishment of signs of convergence, reception of a constructive error estimation, research of speed of convergence, for the equations in the operational form.***

***Keywords: gradient for a variation method, an error estimation, information protection.***

**Вступ.** Для опису функціонування та аналізу систем захисту інформації використовують різні математичні моделі. Система захисту інформації все більше перетворюється на інтелектуальну систему, до якої входять системи підтримки прийняття рішень[1].

Серед різноманітних інструментів, що входять до складу систем підтримки прийняття рішень, важливе місце займає математичне моделювання, як основа багатоваріантного прогнозування й аналізу систем високої степені складності.

Суть методу математичного моделювання – в математичному описі процесів, відтворюючого функціонування системи, що вивчається. Даний метод дозволяє аналізувати складні системи захисту інформації.

Опис систем захисту інформації різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів і так далі. Вибір один із способів опису задає конкретний вигляд математичної моделі.

Для більш ефективного аналізу функціонування систем захисту інформації треба враховувати внутрішні та зовнішні фактори впливу. Ми можемо описати систему взаємодії по кожному параметру із зовнішньою та внутрішньою середою диференційним рівнянням. Але так як у нас багато параметрів, то описуючи кожний параметр ми можемо скласти систему диференційних рівнянь, які дозволять отримати повну картину по функціонуванню та технічному стану системи захисту інформації. В звязку з чим доцільно використовувати математичний апарат диференційних рівнянь.

Математична модель дає можливість вивчати явище в цілому, передбачати його розвиток, робити кількісні оцінки змін, що відбуваються в нім з часом. Важно відзначити, що для перевірки правильності математичної моделі дуже важливі теореми існування рішень відповідних диференціальних рівнянь, оскільки математична модель не завжди адекватна конкретному явищу і з існування рішення реальної задачі не випливає існування рішення відповідної математичної задачі.

Розглянемо системи захисту інформації, що моделюються інтегро-диференціальним рівнянням або системою інтегро-диференціальних рівнянь. Тобто обєктом дослідження буде інтегро-диференціальне рівняння.

Для відшукання розвязків диференціальних рівнянь існує багато наближених методів. Серед великої кількості наближених методів найбільш часто на практиці застосовують варіаційні, проекційні, градієнтні, різницеві методи. Останнім часом стали розвиватися підходи, які суттєво прискорюють швидкість збіжності градієнтних методів, мають більш широку область застосування й більш стійки до збурень. Ці підходи поєднують у собі ідеї як варіаційних, так і градієнтних методів. Одним із представників цього класу є варіаційно-градієнтний метод [2].

Для лінійних систем, оператори яких є $K$ - позитивно визначеними $K$ – симетричними будемо застосовувати однокроковий варіаційно-градієнтний метод. Реалізація цього методу зводиться до побудови ітерації й розвязку лінійної алгебраїчної системи рівнянь.

Розглядаємо математичну модель захисту інформації, що описується крайовою задачею, яка породжена диференційним виразом:

$$Au(t) = u^{(m)}(t) + c_1(t)u^{(m-1)}(t) + \ldots + c_m(t)u(t) + \sum_{j=0}^{m}\int_a^b H_j(t,\xi)u^{(j)}(\xi)d\xi = f(t), \quad t \in [a,b], \tag{1}$$

та крайовими умовами:

$$U_l(u) = \sum_{j=0}^{m-1}(\alpha_{lj}u^{(j)}(a) + \beta_{lj}u^{(j)}(b)) = \sigma_l, \qquad l = \overline{0,m-1}, \tag{2}$$

де $\alpha_{lj}$, $\beta_{lj}$, $\sigma_l$ при $0 \le l,j \le m-1$ сталі числа, а $c_i \in C([a,b])$, $i = \overline{i,m}$.

Оператор $A: D(A) \to H$ визначено на щільній в $L_2[a,b]$ множині $D(A) = \{u : u^{(m)} \in L_2[a,b], U_l = 0, \ l = \overline{0,m-1}\}$.

Для зручності розглянемо задачу (1), (2) в загальному операторном вигляді:

$$Au = f, \qquad f \in H, \tag{3}$$

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 замикаємий оператор $K: D(K) \to H$ і $D(K) \subset D(A)$ такий що

$$\exists \alpha, \beta > 0 \ : \ (Au, Ku) \ge \alpha \|u\|^2, \quad \forall u \in D(A); \tag{4}$$

$$\|Ku\|^2 \le \beta(Au, Ku), \quad \forall u \in D(A); \tag{5}$$

$$(Au, Kv) = (Ku, Av), \quad \forall u, v \in D(A). \tag{6}$$

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:

$$\begin{gathered} \exists \gamma, \delta > 0 \ : \ 0 < \gamma \le \delta < \infty, \ \forall u \in D(A), \\ \gamma(Bu, Ku) \le (Au, Ku) \le \delta(Bu, Ku). \end{gathered} \tag{7}$$

При виконанні умов (4) – (7) рівняння (3) має єдиний узагальнений розвязок [10] і, як відомо, розвязання рівняння (3) рівносильне знаходженню мінімуму функціоналу:

$$F(u) = (Au, Ku) - 2(f, Ku) \tag{8}$$

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

$$u_k = x_k + w_k, \qquad w_k \in H_0, \tag{9}$$

в якій елемент $x_k$ визначається з рівняння:

$$Bx_k = Bu_{k-1} + \tau_k(f - Au_{k-1}), \tag{10}$$

де $\tau_k$ деякий параметр.

Невідомі $\tau_k$ і $w_k$ шукаємо з умови мінімуму функціоналу (8).

Оскільки $B$ має обернений, метод (9) – (10) можна переписати у вигляді:

$$u_k = u_{k-1} + \tau_k B^{-1} r_k + w_k, \tag{11}$$

де $r_k = f - Au_{k-1}$ – невязка.

Після перетворень з урахуванням формул (9) – (11) отримуємо співвідношення:

$$(Au_k, KB^{-1}r_k) = (f, KB^{-1}r_k) \tag{12}$$

$$(r_k - \tau_k AB^{-1}r_k - Aw_k, Kv) = 0, \quad \forall v \in H_0. \tag{13}$$

Формули (12) – (13) можна переписати у вигляді:

$$\tau_k(AB^{-1}r_k, KB^{-1}r_k) + (Aw_k, KB^{-1}r_k) = (r_k, KB^{-1}r_k) \tag{14}$$

$$\tau_k(AB^{-1}r_k, Kv) + (Aw_k, Kv) = (r_k, Kv), \quad \forall v \in H_0. \tag{15}$$

Звертаємо увагу, що

$$(r_k, Kv) = 0, \quad k \ge 2. \tag{16}$$

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 (13).

Якщо $H_0$ підпростір породжений системою лінійно незалежних елементів $\{\varphi_i : i \ge 1\} \subset H_0$, поправку $w_k$ шукаємо у вигляді:

$$w_k = \sum_{i=1}^{k} a_i^k \varphi_i \tag{17}$$

де $\{a_i^k \ : \ k \ge 1, 1 \le i \le n\} \subset R$.

Тоді співвідношення (14) і (15) перетворюються у систему лінійно незалежних рівнянь:

$$\tau_k(AB^{-1}r_k, KB^{-1}r_k) + \sum_{i=1}^{n} a_i^k(AB^{-1}r_k, K\varphi_i) = (r_k, KB^{-1}r_k), \tag{18}$$

$$\tau_k(AB^{-1}r_k, K\varphi_i) + \sum_{j=1}^{n} a_j^k(A\varphi_j, K\varphi_i) = (r_k, K\varphi_i), \quad i = \overline{1,n}. \tag{19}$$

З того, що оператор $A$ є $K$ -позитивно визначеним і $K$ -симетричним випливає, що система (18) – (19) має єдиний розвязок відносно $\tau_k$ і $a_i^k$.

Поправку $w_k$ будемо шукати у вигляді:

$$w_k = x_k - \tau_k y_k = \sum_{i=1}^{n}(b_i^k - \tau_k c_i^k)\varphi_i, \tag{20}$$

де невідомі параметри $b_i^k$ та $c_i^k$ визначаються з умов:

$$(Ax_k, K\varphi_i) = (r_k, K\varphi_i), \quad i = \overline{1,n}; \tag{21}$$

$$(Ay_k, K\varphi_i) = (AB^{-1}r_k, K\varphi_i), \quad i = \overline{1,n}; \tag{22}$$

Якщо введену таким чином поправку $w_k$ підставити в систему (14) – (15), то останні $n$ рівнянь перетворяться на тотожність, а перше набуде вигляду:

$$\tau_k(AB^{-1}r_k, KB^{-1}r_k - Ky_k) = (KB^{-1}r_k, r_k - Ax_k). \tag{23}$$

Таким чином, розвязання системи (18) – (19) зводиться до розвязання систем (21) і (22) з однаковою матрицею і рівняння (23) відносно $\tau_k$.

Зауважимо, що після першої ітерації система (21) матиме тільки тривіальний розвязок.

Розглянемо випадок коли початкове наближення знайдено за методом Ріца. Тоді вже при $k = 1$ буде виконуватись умова (16) і система (21) матиме нульовий розвязок при $k \ge 1$. Тобто з формул (11), (16), (20) – (23) алгоритм, що розглядається зводиться до виду:

$$u_k = u_{k-1} + \tau_k(B^{-1}r_k - y_k), \tag{24}$$

$$(Ay_k, K\varphi_i) = (AB^{-1}r_k, K\varphi_i), \quad i = \overline{1,n}. \tag{25}$$

$$\tau_k(AB^{-1}r_k, KB^{-1}r_k - Ky_k) = (KB^{-1}r_k, r_k). \tag{26}$$

З перетворень:

$$(KB^{-1}r_k, Ax_k) = \sum_{i=1}^{n} b_i^k (AB^{-1}r_k, K\varphi_i) = \sum_{i=1}^{n} b_i^k (Ay_k, K\varphi_i) = (Ay_k, Kx_k) = \\ = \sum_{i=1}^{n} c_i^k (Ax_k, K\varphi_i) = \sum_{i=1}^{n} c_i^k (r_k, K\varphi_i) = (r_k, Ky_k). \quad (27)$$

випливає, що виконується формула:

$$(KB^{-1}r_k, Ax_k) = (r_k, Ky_k) \quad (28)$$

Похибки округлення можуть привести до порушення рівності (16), а тому краще користуватись схемою (11), (20) – (23).

В цій схемі, в силу формули (28), рівняння (23) для визначення параметру $\tau_k$ набуде більш зручний вигляд:

$$\tau_k (AB^{-1}r_k, K(B^{-1}r_k - y_k)) = (r_k, K(B^{-1}r_k - y_k)). \quad (29)$$

Якщо $K = I$ – тотожній оператор, то метод (9) – (13) перетворюється в неявний варіаційно – градієнтний метод, який розглянуто [6].

Якщо $B = K = I$, $A$ – обмежений, позитивно визначений, симетричний
оператор, метод (9) – (13) вироджується в звичайний варіаційно – градієнтний метод [1].

**Обґрунтування методу:**

На множині $D(B)$ задамо новий скалярний добуток [8]:

$$[u, v] = (Bu, Kv), \; u, v \in D(B). \quad (30)$$

Тоді будуть виконуватись всі аксіоми гільбертового простору, і лінійну множину $D(B)$ можна розглядати як дійсний гільбертів простір. Будемо називати замикання множини $D(B)$ в сенсі метрики (30) енергетичним простором $H_B$. Звідси випливає, що $D(B)$ щільно в просторі $H_B$. Норму елемента $u$ в просторі $H_B$ будемо позначати через $\|u\|_B$, так що

$$\|u\|_B = [u, u], \quad u \in D(B). \quad (31)$$

Позначимо

$$G = B^{-1}A, \quad (32)$$

$$g = B^{-1}f \quad (33)$$

і розглянемо рівняння:

$$Gu = g. \quad (34)$$

Оператор $G$ є лінійним, позитивно визначеним симетричним і обмеженим в $H_B$. Дійсно з урахуванням (32) отримаємо:

$$[Gu, v] = [B^{-1}Au, v] = (Au, Kv) = (Ku, Av) = (Av, Ku) = \\ = (BB^{-1}Av, Ku) = [B^{-1}Av, u] = [u, B^{-1}Av] = [u, Gv]. \quad (35)$$

А умова (7) набуде вигляд:

$$\gamma \|u\|_B^2 \le [Gu, u] \le \delta \|u\|_B^2, \quad u \in H_B. \quad (36)$$

Оскільки виконано (35) і (36), рівняння (34) має єдиний розв`язок і, як відомо [7], розв`язання рівняння (34) рівносильно знаходженню мінімуму функціоналу:

$$F(u) = [Gu, u] - 2[g, u]. \quad (37)$$

З урахуванням заміни (32), (33) виконавши певні перетворення, метод (9) – (13) набуде вигляду:

$$u_k = u_{k-1} + \tau_k v_k + w_k, \quad w_k \in H_0 \subset H_B, \quad (38)$$

де $v_k = g - Gu_{k-1}$, а співвідношення (12), (13), для визначення невідомих $\tau_k$ і $w_k$ еквівалентні співвідношенням:

$$[Gu_k, v_k] = [g, v_k], \quad (39)$$

$$[v_k - \tau_k G v_k - G w_k, v] = 0, \quad \forall v \in H_0. \quad (40)$$

Отже розв`язання рівняння (3) методом (9) – (13) в просторі $H$ рівносильно розв`язанню рівняння (34) методом (38) – (40) в просторі $H_B$.

З формули (16) випливає, що

$$[v_k, v] = 0, \quad \forall v \in H_0, \quad k \ge 2. \quad (41)$$

Дійсно,

$$[v_k, v] = [g - Gu_{k-1}, v] = (Bg - BGu_{k-1}, Kv) = \\ = (f - Au_{k-1}, Kv) = 0, \quad \forall v \in H_0, \quad k \ge 2. \quad (42)$$

Тоді система (40) при $k \ge 2$ матиме вигляд:

$$[\tau_k G v_k + G w_k, v] = 0, \quad v \in H_0. \quad (43)$$

Оскільки для оператора $G$ виконані умови (35) і (36), існує самоспряжений позитивно визначений оператор $S : H_B \to H_B$ такий, що:

$$G = S^2. \quad (44)$$

Позначимо через $P$ і $\hat{P}$ оператори ортогонального проектування простору $H_B$ на його підпростір $H_0$ і $\hat{H} = SH_0$, та введемо проекційні оператори:

$$Q = I - P, \quad \hat{Q} = I - \hat{P}, \quad (45)$$

де $I$ – одиничний оператор в $H_B$.

Відзначимо, що співвідношення (41) і (43) рівносильні співвідношенням:

$$P(g - Gu_{k-1}) = 0, \quad k \ge 2, \quad (46)$$

$$P(\tau_k G v_k + G w_k) = 0, \quad k \ge 2. \quad (47)$$

З означення $v_k$ випливає:

$$v_k = g - Gu_{k-1} = G(u^* - u_{k-1}), \quad (48)$$

де $u^* \in H_B$ – узагальнений розв`язок рівняння (34).

На підставі формул (44) і (48) співвідношення (46) і (47) рівносильні співвідношенням:

$$\hat{P}S(u^* - u_{k-1}) = 0, \quad k \ge 2, \quad (49)$$

$$\tau_k \hat{P}S v_k + \hat{P}S w_k = 0, \quad k \ge 2. \quad (50)$$

Дійсно, з (46) маємо:

$$P(g - Gu_{k-1}) = PG(u^* - u_{k-1}) = PSS(u^* - u_{k-1}) = \\ = \hat{P}S(u^* - u_{k-1}) = 0, \quad k \ge 2, \quad \forall u \in H_B. \quad (51)$$

Аналогічно з (47):

$$PG(\tau_k v_k + w_k) = PSS(\tau_k v_k + w_k) = \hat{P}S(\tau_k v_k + w_k), \quad k \ge 2, \quad \forall u \in H_B.$$

З визначення оператора $\hat{P}$ маємо, що

$$\hat{P}S w_k = S w_k, \; w_k \in H_0, \quad k \ge 2, \quad (52)$$

тоді формула (50) матиме вид:

$$S w_k = -\tau_k \hat{P}S v_k, \quad k \ge 2. \quad (53)$$

Введемо оператор

$$W = \hat{Q} G \hat{Q}. \quad (54)$$

Цей оператор відображає простір $H_B$ на його підпростір $\hat{H}^{\perp}$, є симетричним і виконується нерівність:

$$\sigma \|u\|_B^2 \le [Wu, u] \le \eta \|u\|_B^2, \quad \forall u \in H_B, \quad (55)$$

причому

$$\gamma \le \sigma \le \eta \le \delta. \quad (56)$$

Справді $\forall u \in H_B$ маємо:

$$[Wu, v] = [\hat{Q} G \hat{Q} u, v] = [G \hat{Q} u, \hat{Q} v] = [\hat{Q} u, G \hat{Q} v] = \\ = [u, \hat{Q} G \hat{Q} v] = [u, Wv], \quad \forall v \in H_B, \quad (57)$$

тобто $W$ є симетричним.

Враховуючи нерівність (36), $\forall u \in H_B$, отримаємо:

$$[Wu, u] = [\hat{Q} G \hat{Q} u, u] = [G \hat{Q} u, \hat{Q} u] \le \delta \|\hat{Q} u\|_B^2. \quad (58)$$

Аналогічно:

$$[Wu,u]=[\hat{Q}G\hat{Q}u,u]=[G\hat{Q}u,\hat{Q}u]\geq\gamma\left\|\hat{Q}u\right\|_B^2. \tag{59}$$

Аналізуючи останні співвідношення можна стверджувати, що існують сталі $\sigma$ і $\eta$, які задовольняють нерівності (55), такі що виконується умова (56).

З врахування формул (38), (53), (45), (48), (44), (49) і (54) маємо:

$$S(u^*-u_k)=S(u^*-(u_{k-1}+\tau_k v_k+w_k))=S(u^*-u_{k-1})-\tau_k Sv_k+\tau_k\hat{P}Sv_k=$$
$$=S(u^*-u_{k-1})-\tau_k\hat{Q}SG(u^*-u_{k-1})=S(u^*-u_{k-1})-\tau_k\hat{Q}GS(u^*-u_{k-1})=$$
$$=\hat{Q}S(u^*-u_{k-1})-\tau_k WS(u^*-u_{k-1})=(\hat{Q}-\tau_k W)S(u^*-u_{k-1}),\qquad k\geq 2.$$

Отже отримали:

$$S(u^*-u_k)=(\hat{Q}-\tau_k W)S(u^*-u_{k-1}),\qquad k\geq 2. \tag{60}$$

Зауважимо, що функціонал (37) можна записати у вигляді:

$$F(u)=\left\|S(u-u^*)\right\|_B^2-\left\|Su^*\right\|_B^2,\qquad \forall u\in H_B, \tag{61}$$

де $u^*$ – точний розв\`язок рівняння (34).

Дійсно:

$$F(u)=[Gu,u]-2[g,u]=[Gu-g,u]-[g,u]=$$
$$=[G(u-u^*),u]-[Gu^*,u]=[S(u-u^*),Su]-[Su^*,Su]=$$
$$=[S(u-u^*),Su]-[Su^*,Su^*]+[Su^*,\ Su^*]-[Su^*,Su]=$$
$$=[S(u-u^*),Su]-[Su^*,S(u-u^*)]-\left\|Su^*\right\|_B^2=$$
$$=\left\|S(u-u^*)\right\|_B^2-\left\|Su^*\right\|_B^2.$$

З формули (60) випливає:

$$\left\|S(u^*-u_k)\right\|_B^2\leq\left\|(\hat{Q}-\tau W)S(u^*-u_{k-1})\right\|_B^2,\qquad k\geq 2,\quad \forall\tau\in R. \tag{62}$$

З формули (62), отримаємо:

$$\begin{aligned}&\left\|S(u^*-u_k)\right\|_B^2\leq\left\|(\hat{Q}-\tau W)S(u^*-u_{k-1})\right\|_B^2\leq\\ &\leq\left\|(\hat{Q}-\tau W)\right\|_B^{2(k-1)}\left\|S(u^*-u_1)\right\|_B^2,\quad k\geq 2,\quad \forall\tau\in R.\end{aligned} \tag{63}$$

Числовий множник $\tau$ виберемо так, оператор $\hat{Q}-\tau W$ мав як тільки можливо меншу норму. Оскільки спектр оператора $W$ лежить на проміжку $[\sigma,\ \eta]$, то мінімум норми оператора $\hat{Q}-\tau W$ буде коли:

$$\tau=\frac{2}{\eta+\sigma}. \tag{64}$$

При цьому:

$$q=\left\|\hat{Q}-\tau W\right\|_B=\frac{\eta-\sigma}{\eta+\sigma}. \tag{65}$$

Отже, отримали основну оцінку:

$$\left\|S(u^*-u_k)\right\|\leq q^{k-1}\left\|S(u^*-u_1)\right\|_B,\qquad k\geq 2,\qquad \forall\tau\in R. \tag{66}$$

Також з (55) та (54) та визначення оператора $\hat{Q}$ маємо:

$$\forall u\in\hat{H}^{\perp}\qquad \sigma\left\|u\right\|_B^2\leq[Wu,u]=[\hat{Q}S^2\hat{Q}u,u]=[S\hat{Q}u,S\hat{Q}u]=[Su,Su]=\left\|Su\right\|_B^2. \tag{67}$$

Аналогічно з (36) та властивостей оператора $Q$ :

$$\begin{aligned}&\forall u\in\hat{H}_B\qquad [\hat{Q}SQu,\hat{Q}SQu]=[Qu,S\hat{Q}SQu]=\\ &=[Qu,S^2Qu]=[GQu,Qu]\leq\delta\left\|Qu\right\|_B^2,\end{aligned} \tag{68}$$

$$[Wu,u]=[\hat{Q}S^2\hat{Q}u,u]=[S\hat{Q}u,S\hat{Q}u]=\left\|S\hat{Q}u\right\|_B^2\leq\eta\left\|u\right\|_B^2. \tag{69}$$

Таким чином існує $\eta$ таке що $\left\|\hat{Q}SQu\right\|_B^2\leq\eta\left\|Qu\right\|_B^2$.

**Теорема:** Якщо виконані умови (4) – (7), то варіаційно-градієнтний метод (9) – (13) збігається до розв\`язку рівняння (3) і швидкість збіжності характеризується оцінками:

$$\left\|u^*-u_k\right\|_B\leq\sqrt{\frac{\eta}{\gamma}}q^{k-1}\left\|u^*-u_1\right\|_B,\qquad k\geq 2, \tag{70}$$

$$\left\|u^*-u_k\right\|_B\leq\sqrt{\frac{1}{\gamma\sigma}}\left\|B^{-1}(f-Au_k)\right\|_B,\qquad k\geq 2, \tag{71}$$

де

$$q=\frac{\eta-\sigma}{\eta+\sigma};\qquad \gamma\leq\sigma\leq\eta\leq\delta.$$

**Доведення:** Для отримання оцінки (70), використовуємо формули (36), (44), (66), (49), (69) і (41):

$$\left\|u^*-u_k\right\|_B^2\leq\frac{1}{\gamma}[G(u^*-u_k),u^*-u_k]=\frac{1}{\gamma}\left\|S(u^*-u_k)\right\|_B^2\leq\frac{1}{\gamma}q^{2(k-1)}\left\|S(u^*-u_k)\right\|_B^2=$$
$$=\frac{1}{\gamma}q^{2(k-1)}\left\|\hat{Q}S(u^*-u_1)\right\|_B^2\leq\frac{\eta}{\gamma}q^{2(k-1)}\left\|u^*-u_1\right\|_B^2,\qquad k\geq 2.$$

При визначенні конструктивної оцінки (71), врахуємо (36), (44), (49), (67), (41), (48), (33) і отримаємо:

$$\left\|u^*-u_k\right\|_B^2\leq\frac{1}{\gamma}[G(u^*-u_k),u^*-u_k]=\frac{1}{\gamma}\left\|S(u^*-u_k)\right\|_B^2\leq\frac{1}{\sigma\gamma}\left\|G(u^*-u_k)\right\|_B^2=$$
$$=\frac{1}{\sigma\gamma}\left\|g-Gu_k\right\|_B^2\leq\frac{1}{\sigma\gamma}\left\|B^{-1}(f-Au_k)\right\|_B^2,\qquad k\geq 2.$$

Зауважимо, що якщо за перше наближення взяти елемент $u_0\in D(A)$ такий, що виконується умова (16), то нерівність (71) буде виконуватись для $k\geq 1$, а (70) можна переписати у вигляді:

$$\left\|u^*-u_k\right\|_B\leq\sqrt{\frac{\eta}{\gamma}}q^{k-1}\left\|u^*-u_0\right\|_B,\qquad k\geq 1,$$

На основі вищевикладеної теореми приходимо до **висновку**, що однокроковий варіаційно-градієнтний метод (9) – (13) рівняння (3) збігається краще ніж метод найскорішого спуску. Тому для аналізу функціонування систем захисту інформації більш ефективно використовувати однокроковий варіаційно-градієнтний метод.

1. Герасимов Б.М., Тарасов В.А., Токарев И.В. Человеко-машинные системы принятия решений с элементами искусственного интеллекта. – К. Наукова думка, 1993 – 184 с. 2. Лучка А.Ю. Нощенко О.Э. Тухалевская Н.И. Вариационно–градиентный метод //Журнал вычислительной математики и математической физики, 1984 – 24,№7. – С.963-971. 3. Рябова Н.Б. Неявний варіаційно-градієнтний метод. – Київ, 1993 – 8с. 4. Рябова Н.Б. Варіаційно-градієнтний метод для рівнянь з $K$ - додатньо визначеним оператором //Нелинейные краевые задачи математической физики и их приложения. --Київ, ін-т матем.НАН України, 1996. С.223-225. 5. W.V.Petryshyn On Clas of $K$ -p.d. and Non- $K$ -p.d. Operators and Operator Equation. //Journal of Matheamatical analysis and applications, Vol.10, No 1, February 1965.—P.1-24.

**Надійшла до редколегії 19.07.09**