

УДК 519.8

Горбачук В. М.¹, д.ф.-м.н., с.н.с.,
Дунаєвський М. С.¹, аспірант,
Морозов О. О.², магістр

Рівноважні інвестиції у кібербезпеку мережі ланцюгів постачання

¹Інститут кібернетики імені В.М.Глушкова
НАН України, проспект Глушкова 40, Київ
03187
e-mail: GorbachukVasyl@netscape.net

²Делойт, Лесная 5Б, Москва 101000

V.M. Gorbachuk¹, D.Sc.(Phys.-Math.),
M.S. Dunaievskiy¹, Ph.D. student,
O.O. Morozov², M.Sc. (Syst. of Autom.Control)

Equilibrium investments to cybersecurity of supply chain network

¹V.M.Glushkov Cybernetics Institute, NAS of
Ukraine, Glushkov ave., 40, Kyiv 03187
e-mail: GorbachukVasyl@netscape.net

²Deloitte, 5B Lesnaya, Moscow 101000

Розроблено ігрову модель мережі ланцюгів постачання, що складається з ряду роздрібних торговців продуктом і ряду ринків збуту даного продукту, де роздрібні торговці некооперативно конкурують, максимізуючи свої сподівані прибутки шляхом визначення своїх оптимальних трансакцій для продукту, а також оптимальних інвестицій у кібербезпеку, які входять у нелінійні бюджетні обмеження.

Ключові слова: мережа ланцюгів постачання, рівновага Неша, кібербезпека, інвестиції.

The game theory model for supply chain network consisting of a set of retailers selling a product and a set of demand markets buying that product, where retailers compete noncooperatively maximizing their expected profits by determining their optimal transactions for that product as well as the optimal cybersecurity investments entering nonlinear budget constraints, has been developed. The expected profit of each retailer depends on volumes of its transactions with all the markets, its cybersecurity level and general network cybersecurity level as well as on the probability of successful cyberattack versus that retailer dependent on cybersecurity levels. The modified approach of variational inequalities, requiring some assumptions of convexity and compactness, is suggested for application in such a problem of competition and search of Nash equilibria.

Key words: supply chain network, Nash equilibrium, cybersecurity, investments.

Статтю представив д.т.н., проф. Гарашенко Ф.Г.

Переваги споживачів на ринках збуту відбивають функції ціни попиту, які залежать від обсягу попиту на продукт і середнього рівня кібербезпеки у мережі ланцюгів постачання (МЛП). Тоді можна оцінювати вразливість до кібератак як МЛП, так і кожного торговця окремо [1]. Відповідні умови рівноваги Неша можна визначати за допомогою задачі розв'язання певної варіаційної нерівності [2].

Мета роботи – розробити теоретико-ігрову модель МЛП інвестицій у кібербезпеку, яка складається з роздрібних торговців $i = 1, \dots, m$ і ринків попиту $j = 1, \dots, n$. Розрібними торговцями можуть бути продавці споживчих товарів, високотехнологічних або фінансових продуктів. Суттєво, щоб такі торговці працювали в одній галузі та своїми рішеннями могли впливати на рішення інших торговців галузі стосовно обсягу постачання та рівня інвестицій у

кібербезпеку. При цьому важливо вірно оцінювати інвестиції у кібербезпеку, формуючи уявлення про справжню цінність активів інтелектуальної власності.

На відміну від моделей [3–5], у моделі [2, 6] кожний торговець має свої бюджетні обмеження на свої інвестиції у кібербезпеку. Нелінійність цих обмежень ускладнює теоретичні та практичні підходи до розв'язання відповідної ігрової задачі. Відомі застосування теорії ігор до питань безпечності і приватності [7], моделі інвестицій у кібербезпеку (моделі затрати–випуск, моделі інвестиційної віддачі, евристичні моделі тощо), статті з криптографії та мережевої безпеки. Модель [2, 6] застосовує сучасні теорії ігор і варіаційних нерівностей до інвестицій у кібербезпеку, розвиваючи роботу [8] в області моделей мережевої рівноваги для життєво важливих продуктів.

Роздрібним торговцем може бути як магазин

у будівлі чи приміщенні, так і онлайнвий постачальник. У широкому сенсі роздрібним торгівцем може бути надавач фінансових послуг (банківська філія), крамниця споживчих товарів, фізична особа-підприємець тощо. Припустимо, що роздрібні торговці здійснюють трансакції одного й того самого продукту. При електронних платіжних трансакціях між двома сторонами, інвестиції у кібербезпеку мають брати до уваги можливість кібератак, які супроводжуються фінансовою шкодою, втратою репутації, альтернативною вартістю та відповідними розривами. Коли споживачі на ринках збуту здійснюють свої покупки кредитними чи дебітними картками через онлайнну платіжну систему, то виражають свої переваги щодо кібербезпеки МЛП через функції ціни попиту. Ці переваги можуть ґрунтуватися на середній кібербезпеці МЛП, яку називають безпекою МЛП або мережі: напевне, споживачі мають інформацію про безпеку галузі в цілому, а не про безпеку окремого роздрібного торговця. Оскільки роздрібні торговці належать до МЛП, то є вразливими до кібератак через своїх постачальників та/або спільні платіжні системи, а також через спільну критичну інфраструктуру.

Розробимо теоретико-ігрову модель МЛП з конкуруючими роздрібними торговцями, кожний з яких прагне максимізувати свою сподівану корисність, що враховує сподівані виручку, втрати внаслідок кібератаки і витрати на інвестиції у кібербезпеку.

Роздрібні торговці і ринки збуту формують двочастинну структуру МЛП. Спочатку визначимо обмеження кожного роздрібного торговця, а потім – його цільову функцію. Попит d_j на продукт на ринку збуту j має задовольняти рівнянню збереження потоку

$$d_j = \sum_{i=1}^m Q_{ij}, j = 1, \dots, n, \quad (1)$$

де Q_{ij} – невід’ємний обсяг продукту у трансакції між роздрібним торговцем i та споживачами ринку збуту j , обмежений зверху заданою величиною $\bar{Q}_{ij}$:

$$0 \leq Q_{ij} \leq \bar{Q}_{ij}. \quad (2)$$

На відміну від моделі [5], тут кожний торговець характеризується своєю межею $\bar{Q}_{ij}$.

Невід’ємний рівень s_i кібербезпеки роздрібного торговця i обмежений зверху заданим значенням u_{si} :

$$0 \leq s_i \leq u_{si} < 1, \quad (3)$$

де $s_i = 1$ відповідає повній безпеці (яка може не досягатися), а $s_i = 0$ – відсутності безпеки. На відміну від моделі [5], тут кожний торговець характеризується своїм значенням $u_{si} < 1$.

Набуття рівня s_i безпеки пов’язується з функцією $h_i(s_i)$ інвестиційних витрат, яка припускається неперервно диференційованою й опуклою. Тоді для роздрібного торговця i повна безпека відповідає його інвестиціям $h_i(1) = \infty$, а відсутність безпеки – його інвестиціям $h_i(0) = 0$. Такою функцією є, наприклад, нелінійна функція

$$h_i(s_i) = \alpha_i[(1 - s_i)^{-0.5} - 1], \quad (4)$$

де множник α_i дозволяє розрізняти масштаби і потреби роздрібних торговців [3–5]. У моделях [3–5] функції інвестиційних витрат на кібербезпеку входили лише в цільові функції осіб, які приймають рішення (ОПР), але не входили у бюджетні обмеження.

Нехай для кожного роздрібного торговця $i = 1, \dots, m$ його бюджет (budget) на інвестиції у кібербезпеку обмежений зверху заданою величиною B_i :

$$h_i(s_i) \leq B_i. \quad (5)$$

Припустимо, що ймовірність (probability) успішної кібератаки на роздрібного торговця i становить

$$p_i = (1 - s_i)(1 - \bar{s}), \quad (6)$$

де $\bar{s} = \frac{1}{m} \sum_{k=1}^m s_k$ – рівень кібербезпеки МЛП, $\bar{v} = 1 - \bar{s}$ – рівень вразливості (vulnerability) МЛП, $v_i = 1 - s_i$ – рівень вразливості роздрібного торговця i [2–7]. З урахуванням співвідношення (1) визначимо функцію ціни попиту на продукт на ринку збуту j

$$\hat{\rho}_j(Q, s) = \rho_j(d, \bar{s}),$$

де $Q \in R_+^{mn}$ – матриця трансакцій Q_{ij} на всіх n ринках збуту всіх m роздрібних торговців, $d \in R_+^n$ – вектор обсягів d_j попиту на продукт на всіх n ринках збуту, $s \in R_+^m$ – вектор рівнів s_i безпеки всіх m роздрібних торговців. Споживчі переваги щодо продукту виражаються обсягами попиту, а також безпекою відповідної МЛП: мабуть, споживачі готові платити за вищу

мережеву безпеку, але така готовність може бути різною для різних споживачів. До того ж, існує інформаційна асиметрія між роздрібними торговцями та споживачами [9, 10] (автор роботи [9] – Нобелівський лауреат 2001 р.): кожний роздрібний торговець i знає свої інвестиції $h_i(s_i)$ у кібербезпеку, а кожний споживач уявляє середній рівень $\bar{s}$ кібербезпеки.

За відсутності кібератаки та інвестицій у кібербезпеку, прибуток роздрібного торговця i дорівнює різниці між його виручкою та витратами

$$f_i(Q, s) = \sum_{j=1}^n Q_{ij} \hat{p}_j(Q, s) - \left(c_i \sum_{j=1}^n Q_{ij} + \sum_{j=1}^n c_{ij}(Q_{ij}) \right), \quad (7)$$

де c_i – витрати роздрібного торговця i , пов'язані з поводженням та обробкою продукту, $c_{ij}(Q_{ij})$ – витрати, пов'язані з трансакцією між роздрібним торговцем i та ринком збуту j .

Враховуючи співвідношення (6), очікувана (expected) фінансова шкода (damage) роздрібного торговця i від кібератаки становить

$$E(D_i) = p_i D_i, \quad (8)$$

де $0 < D_i$ – фінансова шкода, яку зазнає роздрібний торговець i при успішній кібератаці.

Тоді, враховуючи співвідношення (6)–(8), сподівана корисність (utility) роздрібного торговця i становить

$$E(U_i) = (1 - p_i) f_i(Q, s) + p_i [f_i(Q, s) - D_i] - h_i(s_i) = f_i(Q, s) - p_i D_i - h_i(s_i), \quad (9)$$

де $h_i(s_i)$ – інвестиційні витрати цього торговця на кібербезпеку. Враховуючи нерівності (2), (3), (5), допустиму множину для роздрібного торговця i позначимо

$$K_i \equiv \{(Q_i, s_i) : 0 \leq Q_{ij} \leq \bar{Q}_{ij} \forall j; 0 \leq s_i \leq u_{si}; h_i(s_i) \leq B_i\}. \quad (10)$$

Вважаємо, що всі роздрібні торговці некооперативно конкурують у постачанні однорідного продукту (продукт може бути диференційованим [11]), а кожний з них максимізує свою сподівану корисність, обираючи свої значення $Q_i = (Q_{i1}, \dots, Q_{in})$, s_i . Бажано

знайти такий набір значень $(Q^*, s^*) \in K \equiv \prod_{i=1}^m K_i$,

при яких m роздрібних торговців перебувають у стані рівноваги у сенсі Курно–Неша. Лауреат Нобелівської премії 1994 р. Неш узагальнив поняття рівноваги Курно на кількох гравців

(ОПР), кожний з яких діє виключно у своїх власних інтересах, тобто некооперативно.

Набір значень $(Q^*, s^*) \in K$ називають рівновагою Неша для МЛП, якщо для кожного роздрібного торговця $i = 1, \dots, m$ має місце $\forall (Q_i, s_i) \in K_i$ нерівність

$$E(U_i(Q^*, s^*)) \geq E(U_i(Q_1^*, \dots, Q_{i-1}^*, Q_i, Q_{i+1}^*, \dots, Q_m^*, s_1^*, \dots, s_{i-1}^*, s_i, s_{i+1}^*, \dots, s_m^*)), \quad (11)$$

тобто будь-який роздрібний торговець i не може в односторонньому порядку збільшити свій очікуваний прибуток порівняно з рівновагою Неша, обираючи свої допустимі значення Q_i, s_i .

Щоб нерівності (11) звести до варіаційної нерівності, спочатку доведемо, що допустима множина K опукла. В силу співвідношень (4) і (5) ця множина містить нелінійні обмеження, на відміну від допустимої множини багатьох мережевих рівноважних задач, пов'язаних з перенавантаженням мереж міського транспорту, ланцюгами постачання чи фінансовими послугами [12–14].

Лема 1. Якщо $h_i(s_i)$ – опукла функція, $i = 1, \dots, m$, то допустима множина K опукла.

Доведемо спочатку опуклість множини

$$\bar{K}_i \equiv \{s_i \in R : h_i(s_i) \leq B_i\}.$$

Справді, для $s_i^1, s_i^2 \in \bar{K}_i$, $\lambda \in [0, 1]$ маємо

$$h_i(s_i^1) \leq B_i \leq h_i(s_i^2),$$

звідки в силу опуклості $h_i(s_i)$ випливає

$$h_i[\lambda s_i^1 + (1 - \lambda) s_i^2] \leq$$

$$\lambda h_i(s_i^1) + (1 - \lambda) h_i(s_i^2) \leq \lambda B_i + (1 - \lambda) B_i = B_i,$$

тобто $\lambda s_i^1 + (1 - \lambda) s_i^2 \in \bar{K}_i$.

Оскільки множина K_i є перетином опуклих множини $\bar{K}_i$, можини двосторонніх обмежень (3) і множини двосторонніх обмежень (2), то є опуклою. Тоді декартовий добуток опуклих множин $K \equiv \prod_{i=1}^m K_i$ також є опуклою множиною.

Оскільки для функції $h_i(s_i)$ інвестиційних витрат, що визначається формулою (4), за умови (3) мають місце нерівності

$$\begin{aligned} \frac{\partial h_i(s_i)}{\partial s_i} &= \alpha_i [-0.5(1 - s_i)^{-0.5-1} \times (-1)] = \\ &= \frac{\alpha_i}{2} (1 - s_i)^{-1.5} < 0, \end{aligned} \quad (12)$$

$$\begin{aligned}\frac{\partial^2 h_i(s_i)}{\partial^2 s_i} &= (-1.5) \frac{\alpha_i}{2} (1-s_i)^{-1.5-1} \times (-1) = \\ &= \frac{3\alpha_i}{4} (1-s_i)^{-2.5} > 0,\end{aligned}$$

то ця функція опукла.

Теорема 1. Припустимо, у кожного роздрібного торговця $i = 1, \dots, m$ сподівана корисність неперервно диференційована й увігнута відносно змінних Q_i, s_i . Тоді рівні трансакцій продукту і безпеки $(Q^*, s^*) \in K$ є рівноважними за Нешем для МЛП тоді й тільки тоді, коли задовольняється варіаційна нерівність

$$\begin{aligned}&\sum_{i=1}^m \sum_{j=1}^n \frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} (Q_{ij} - Q_{ij}^*) + \\ &+ \sum_{i=1}^m \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} (s_i - s_i^*) \leq 0 \quad \forall (Q, s) \in K, \quad (13)\end{aligned}$$

де в силу співвідношень (6), (7), (9) мають місце рівності

$$\begin{aligned}\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} &= \frac{\partial f_i(Q^*, s^*)}{\partial Q_{ij}} = \hat{\rho}_j(Q^*, s^*) + \\ &+ \sum_{k=1}^n Q_{ik}^* \frac{\partial \hat{\rho}_k(Q^*, s^*)}{\partial Q_{ij}} - c_i - \frac{\partial c_{ij}(Q_{ij}^*)}{\partial Q_{ij}};\end{aligned}$$

$$\begin{aligned}\frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} &= \frac{\partial f_i(Q^*, s^*)}{\partial s_i} - \frac{\partial [p_i(s^*) D_i]}{\partial s_i} - \\ &- \frac{\partial h_i(s_i^*)}{\partial s_i} = \sum_{k=1}^n Q_{ik}^* \frac{\partial \rho_k(Q^*, s^*)}{\partial s_i} - \frac{\partial h_i(s_i^*)}{\partial s_i} + \\ &+ D_i \left(\bar{s}^* - 1 - \frac{1-s_i^*}{m} \right);\end{aligned}$$

$$\frac{\partial f_i(Q^*, s^*)}{\partial s_i} = \sum_{k=1}^n Q_{ik}^* \frac{\partial \rho_k(Q^*, s^*)}{\partial s_i};$$

$$\frac{\partial [p_i(s^*) D_i(Q^*)]}{\partial s_i} = D_i \frac{\partial p_i(s^*)}{\partial s_i} =$$

$$= D_i \left[-(1-\bar{s}^*) - \frac{1-s_i^*}{m} \right],$$

$$\frac{\partial p_i(s^*)}{\partial s_i} = \frac{\partial [(1-s_i)(1-\bar{s})]}{\partial s_i} =$$

$$= (1-s_i^*) \frac{\partial (1-\bar{s})}{\partial s_i} - (1-\bar{s}^*),$$

$$\frac{\partial (1-\bar{s})}{\partial s_i} = \frac{\partial \left(1 - m^{-1} \sum_{k=1}^m s_k \right)}{\partial s_i} = -\frac{1}{m}.$$

Скористаємося опуклістю допустимої множини K за лемою 1. За умов теореми 1 розв'язання задачі рівноваги Неша рівносильне розв'язанню відповідної варіаційної нерівності [15]. Перепишемо варіаційну нерівність (11) у стандартній формі скалярного добутку

$$\langle F(X^*), X - X^* \rangle \geq 0 \quad \forall X \in K, \quad (14)$$

де $F: K \rightarrow R^n$ – деяка задана неперервна функція, K – замкнута опукла множина. Для цього визначимо вектор-стовпці $X = (Q, s)$ та $F(X) = (F^1(X), F^2(X))$ вимірності $(mn + m)$, що при $X \in K = K$ задовольняють рівнянням

$$\frac{\partial E(U_i(Q^*, s^*))}{\partial Q_{ij}} = F_{ij}^1(X), \quad \frac{\partial E(U_i(Q^*, s^*))}{\partial s_i} = F_i^2(X).$$

Такі рівняння задовольняються, коли оператор $F(X)$ має властивості потенційності [16].

За умов (12) та $B_i = \infty = \bar{Q}_{ij}$, $u_{si} \leq 1$ [5] задача (13) зводиться до подібної задачі [5], що має значно простішу допустиму множину.

Теорема 2. Варіаційна нерівність (14) має розв'язок $X^* = (Q^*, s^*) \in K$.

Дійсно, варіаційна нерівність (14) має розв'язок, якщо функція $F(X)$ неперервна, а допустима множина K компактна [17].

Теорема 3. Варіаційна нерівність (14) має єдиний розв'язок $X^* = (Q^*, s^*) \in K$.

Достатньо показати, що функція $F(X)$ строго монотонна на K [17]:

$$\langle F(X^1) - F(X^2), X^1 - X^2 \rangle > 0 \quad \forall X^1, X^2 \in K, \quad X^1 \neq X^2.$$

У свою чергу, функція $F(X)$ є строго монотонною на K , якщо її якобіан $\nabla F(X)$ є позитивно визначеним на K .

Оскільки нелінійні обмеження (5) у допустимій множині K можуть ускладнювати чисельне розв'язання варіаційної нерівності (13), то виведемо альтернативну варіаційну нерівність, яка використовує множник Лагранжа $\lambda_i \geq 0$ для кожного такого обмеження. Позначимо $\lambda \in R_+^m$ вектор усіх цих множників. Тоді замість допустимої множини (10) використовуватимемо множину

$$K_i^1 \equiv \{(Q_i, s_i) : 0 \leq Q_{ij} \leq \bar{Q}_{ij} \forall j; 0 \leq s_i \leq u_{si}\},$$

а замість множини K – множини

$$K^2 = R_+^m \times \prod_{i=1}^m K_i^1.$$

Теорема 4. Вектор $(Q^*, s^*, \lambda^*) \in K^2$ є розв'язком варіаційної нерівності (13) тоді й тільки тоді, коли є розв'язком альтернативної варіаційної нерівності

$$\begin{aligned} & \sum_{i=1}^m \sum_{j=1}^n \frac{\partial L_i(Q^*, s^*, \lambda^*)}{\partial Q_{ij}} (Q_{ij} - Q_{ij}^*) + \\ & + \sum_{i=1}^m \frac{\partial L_i(Q^*, s^*, \lambda^*)}{\partial s_i} (s_i - s_i^*) + \\ & + \sum_{i=1}^m \frac{\partial L_i(Q^*, s^*, \lambda^*)}{\partial \lambda_i} (\lambda_i - \lambda_i^*) \leq 0 \\ & \forall (Q, s, \lambda) \in K^2, \end{aligned}$$

де використано лагранжіан (Lagrangian)

$$L_i = E(U_i(Q, s)) + \lambda_i [h_i(s_i) - B_i],$$

Список використаних джерел

1. Горбачук В.М. Економічні стимули до спільного володіння безпековою інформацією: узагальнення/ Горбачук В.М., Мартинів А.М. // Теоретичні і прикладні проблеми фізики, математики та інформатики. Ч. 2. – К.: НТУУ «КПІ», 2009. – С. 39–40.
2. Gorbachuk V. Equilibria in supply chain networks/ Gorbachuk V., Morozov O. // PDMU (August 14–19, 2017, Vilnius, Lithuania). – Kyiv, 2017. – P. 55.
3. Shetty N.G. Design of network architectures: role of game theory and economics. / Shetty N.G. - PhD dissertation. Technical Report UCB/EECS-2010-91. – Berkeley, CA: Electrical Engineering and Computer Sciences, University of California at Berkeley, 2010.
4. Shetty N. Competitive cyber-insurance and Internet security / Shetty N., Schwartz G., Felegahazy M., Walrand J. // Proceedings of the 8-th Workshop on the Economics of Information Security (WEIS 2009). – London, UK: University College London, 2009.
5. Nagurney A. A supply chain game theory framework for cybersecurity investments under network vulnerability / Nagurney A., Nagurney L.S., Shukla S. // Computation, cryptography, and network security. N.Daras, M.Th.Rassias (eds.) – Springer International Publishing, 2015. – P. 381–398.

$$\frac{\partial L_i(Q^*, s^*, \lambda^*)}{\partial \lambda_i} = h_i(s_i) - B_i.$$

Таким чином, для розв'язання задачі пошуку рівноважних інвестицій у кібербезпеку МЛП можна запропонувати ітеративний алгоритм, який на кожній ітерації дає в явному вигляді співвідношення для трансакцій продукту, рівнів безпеки та множників Лагранжа, пов'язаних з бюджетними обмеженнями. Цей алгоритм можна застосувати до обчислення розв'язків широкого кола чисельних прикладів інвестицій у кібербезпеку МЛП.

Чисельні приклади, скажімо, для кібератаки на Україну 27 червня 2017 р., сприятимуть глибшому розумінню впливу додаткових роздрібних торговців, бюджетних змін, функцій ціни попиту, фінансових збитків на рівноважні трансакції продукту та інвестиції у кібербезпеку, а також на вразливість МЛП чи роздрібного торговця при бюджетних обмеженнях.

References

1. GORBACHUK, V.M., MARTYNIV, A.M. (2009) Economic incentives to joint possession by security information: generalizations, *Theoretical and applied problems of physics, mathematics and informatics*, P. 2. Kyiv, NTUU «KPI», pp. 39–40.
2. GORBACHUK, V. and MOROZOV, O. (2017) Equilibria in supply chain networks, *PDMU (August 14–19, 2017, Vilnius, Lithuania)*, Kyiv, p. 55.
3. SHETTY, N.G. (2010) Design of network architectures: role of game theory and economics. PhD dissertation. *Technical Report UCB/EECS-2010-91*. Berkeley, CA, Electrical Engineering and Computer Sciences, University of California at Berkeley.
4. SHETTY, N., SCHWARTZ, G., FELEGEHAZY, M. and WALRAND, J. (2009) Competitive cyber-insurance and Internet security, *Proceedings of the 8-th Workshop on the Economics of Information Security (WEIS 2009)*, London, UK, University College London.
5. NAGURNEY, A., NAGURNEY, L.S. and SHUKLA, S. (2015) A supply chain game theory framework for cybersecurity investments under network vulnerability, *Computation, cryptography, and network security*. N.Daras, M.Th.Rassias (eds.) Springer International Publishing, pp. 381–398.

6. Nagurney A. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints/ Nagurney A., Daniele P., Shukla S. // *Annals of operations research*. – 2017. – 248(1). – P. 405–427.
7. Manshei M.H. Game theory meets networks security and privacy / Manshei M.H., Zhu Q., Alpcan T., Basar T., Hubaux, J.-P. // *ACM computing surveys*. – 2013. – 45 (3). – P. 25:1–25:39.
8. Toyasaki F. A variational inequality formulation of equilibrium models for end-of-life products with nonlinear constraints/ Toyasaki F., Daniele P., Wakolbinger T. // *European journal of operational research*. – 2014. – 236. – P. 340–350.
9. Akerlof G.A. The market for lemons: quality uncertainty and the market mechanism/ Akerlof G.A. // *Quarterly journal of economics*. – 1970. – 84(3). – P. 488–500.
10. Горбачук В.М. Проектирование контрактов в условиях риска / Горбачук В.М., Бойко В.В., Русанов И.А. // *Теория оптимальных решений*. – 2011. – № 10. – С. 116–122.
11. Gorbachuk V.M. Cournot–Nash equilibria and Bertrand–Nash equilibria for a heterogenous duopoly of differentiated products/ Gorbachuk V.M. // *Cybernetics and Systems Analysis*. – 2010. – V. 46. – № 1. – P. 25–33.
12. Nagurney A. Network economics: a variational inequality approach. 2-nd, revised edition / Nagurney A. – Boston, MA: Kluwer Academic Publishers, 1999.
13. Nagurney A. Supply chain network economics: dynamics of prices, flows, and profits / Nagurney A. – Cheltenham, UK: Edward Elgar Publishing, 2006.
14. Daniele P. Dynamic networks and evolutionary variational inequalities /Daniele P. – Cheltenham, UK: Edward Elgar Publishing, 2006.
15. Gabay D. On the uniqueness and stability of Nash equilibria in noncooperative games / Gabay D., Moulin H. // *Applied stochastic control in econometrics and management science*. A.Bensoussan, P.Kleindorfer, C.S.Tapiero (eds.) – Amsterdam, The Netherlands: North-Holland, 1980. – P. 271–294.
16. Gorbachuk V. Methods for Nash equilibria search / Gorbachuk V. // *Nonsmooth analysis and its applications to mathematical economics*. – Baku: Ac. Sci. USSR, 1991. – P. 65.
17. Киндерлерер Д. Введение в вариационные неравенства и их приложения/ Киндерлерер Д., Стампакия Г. – М.: Мир, 1983. – 256 с.
6. NAGURNEY, A., DANIELE, P., SHUKLA, S. (2017) A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints, *Annals of operations research*, 248(1), pp. 405–427.
7. MANSHEI, M.H., ZHU, Q., ALPCAN, T., BASAR, T., HUBAUX, J.-P. (2013) Game theory meets networks security and privacy, *ACM computing surveys*, 45(3), pp.25:1–25:39.
8. TOYASAKI, F., DANIELE, P., WAKOLBINGER, T. (2014) A variational inequality formulation of equilibrium models for end-of-life products with nonlinear constraints, *European journal of operational research*, 236, pp. 340–350.
9. AKERLOF, G.A. (1970) The market for lemons: quality uncertainty and the market mechanism, *Quarterly journal of economics*, 84(3), pp. 488–500.
10. GORBACHUK, V.M., BOYKO, V.V., RUSANOV, I.A. (2011) Contract design at risk conditions, *Theory of optimal decisions*, № 10, pp. 116–122.
11. GORBACHUK, V.M. (2010) Cournot–Nash equilibria and Bertrand–Nash equilibria for a heterogenous duopoly of differentiated products, *Cybernetics and systems analysis*, vol. 46, № 1, pp. 25–33.
12. NAGURNEY, A. (1999) *Network economics: a variational inequality approach*. 2-nd, revised edition, Boston, MA, Kluwer Academic Publishers.
13. NAGURNEY, A. (2006) *Supply chain network economics: dynamics of prices, flows, and profits*, Cheltenham, UK, Edward Elgar Publishing.
14. DANIELE, P. (2006) *Dynamic networks and evolutionary variational inequalities*, Cheltenham, UK: Edward Elgar Publishing.
15. GABAY, D., MOULIN, H. (1980) On the uniqueness and stability of Nash equilibria in noncooperative games, *Applied stochastic control in econometrics and management science*, A.Bensoussan, P.Kleindorfer, C.S.Tapiero (eds.) Amsterdam, The Netherlands, North-Holland, pp. 271–294.
16. GORBACHUK, V. (1991) Methods for Nash equilibria search, *Nonsmooth analysis and its applications to mathematical economics*, Baku, Ac. Sci. USSR, p. 65.
17. KINDERLEHRER, D., STAMPACCHIA, G. (1983) *Variational inequalities and their applications*, New York, NY, Academic Press.

Надійшла до редколегії 19.08.2017