

показателів не являється остаточно визначеним і може бути доповнено новими показателями для оцінки рівня КІБ.

Список використаної літератури: 1. Сайт <http://infowatch.com> [Електрон. ресурс]. – Режим доступу: <http://infowatch.com/analytics>. 2. Alfawaz, Salahuddin M. Information security management: a case study of an information security culture. PhD thesis, Queensland University of Technology, 2011. 3. Potiy A.V. The prerequisites of information security culture development and an approach to complex evaluation of its level / A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy // Науково-технічний журнал "Радіоелектроніка і комп'ютерні системи" № 5(57). Харків "ХАІ". – 2012 р. – С. 72 – 77. 4. Паронджанов В. Д. Как улучшить работу ума? Алгоритмы без программистов – это очень просто! / В. Д. Паронджанов. – М.: Дело, 2001. – 360 с. 5. Поміт О. В. Аналіз систем показників безпеки інформації / О. В. Поміт, Д. Ю. Пилипенко // Науково-технічний журнал «Прикладна радіоелектроніка. Тематичний випуск, присвячений проблемам забезпечення інформаційної безпеки». Харків, ХНУРЕ, 2010. – Том 9. – №3. – С. 435-443. 6. Rayford Vaughn Jr., Ronda Henning, Ambareen Siraj, Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7- 10, 2002. 7. Alberts C., Dorofee A. Managing Information Security Risks "The OCTAVE Approach" Addison-Wesley Publishing 2003. 8. Corporate Information Security Working Group (CISWG). November 17, 2004 (Revised January 10, 2005). Report of the Best Practices and Metrics Teams, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Government Reform Committee, United States House of Representatives. 9. Erkan Kahraman. Evaluating its security performance with quantifiable metrics. Master's thesis, DSV SU/KTH, 2005. 10. NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Aug. 2009. 11. Stemler, S., and Bebell, D. (1998). An Empirical Approach to Understanding and Analyzing the Mission Statements of Selected Educational Institutions. Paper presented at the annual meeting of the New England Educational Research Organization. Portsmouth, New Hampshire.

Володимир Бурячок, Анатолій Шиян*

Військова частина А1906, *Вінницький національний технічний університет

УДК: 004.056:159.95

ТЕОРІЯ ІГОР ЯК МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація: Проаналізовано теорію ігор як кількісний метод, який суттєво розширює можливості при управлінні інформаційною безпекою, та визначено основні особливості його застосування. Описано характеристики теорії ігор, які є перспективними для застосування в управлінні інформаційною безпекою, та наведено приклади застосування для задач управління інформаційною безпекою. Проаналізовано розвиток теорії ігор в Україні.

Summary: The paper analyzes the game theory as a quantitative method, which significantly expands the possibilities in the information security management, and describes the main features of its application. We describe the characteristics of game theory, which are promising for use in the information security management, and are presented the solutions of problems for information security management. The development of game theory in Ukraine is described.

Ключові слова: Інформаційна безпека, теорія ігор, управління, узгодження інтересів, рівновага Неша.

І Вступ

Управління інформаційною безпекою включає в себе управління людськими, інформаційними, технічними, програмними, фінансовими та іншими ресурсами [1]. Саме людина, сукупність людей (як організована – підприємство, організація тощо, так і неорганізована – сукупність футбольних фанатів чи хакерів), суспільство і держава (та їх інститути) складають суб'єкти управління інформаційною безпекою.

Все зростаюче поширення інформаційних технологій, зростання числа користувачів Інтернету, створення та структурування міжнародного та регіонального кіберпросторів приводить до все зростаючої ролі процесу узгодження інтересів різних суб'єктів. Саме рівень узгодженості інтересів суб'єктів інформаційних процесів, який визначає мотивацію суб'єктів, сьогодні часто визначає і рівень інформаційної безпеки.

Володимир Бурячок, Анатолій Шиян ©

Цю проблему висвітлено в багатьох публікаціях вітчизняних та зарубіжних авторів, серед яких слід виділити В.М. Богуша, Г. Грачова, Е. Доценко, Т. Кабаченко, П. Конотопова, М. Кузнєцова, Ю. Курносова, А. Манойло, М. Петрова, С. Раторгуєва, В. О. Хорошка, О. К. Юдіна та інших фахівців, які розглядали широке коло задач інформаційної безпеки на різних рівнях ієрархії, починаючи від окремої людини і закінчуючи державою в цілому. В рамках управління інформаційною безпекою добре досліджені такі методи управління інформаційною безпекою, які розроблені школами наукового управління (Ф. Телор, Г. Гантт та інші), адміністративного управління (А. Файоль, М. Вебер та інші), людських відносин (Е. Мейо, А. Маслоу та інші), кількісного підходу в управлінні (Т. Сааті, Д. Шеннон та інші) [1-3].

Разом із тим існує клас методів для кількісного моделювання управління, який ще недостатньо використовується в Україні для управління інформаційною безпекою. Це – сучасна теорія ігор, яка є потужним методом для узгодження інтересів суб'єктів [4]. Вона використовується в світі переважно як інструмент для моделювання економічних і політичних процесів та явищ, проте відносно недавно почала активно використовуватися для аналізу деяких аспектів державної безпеки, – передовсім до аналізу терористичної діяльності [5].

Метою статті є аналіз теорії ігор як кількісного методу, який суттєво розширює можливості при управлінні інформаційною безпекою, та визначення основних особливостей його застосування в даній предметній області.

II Сучасна теорія ігор та концепції рішень гри

Існує багато різних визначень теорії ігор. В [4] наведено такі визначення:

- Теорія ігор – це теорія раціональної поведінки людей з інтересами, що не збігаються;
- Теорія ігор – це наука про стратегічне мислення;
- Теорія ігор – це теорія математичних моделей для прийняття оптимальних рішень в умовах конфлікту;
- Теорія ігор – це розділ прикладної математики, який досліджує моделі прийняття рішень в умовах незбігання інтересів сторін (гравців);
- Теорія ігор – це математичний апарат для моделювання узгодження інтересів сторін.

Останнє визначення теорії ігор і буде використане в рамках статті, бо воно відображає основну суть того, що застосовується в управлінні інформаційною безпекою для суб'єктів інформаційного процесу.

При описі теорії ігор буде широко використано матеріали [4].

Гравець здатний формувати *стратегії* або *дії* та вибирати їх із деякої множини A . Стратегію гравця будемо позначати y ($y \in A$). Під стратегією найчастіше розуміють опис послідовності дій, технологій застосування, методів, алгоритмів, способів тощо.

В результаті вибору дії $y \in A$ гравець під впливом обстановки отримає результат, який позначимо як $z \in A_0$, де A_0 – множина всіх можливих для даної гри результатів діяльності. Відмітимо, що множини A та A_0 можуть не збігатися.

Гравець має здатність визначати переваги на множині результатів $z \in A_0$ шляхом *порівняння між собою* різних результатів своєї діяльності.

Ключовим елементом в теорії ігор є концепція *раціональної поведінки* для гравця, під якою розуміють, що він з урахуванням усієї наявної інформації вибирає саме ті стратегії, які приводять до найбільш бажаних для нього результатів.

Щоб завершити побудову опису *окремого гравця* в теорії ігор, необхідно ввести в розгляд *функцію корисності* $U(z)$ для результату вибору стратегії (дії) даним гравцем, яка виражає в *кількісному* вигляді результат діяльності гравця. В рамках теорії ігор користуються, як правило, не функцією корисності $U(z)$, а функцією корисності $U(y)$, тобто функцією корисності, заданою на множині *стратегій* діяльності гравця A , а не на множині *результатів* його діяльності A_0 .

Для багатьох гравців кожному із n гравців відповідає його функція корисності для даної гри, яку називають функцією виграшу $U_i(y)$ для i -того гравця ($I = \{1, 2, \dots, n\}$ – множина всіх гравців). Тут $y = (y_1, y_2, \dots, y_n)$ називається *вектором дій* всіх гравців, $y \in A_n = \prod A_i$. A_n – *простір стратегій* всіх гравців, а A_i – *простір стратегій* i -го гравця. Таким чином, y_i називається *стратегією* i -того гравця, а

вектор y - *ситуацією* гри (тобто вектором стратегій усіх гравців). Сукупність стратегій $y_{-i} = (y_1, y_2, \dots, y_{i-1}, y_{i+1}, \dots, y_n)$ називається *обстановкою* гри для i -го гравця (це вектор, в якому зібрані стратегії всіх *інших* гравців).

Гра задається описом характеристик:

- усіх гравців;
- функції корисності для кожного із гравців;
- правил гри;
- рівня інформованості гравців (про інших гравців, цілі гравців тощо).

Таким чином, гра задається таким кортежем:

$$\langle A_i, n, A_n, y, y_i, U_i(y_i, y_{-i}), R, Inf \rangle. \quad (1)$$

Тут R - це правила гри (включаючи також *концепцію рішення* гри – див. далі), Inf - множина рівнів інформованості, яка описує інформованість кожного із гравців.

Існують різні класифікації теорії ігор. Вони є дискретні та непервні (за характеристиками функції корисності), одночасні (гравці здійснюють вибір одночасно) та динамічні (здійснення вибору гравцями послідовно), з повною інформованістю та неповною (щодо різних характеристик гри), одноразові чи повторювані, кооперативні (із можливістю створення коаліцій) та некооперативні.

Існує декілька основних концепцій рішень гри [4]. Для простоти розглядаються ігри з досконалою інформацією (повним інформуванням гравців).

Максимінна рівновага. Гравець вважає, що в грі реалізується найгірша для нього обстановка, і вибором своєї стратегії $y_i \in A_i$ він максимізує гарантоване значення цільової функції $U_i(y_i)$:

$$y_i = \arg \max_{y_i \in A_i} \min_{y_{-i} \in A_{-i}} U_i(y_i, y_{-i}). \quad (2)$$

Інтерпретація: «всі довкола мої вороги і всі вони прагнуть зробити мені якнайгірше (при цьому наавіть не аналізуючи *свої власні* виграші), - а я вибираю найкращий варіант».

В рамках предметної області «управління інформаційною безпекою» (2) описує *песимістичний* сценарій.

Парето-оптимум. Вектор стратегій усіх гравців y^P називається *Парето-оптимальним*, якщо не існує іншої ситуації гри, за якої всі гравці виграють не менше і хоча б один гравець виграє більше:

$$\forall y \in A, \exists i \in I : U_i(y) < U_i(y^P). \quad (3)$$

Парето-оптимум розраховано на *альтруїстичних* гравців: ніхто із них не дозволить собі вибрати стратегію $y_i \neq y_i^P$ та виграти *більше*, якщо хоч один із *інших* гравців при цьому отримає *менше*.

В рамках предметної області «управління інформаційною безпекою» (3) описує *оптимістичний* сценарій.

Рівновага Неша. Вектор y^N називається *рівновагою Неша* (точкою Неша) для даної гри, якщо виконана така нерівність:

$$\forall i \in I, \forall y_i : U_i(y_i^N, y_{-i}^N) \geq U_i(y_i, y_{-i}^N). \quad (4)$$

Інакше кажучи, нікому із гравців не вигідно змінювати стратегію Неша за умови, що інші гравці будуть притримуватися стратегії Неша.

В рамках предметної області «управління інформаційною безпекою» (4) описує ситуацію, яку можна назвати *оптимально прогнозованою*: всі гравці *самостійно* і *без примусу* слідкують за тим, щоб виконувати *відому* діяльність.

III Управління інформаційною безпекою із використанням теорії ігор

Наведемо ті характеристики теорії ігор [4, 6], які є перспективними для використання в методах управління інформаційною безпекою.

1. Всі концепції рішення ігор базуються на умові, коли *порівнюються* між собою різні виграші лише для одного й того гравця. Виграші *різних* гравців між собою *не порівнюються*. Це дозволяє розглядати як *рівноправних* гравців суб'єкти різного рівня ієрархій. Наприклад, один із гравців може бути окремою людиною, інший – організацією (фірмою), ще один – суспільним інститутом чи державою. В результаті виникає можливість, наприклад, узгодити реакцію окремої людини на той чи інший законодавчий акт.

2. Можна задавати *різні* умови для гри, тобто різні інтер'єри, в яких розгортається гра. Це буде відображатися передовсім у тому, що будуть змінюватися функції виграшу для гравців. Можна також

задавати різні набори множин стратегій для гравців, що теж буде приводити до того, що набір *найбільш ефективних* стратегій для гравців буде іншим.

3. Змінюючи набори стратегій для гравців та змінюючи для них кількісні значення функцій виграшу (про це нижче), можна добитися того, щоб *рівновагою Неша* були саме ті стратегії гравців, які є *потрібними* для досягнення *потрібного рівня інформаційної безпеки*. За таких умов потреба в *контролі* за гравцями буде різко знижена, бо для гравцям *невигідно* відхилятися від стратегій, які утворюють *рівновагу Неша*. Більше того, навіть якщо *раніше* гравці вибирали «непотрібні» (з точки зору управління інформаційною безпекою) стратегії, то вони (після відповідного інформування) обов'язково *самі* будуть виконувати «потрібну» діяльність із забезпечення інформаційної безпеки. Таким чином, створюються умови для *самоорганізації* суб'єктів у системі управління інформаційною безпекою. Це дозволить надзвичайно сильно *зменшити* необхідні фінансові ресурси для забезпечення заходів інформаційної безпеки.

4. В рамках *однієї* теоретико-ігрової задачі може бути *декілька* рівноваг Неша. Їх можна впорядкувати за рівнем ефективності управління інформаційною безпекою. Але тільки одна *рівновага Неша* буде найефективнішою, - всі інші будуть менш ефективними. В задачах моделювання суспільних інститутів такі «менш ефективні» *рівноваги Неша* зветься *інституціональними пастками* [6]. Це означає, що якщо ситуація знаходиться в рамках однієї із інституціональних пасток, то *вийти* із неї гравці *самостійно не можуть*. Іншими словами, потрібно здійснити таке *втручання* в систему, щоб *рівновагою Неша* стали *потрібні* стратегії гравців. Власне, саме в розробці таких умов і полягає діяльність з управління інформаційною безпекою. Ще раз підкреслимо: спроби «адміністративно» вплинути на неефективну *рівновагу Неша* не здатні привести до успіху, бо «потрібні» стратегії будуть, в загальному випадку, *невигідні* для гравців. За цих умов спроби вплинути на виграші *фінансовими методами* (заохочення, штрафи, бонуси тощо) також є неефективними внаслідок того, що виникає потреба у створенні спеціальної *системи для контролю* за діяльністю суб'єктів інформаційної безпеки.

5. Особливий клас задач теорії ігор складають ігри із *асиметрією* інформації [4, 6]. Вони мають місце у випадку, коли деяка сукупність гравців має *більш повну* інформацію про гру порівняно із іншими. За умов застосування теорії ігор до економіки – це якраз той випадок, коли вираз «інформація – це гроші» є не метафорою, а реальністю. Ці ігри можуть описувати типові ситуації з управління інформаційною безпекою, коли частина суб'єктів інформаційного процесу не має всієї повноти інформації. Як показано в рамках теорії ігор, за цих умов виникає багато *негативних* ситуацій. Наприклад, ситуація так званого *негативного відбору*, коли *раціональним вибором* для гравця, який володіє більш повною інформацією, буде надавати іншому гравцю *неякісну* інформацію (неповну, викривлену тощо). В задачах з управління інформаційною безпекою ситуації, виникає потреба звертатися, наприклад, до *експертів* (як до людей, так і, що особливо загрозливо, до фірм) за *потрібною* інформацією. Разом із тим, в рамках цього напрямку теорії ігор розроблено потужні теоретико-ігрові механізми для того, щоб *розділяти* гравців за рівнем їх інформаційного наповнення (наприклад, так звана «теорія контрактів»).

6. В рамках теорії ігор розв'язано також ряд практично важливих для управління інформаційною безпекою задач, які пов'язані із корупцією, тероризмом, здійсненням революцій тощо.

Використання теорії ігор відноситься саме до предметної області інформаційної безпеки держави внаслідок таких специфічних особливостей.

- Теорія ігор працює виключно з інформацією щодо інтересів гравців - суб'єктів, які приймають рішення.
- Теорія ігор використовує показники інформаційного характеру: для всіх задач теорії ігор важливим є не кількісний вираз показників, що порівнюються, а лише можливість їх *впорядкування*.
- Теорія ігор широко використовує припущення щодо *раціональності* гравців, тобто їх здатності до аналізування інформації.
- Теорія ігор явно враховує можливості наявності інформаційної асиметрії, що є взагалі характерною рисою предметної області інформаційної безпеки держави.
- Теорія ігор дозволяє узгоджувати інтереси суб'єктів, які належать до різних рівнів ієрархії; це теж є специфічною особливістю предметної області саме інформаційної безпеки держави, коли *одна людина* може зменшити рівень національної безпеки цілої держави (останні приклади – Сноудена та Вікілікс).

IV Приклади підходів до теоретико-ігрового розв'язання задач з управління інформаційною безпекою

Наведемо ряд прикладів застосування теорії ігор до розв'язання задач із управління інформаційною безпекою. Як предметні області будемо розглядати класичні задачі [1, 4, 6].

В теорії ігор замість того, щоб розглядати кожну людину (як суб'єкт управлінської діяльності) застосовується підхід, в основу якого покладена ідея «типового представника» [4,6]. Звичайно, це звужує коло можливих задач до таких, які задовольняють наступним умовам.

- Всі суб'єкти управління з даного класу (наприклад, вищий менеджмент фірми) покладаються однаковими. Тобто *індивідуальні* особливості людей не враховуються.
- Розглядаються лише *типові* стратегії, що дозволяє суттєво зменшити їх кількість. Однак це означає, що розглядаються лише ситуації, які найчастіше зустрічаються в процесі управління. Для задач з управління інформаційною безпекою це означає, що, цілком ймовірно, для кожного сценарію розвитку подій потрібно будувати окрему теоретико-ігрову модель.
- Вплив інтер'єру покладається заданим та фіксованим для того, щоб можна було однозначно задати функцію корисності гравців. Це означає, що, цілком ймовірно, для різних аспектів діяльності підприємства потрібно буде будувати різні теоретико-ігрові моделі (наприклад, для спілкування із різними іншими суб'єктами, наприклад, споживачами та постачальниками).

1. Розглянемо узгодження інтересів гравців (суб'єктів) у випадку, коли всі вони є окремими людьми.

Приклад 1. Інформаційна безпека є складовою економічного потенціалу підприємства [1]. В [4] розглянута теоретико-ігрова модель для узгодження інтересів керівників (вищого менеджменту) підприємства та його акціонерів. Загалом, інтереси керівників та акціонерів не збігаються: акціонери зацікавлені у збільшенні *виплат за акціями*, тоді як керівники зацікавлені у збільшенні *виплат на розвиток* підприємства. Для того, щоб мотивувати керівників до збільшення виплат акціонерам, в [4, с. 93 – 97] розроблено таку схему *розподілу виплат* між акціонерами та керівниками, що для керівників стає *вигідним* приймати поточні рішення з управління підприємством таким чином, щоб *збільшувати* виплати акціонерам (які не беруть участь в управлінні підприємством).

Відмітимо, що тут ми маємо типову задачу з управління інформаційною безпекою, причому в умовах *асиметрії* інформації: акціонери мають про підприємство набагато менше інформації, аніж керівники. Звичайно, можна *примусити* керівників «працювати на виплату за акціями», наприклад, шляхом *встановлення контролю* за ними. Але ж, по-перше, контролерам потрібно платити *багато* («за чесність»), по-друге, контролери самі повинні бути керівниками високого рівня (щоб розібратися в діяльності керівників), і, по-третє, їх наявність приведе до *затримок у часі* при прийнятті рішення та *боязні* керівників примати самостійне рішення (на яке немає «квитанції» контролерів). А це вже, як наслідок, приведе до *додаткових* економічних втрат підприємства.

Таким чином, запропонований в [4] метод стимулювання дозволяє *зменшити* рівень ризику для акціонерів.

Приклад 2. При взаємодії декількох підприємств (як суб'єктів діяльності) між собою часто виникає ситуація, коли рішення приймають *конкретні люди*. Це дозволяє моделювати такі випадки як задачі з узгодження інтересів сторін – людей, які приймають рішення в цих підприємствах.

В [6, с. 154 – 159] побудована динамічна теоретико-ігрова модель, яка описує узгодження інтересів чиновника накопичувального пенсійного фонду та підприємця, якому надається кредит від цього фонду. Ця задача відноситься до забезпечення економічної безпеки держави, але, як свідчать результати [5], її вирішення можливе в рамках управління інформаційною безпекою за стратегіями [1].

Теоретико-ігрова модель розроблена для умов впровадження другого рівня пенсійної реформи (накопичувальна система) в умовах України. Враховано можливість зловмисних дій як з боку чиновника, так і з боку підприємця, а також можливість покарання за такі дії та за бездіяльність.

Виявлено кількісні умови на показники діяльності чиновника та підприємця, за яких накопичувальна пенсійна система буде працювати ефективно.

$$\begin{cases} (\alpha - \beta)S_0 - V_1 > p(S_0 - V); \\ \delta > r - w \end{cases} \quad (5)$$

Ці умови включають співвідношення (нерівність) між зарплатою чиновника δ , (усередненою) величиною r отримуваних хабарів та витратами на обслуговування хабара w . Для підприємця як умову отримано нерівність між певними комплексами, які включають в себе норму прибутку від підприємницької діяльності α , величину отриманих від фонду коштів S_0 та норму кредитної ставки β , витрати на випуск продукції (надання послуг) V_1 , витрати на приховання крадіжки V та ймовірність p уникнути покарання за неї.

Аналіз результатів цієї моделі дозволив сформулювати ряд умов для напрямків діяльності держави, тільки *після* виконання яких можна впроваджувати другий рівень пенсійної реформи.

2. Розглянемо узгодження інтересів гравців (суб'єктів) у випадку, коли один із них є окремою людиною, а інший – підприємством, суспільним інститутом чи державою.

Приклад 3. До економічного потенціалу підприємства, складовою якого є інформаційна безпека [1], відноситься інноваційний потенціал підприємства. Забезпечується він, в основну, за рахунок власних працівників (які або самі пропонують інновації, або ж здатні їх впроваджувати).

В [6, с. 123 – 129] побудовано динамічну теоретико-ігрову модель для взаємодії працівника і підприємства в інтер'єрі участі підприємства в інноваційній діяльності. Враховано витрати підприємства на 1) закупівлю нового обладнання (технологій) як на вітчизняному, так і на закордонному ринках, 2) доплату працівникам за *підвищений* рівень освіти, 3) дохід підприємства (з урахуванням рівня освіти працівників). Для працівників враховано тільки доплати за *підвищений* рівень освіти.

В результаті розв'язання гри показано, що за *припущення*, коли дохід від використання *інноваційного* вітчизняного чи закордонного обладнання (технологій) є однаковим, рівновагою Неша є купівля вітчизняного обладнання (технологій) та інвестування в інноваційні структури України, а навчати працівників (підвищувати їх кваліфікацію) доцільно в Україні. Загалом ця умова може бути записана у вигляді такої нерівності:

$$(I_{in} - I_{out}) + (C_{out} - C_{in}) + (\delta_{out} - \delta_{in}) + t > 0. \quad (6)$$

Тут індексами *in* і *out* відповідають Україні та закордону відповідно, *C* - витрати на закупівлю обладнання, δ - доплата працівнику за здобуту ним *додаткову* освіту, *t* - виплати підприємства на тренінг працівника за кордоном, *I* - дохід підприємства від використання інноваційного обладнання.

Нерівність (6) дозволяє здійснити цілий ряд заходів із управління безпекою вітчизняної економіки. Підкреслимо, що ця нерівність визначає коло інформації, яка необхідна для прийняття рішення.

Приклад 4. Безпека підприємства вимагає інформування щодо вигідності використання фінансових інститутів. Сьогодні, з розвитком доступу до інформації у світі, трансакційні витрати за доступ до міжнародних фінансових структур стали досить малими. Внаслідок цього підприємства з України цілком можуть використовувати в своїй *поточній* діяльності не українські, а міжнародні фінансові структури.

В [6, с. 145-153] побудовано базову теоретико-ігрову модель для аналізу вибору підприємця щодо каналу інвестування у розвиток власного підприємства. Розглянуто дві можливості: власне інвестування через фінансові структури України, і через міжнародні структури. Аналіз моделі свідчить, що інвестування через закордонні фінансові структури стає вигідним за такої умови:

$$I > I_c = \frac{(1 - \alpha_2)\Delta_1 + \Delta_2 + (\Delta_{IH} - \Delta_H)}{\beta - \alpha_1 - \alpha_2 + \alpha_1 \cdot \alpha_2}. \quad (7)$$

Тут *I* - інвестиційні кошти, які підприємець хоче вкласти, *I_c* - критичне значення інвестиційних коштів, α_1 - трансакційні витрати в Україні, які пропорційні сумі інвестицій, а Δ_1 - виражені у вигляді *фіксованої* суми, α_2 та Δ_2 - те ж саме для закордонних фінансових структур (причому витрати на створення закордонної фінансової структури потрібно включити у фіксовану суму), Δ_{IH} - трансакційні витрати в Україні на переведення суми за кордон, β - трансакційні витрати при інвестуванні в Україні (наприклад, «відкати»), Δ_H - трансакційні витрати при інвестуванні в Україні, які сплачуються у вигляді *фіксованої* суми.

Як показують кількісні оцінки, здійснені в [6], інвестування «через закордон» для підприємств України стає вигідним мінімально при сумах понад 200 тис. євро. Таким чином, таким каналом інвестування можуть користуватися *напрямку* лише достатньо великі підприємства. В Україні такий канал працює надзвичайно ефективно: основний масив прямих іноземних інвестицій як експортного, так і імпортного характеру, орієнтовано на Кіпр, де трансакційні витрати є найменші. В [6] виділено також ряд загроз для економічної безпеки держави.

3. Розглянемо узгодження інтересів гравців (суб'єктів) у випадку, коли вони є підприємствами, суспільними інститутами та державами.

Приклад 5. Для випадку, коли суб'єктами гри є фінансові структури розвиненої та нерозвиненої країни, динамічну теоретико-ігрову модель для узгодження інтересів сторін побудовано в [6, с. 246 – 255]. Із аналізу цієї гри отримано два основних висновки.

Перший висновок стосується умов, за яких розвинені фінансові структури будуть приходити на нерозвинені ринки, зокрема, в Україну. Така умова має наступний вигляд:

$$p_U \geq \frac{p_d \cdot c_d}{c_U} \quad (8)$$

Тут p - ймовірність повернення кредиту, c - величина кредитної ставки, індекси U та d позначають характеристики для України та розвинених країн, відповідно.

Оцінюючи співвідношення кредитних ставок в Європі і в Україні як 1:5, можна отримати для (8) оцінку $p_U \geq 0,2 \cdot p_d$. Із оцінки видно, що навіть за умови, коли в розвинені країни повертають *всі* кредити, іноземній фінансовій структурі *вигідно* зайти на ринок України навіть за умови, коли ймовірність повернення кредиту є досить мала. А в умовах фінансової кризи, коли *ризикованість* кредитів в розвинених країнах зростає (відповідно ймовірність повернення зменшується), фінансові структури розвинених країн будуть заходити на ринок України більш активно.

Така ситуація збільшує загрози національній безпеці України внаслідок зростання ризиків нестабільності фінансової системи: іноземні банки налаштовані на *вивезення капіталу* з України (для виплати дивідендів своїм акціонерам, наприклад), до того ж у випадку погіршення фінансової ситуації в Україні вони відразу згортають свою роботу, залишаючи економіку України без кредитної підтримки (банки України не мають відповідних фінансових ресурсів).

Власне, саме така ситуація й спостерігалася під час світової фінансової кризи.

Другий висновок стосується формування внутрішніх цін на *власність* в Україні, та роль в цьому фінансових структур розвинених країн.

Рівень цін на власність можна оцінити таким чином:

$$C \leq \frac{P}{r} \quad (9)$$

C - ціна власності, P - річний прибуток від володіння власністю, r - депозитна ставка.

Співвідношення (9) отримано за умови, що отримані за власність кошти, покладені на депозит, повинні приносити прибуток не більший, аніж коли ці кошти покладені в банк (за іншої умови власність не куплять).

Тоді індекс i для порівняння цін на *однакову* власність в Україні та в розвинених країнах можна розрахувати за такою формулою:

$$i = \frac{C_d}{C_U} = \frac{r_U}{r_d} \cdot \frac{P_d}{P_U} \quad (10)$$

Індекси U та d позначають характеристики для України та розвинених країн, відповідно.

Співвідношення депозитних ставок в Україні та в розвинених країнах можна оцінити як 1:10. Річний прибуток від власності можна оцінити як 1:(1÷10): для власності на великі виробничі підприємства *експортного* напрямку (металургійної, хімічної тощо) цей прибуток не дуже відрізняється від прибутку відповідних іноземних фірм, а для малого та середнього бізнесу (який орієнтовано переважно на внутрішній ринок) різниця буде суттєвою. Тоді для індексу порівняння (10) можна отримати таке співвідношення:

$$\frac{C_U}{C_d} \approx 0,1 \div 0,01 \quad (11)$$

Співвідношення (11) свідчить, що існують досить великі ризики для економічної безпеки України на етапі переходу до розвиненого стану. Ці ризики полягають в тому, що *на початку* такого переходу ціна власності є в десятки разів меншою, і доступною для людей та структур, які не здатні здійснювати *ефективне* управління нею. Тому *масована* купівля власності іноземними резидентами може суттєво *уповільнити* розвиток економіки. Ще один ризик полягає в тому, що власність може скуповуватися із *спекулятивною* метою: різниці в її ціні може складати, як видно із (11), *десятки* разів.

V Розвиток теорії ігор в Україні

В Україні теоретико-ігрові методи практично не застосовуються до моделювання не тільки задач інформаційної безпеки держави, але й до моделювання економічних та політичних задач (як це вже багато десятиків років стало *нормою* в розвинених країнах).

Власне, так звані *ігри з нульовою сумою* є складовою нормативного навчального курсу «Дослідження операцій» для економістів та менеджерів. Але це ігри, в яких, по-перше, *порівнюються* виграші різних гравців та, по-друге, сума виграшів гравців є *нульовою* (тобто «скільки перший виграв, стільки другий

програв»). Такі ігри *неможливо* застосувати до опису задач *реального* життя, а особливо до задач моделювання аспектів інформаційної безпеки (наприклад, витрати хакера є набагато менші за втрати підприємства чи державної структури) чи ринкової економіки.

Для задач *технічної* кібернетики в Україні широко застосовувалися *диференціальні* ігри, застосування яких для задач інформаційної безпеки є або дуже обмеженим, або неможливим.

Натомість сучасна теорія ігор (див. частину II статті та [4]) є *практично невідомою* в Україні. В результаті на ринку сучасної суспільно-економічної аналітики Україна є *практично невідомою у світі*.

Наприклад, в Україні практично відсутні спеціалісти, які знають основні закономірності функціонування ринкової економіки. Наприклад, в [7] показано, що з 1969 по 2005 рік 86 науковцями України було опубліковано всього 121 статтю в іноземних наукових журналах, причому переважно в третьосортних (використана база даних EconLit, в якій зібрані практично всі *англомовні* журнали світу). Із цих науковців менше 20 працювали у ВНЗ.

В останні роки застосуванню теорії ігор навчають у Київській школі економіки (готує лише магістрів, викладання переважно англійською мовою, на курсі близько 50 студентів, кількість викладачів близько 20 осіб). Наукові дослідження в Україні здійснюють на *постійній* основі у Київській школі економіки та у вінницькому національному технічному університеті, де видано перший в Україні навчальний посібник з сучасної теорії ігор українською мовою [4].

Таким чином, в Україні відсутні спеціалісти, які здатні масово навчити студентів методам та технологіям діяльності, які відповідають ринковій економіці. Разом із тим, щороку в Україні близько 1 тисячі людей отримують ступінь кандидата та доктора економічних наук, причому кількість дисертацій, які використовують *сучасну* теорію ігор, складає, в кращому випадку, лічені одиниці. В результаті, наявність критичного стану інформаційної безпеки держави у предметній області економіки в Україні навіть не усвідомлюється.

VI Висновки

Виділено характеристики теорії ігор, які є перспективними для застосування в методах управління інформаційною безпекою. Наведено приклади застосування теорії ігор для задач інформаційної безпеки та показано, що вона дозволяє за єдиною методологією вирішувати задачі узгодження інтересів для суб'єктів діяльності, в тому числі тих, які належать до різних рівнів ієрархії. Приклади підтверджують високу ефективність теорії ігор для управління інформаційною безпекою. Більше того: клас задач з управління інформаційною безпекою, який потребує узгодження інтересів суб'єктів діяльності, не може бути розв'язаний без застосування теорії ігор. Проаналізовано розвиток теорії ігор в Україні як засіб моделювання.

Список використаної літератури: 1. Андреев В. І., Козюра В. Д., Скачек Л. М., Хорошко В. О. Стратегія управління інформаційною безпекою. – К. : ДУІКТ, 2007. – 277 с. 2. Манойло А. В. Государственная информационная политика в особых условиях: Монография. М. : МИФИ, 2003. – 388 с. 3. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с. 4. Шиян А. А. Управління розвитком соціально-економічних систем. Теорія ігор: основи та застосування в економіці та менеджменті: Навчальний посібник. – Вінниця: ВНТУ, 2010. – 162 с. 5. Sandler T. The analytical study of terrorism: Taking stock // Journal of Peace Research. – 2013. – To be published. The online version of this article can be found at: <http://jpr.sagepub.com/content/early/2013/08/02/0022343313491277>. 6. Шиян А. А., Нікіфорова Л. О. Управління формуванням ефективних економічних інститутів для України. – Вінниця: ВНТУ, 2011. – 300 с. 7. Courpe T. The visibility of Ukrainian economists 1969–2005 // The Journal of Socio-Economics. – 2008. – V.37. – P.2114–2125.