Ольга Діброва
Київський національний університет технологій та дизайну, Україна

МЕТОДИКА ВИЗНАЧЕННЯ ПОКАЗНИКІВ, ЩО ХАРАКТЕРИЗУЮТЬ РІВЕНЬ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НАУКОЄМНОГО СЕКТОРУ

Olga Dibrova
Kyiv National University of Technologies and Design, Ukraine

METHODS TO DETERMINE INDICATORS THAT CHARACTERIZE THE LEVEL OF THREATS TO INFORMATION SECURITY OF KNOWLEDGE-INTENSIVE SECTOR

The need to ensure effective information security and management of knowledge-based economy is caused by the next: rapid informatisation of every activity, when the information became the main economic category of nowadays and requirements for knowledge-intensive products increase day by day.

Development of high technology sector is a first priority for the government as it directly affects the national economy. That's why, the assessment of threats to information security of knowledge-based sector is important to consider.

Given its strategic importance to the national economy, its scientific and technological progress and innovative development in this article we attempt to form key threats indicators and information security threats to knowledge-based economy, and to show their interconnections by using the Bayesian networks.

Key words: information security, Bayesian network, innovation, knowledge-based, knowledge-intensive sector, technological progress, threats to information security, high-tech sector.

Постановка проблеми. Наукоємний сектор стає пріоритетним для держави, оскільки прямо впливає на розвиток національної економіки, а отже й на конкурентоспроможність держави на міжнародній арені, а управління інформаційною безпекою наукоємного сектору є стратегічним напрямком розвитку, впливає на економічну безпеку національної економіки, на науково-технічний прогрес держави. Тому питання оцінки рівня загроз інформаційній безпеці наукоємного сектору є важливими для розгляду.

Мета статті полягає в тому, щоб сформувати ключові показники загроз та загрози інформаційній безпеці наукоємного сектору економіки, та обґрунтувати методику оцінки визначення показників, що характеризують рівень загроз інформаційній безпеці наукоємного сектору, з використанням байєсівських мереж.

Стан дослідження. Велика увага вітчизняних та зарубіжних науковців приділена питанням інформаційної безпеки держави, підприємства та особистості, формуванню ефективних систем захисту інформації. Це Ліпкан В.[1] , Цимбалюк В.[2], В. В. Глушак[3], Горбатюк О.М.[4]. Питаннями визначення наукоємності, ефективного управління наукоємними виробництвами, створенням

[1] Ліпкан, В.А. (2008). *Національна безпека України*. Київ: Кондор.

[2] Цимбалюк, В. (2004). Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 8*, 30-33.

[3] Глушак, В.В. (2012). Підхід до аналізу загроз інформаційної безпеки з використанням байєсівських мереж. *Інформаційні технології та комп'ютерна інженерія, 2,* 12-17 <http://nbuv.gov.ua/UJRN/Itki_2012_2_4>.

[4] Горбатюк, О.М. (1999). Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка*, *14,* 46-48.

та модернізацією класифікацій наукоємних галузей займалися: Манойленко О. В.[1], Борисенко П.А.[2], Кошевий М. М.[3]. Проте питання оцінки рівня загроз інформаційної безпеки наукоємного сектору потребують подальших розробок.

Постановка завдання. В Україні на сьогодні практично відсутні дослідження цієї проблематики. Враховуючи її стратегічне значення для національної економіки, науково-технічного прогресу та інноваційного розвитку в даній статті робиться спроба сформувати ключові показники загроз та загрози інформаційній безпеці наукоємного сектору економіки. А також обґрунтувати методику оцінки визначення показників, що характеризують рівень загроз інформаційній безпеці наукоємного сектору, що ґрунтується на застосуванні байєсівських мереж.

Виклад основних положень. Необхідність забезпечення та ефективного управління інформаційною безпекою наукоємного сектору економіки зумовлена стрімким розвитком інформатизації, коли інформація стала ключовою економічною категорією, а також зростають вимоги до рівня наукоємності продукції на світових ринках. Передовими країнами світу стають ті, що виготовляють високотехнологічну продукцію, використовуючи при цьому новітні розробки та технології, забезпечуючи високий рівень впровадження інновацій, а також приділяють увагу власній енергоефективності.

Наукоємність – це один з показників, що характеризують технологію виробництва продукції та відображає ступінь її зв'язку з науковими дослідженнями та розробками. Наукоємний сектор характеризується досить високими витратами на науково-технічні розробки, високим рівнем впровадження інновацій, реалізації новітніх технологій та виконання науково-дослідних робіт. Тобто до наукоємного сектору ми можемо віднести галузі виробництва та сфери послуг, продукція та послуги яких є наукоємними та які здійснюють наукові та науково-технічні дослідження, широко впроваджують інновації та стимулюють розвиток науки. Виходячи з цього, наукоємність державної економіки в цілому, її окремої галузі та певної групи галузей може бути показником, що характеризує певні особливості об'єкта, до якого він належить. Проте виникає питання, які ж галузі відносяться до наукоємних.

Віднесення галузі або виробництва до числа наукоємних або високотехнологічних, прийняте в закордонній і вітчизняній літературі, є досить умовним: у цю групу включаються ті галузі, для яких характерно перевищує деякий фіксований рівень співвідношення витрат ресурсів на НДДКР і обсягу продукції, що випускається або відвантаженої продукції, доданої вартості або ж величини основних факторів виробництва (виробничих фондів і праці)[4].

Відповідно до методології запропонованої Організацією економічного співробітництва і розвитку до наукоємних належать галузі, в яких витрати на науково-дослідні та дослідно-конструкторські роботи складають більше 4% обороту.

На основі цього до наукоємних галузей відносять: виробництво комп'ютерів, електронного устаткування та його компонентів, електротехнічного устаткування, наукових приладів, контрольно-вимірювальної апаратури, аерокосмічну промисловість, хімічну промисловість, фармацевтичну промисловість[5]. Значну частину витрат становить розробка конструкції виробів, створення нових матеріалів, розробка нових схем, забезпечення надійності, екологічної чистоти та безпеки обслуговування.

Що стосується сфери послуг, то тут до наукомістких відносяться п'ять галузей: сучасні види зв'язку, фінансові послуги, освіта, охорона здоров'я, бізнес-послуги, які включають розробку

[1] Манойленко, О.В. (2014). Теоретико-методичні аспекти вдосконалення державної інвестиційної політики з розвитку сектора наукоємних виробництв. *Проблеми економіки*, *4,* 104-109. <http://nbuv.gov.ua/UJRN/Pekon_2014_4_14>

[2] Борисенко, П.А. (2008). Методичні підходи до визначення поняття „наукоємне виробництво" (на прикладі авіаційної промисловості). *Схід*, *5 (89),* 27–32.

[3] Кошевий, М. (2013). Формування організаційно-економічних умов розвитку наукоємних виробництв у промисловості України. *Економіст*, *8,* 58-60. <http://nbuv.gov.ua/UJRN/econ_2013_8_15>.

[4] Макаров, В.Л., Варшавский, А.Е. (2001). *Наука и высокие технологии России на рубеже третьего тысячелетия (социально-экономические аспекты развития).* Москва: Наука.

[2] *Економічна енциклопедія в 3-х т.* (2001). Київ: Академія, 2.

програмного забезпечення, контрактні дослідження і розробки, консультативні, маркетингові та інші послуги, використовувані при організації і веденні бізнесу[1].

Інформаційною безпекою наукоємного сектору економіки слід вважати – комплексну систему механізмів забезпечення інформаційної безпеки та методів захисту інформації, якою володіють підприємства наукоємних галузей, від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні, та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитків, а також система попередження та реагування на негативні інформаційний впливи та операції, що можуть спричинити негативні наслідки для науково-технологічного потенціалу держави.

Факторами, що визначають рівень інформаційної безпеки наукоємного сектору економіки є:

1. Визначення пріоритетів науково-технічної політики.
2. Системний і оперативний розвиток законодавчої бази.
3. Чітке і послідовне здійснення структурних перетворень.
4. Комерціалізація науково-виробничої діяльності.
5. Міжнародне співробітництво.
6. Раціональний захист внутрішнього ринку, цілеспрямовані активні дії по завоюванню вітчизняними товаровиробниками світового ринку.
7. Створення ефективного державного механізму поширення і впровадження інновацій.
8. Створення науково-технічних та інвестиційних відділів в новітніх областях досліджень і розробок.

Показниками, що характеризують рівень інформаційної безпеки є ймовірності виникнення загроз інформаційній безпеці.

До основних загроз інформаційній безпеці наукоємного сектору можна віднести наступні: загрозу втрати інформації, загрозу порушення конфіденційності інформації, загрозу неповноти інформації,загрозу недостовірності інформації, загроза інвестиціям у сферу інформатизації. До чинників, що впливають на загрози інформаційній безпеці належать: політики інформаційної безпеки, вартість інформації, вартість системи управління інформаційною безпекою, частота виникнення технічних збоїв, рівень мотивації персоналу, фінансування, нормативно-правове забезпечення, використання державних та міжнародних стандартів.

Загрози інформаційній безпеці наукоємного сектору економіки залежать від ряду внутрішніх та зовнішніх факторів, тому на нашу думку, для аналізу та отримання результатів варто використовувати мережі Байєса. Серед багатьох методів аналізу даних, вони надають зрозуміліше пояснення висновків, а також допускають можливість використання у якості вхідних даних частоти появи різних значень змінних, а представлення у вигляді графа є зручним інструментом для вирішення задачі оцінки ймовірностей виникнення загроз [2].

Так як байєсівська мережа є графом, вершинами якого є випадкові змінні, а ребра графа описують впливи між ними, то процес побудови мережі має починатися з визначення змінних, що приймають участь в задачі і є цільовими. Наступним етапом є опис можливих значень змінних після чого на основі наявної інформації визначаються ймовірності значень змінних та описуються причинно-наслідкові зв’язки між змінними, які представлені ребрами графа. У описаній мережі Байєса цільовими змінними є потенційні загрози, що можуть впливати на інформаційну безпеку наукоємного сектору. Всі інші змінні – чинники, які дають можливість визначити загрозу та оцінити її ймовірність. Для кожної змінної необхідно виписати умовні ймовірності.

Для визначення цих ймовірностей можна використовувати статистичний, експертний та математичний методи. Також необхідною умовою є опис причинно-наслідкових зв’язків між змінними. У процесі моделювання ми отримаємо граф з ймовірностями виникнення загроз, при розрахунку яких враховується частота виникнення та інтенсивність чинників, що впливають на загрози. Приклад байєсової мережі для загроз інформаційній безпеці наукоємного сектору наведений на рис. 1.

[1] Манойленко, О.В. (2014). Теоретико-методичні аспекти вдосконалення державної інвестиційної політики з розвитку сектора наукоємних виробництв. *Проблеми економіки*, *4,* 104-109. <http://nbuv.gov.ua/UJRN/Pekon_2014_4_14>

[2] Глушак, В.В., Новіков, О.М. (2012). Підхід до аналізу загроз інформаційної безпеки з використанням байєсівських мереж. *Інформаційні технології та комп'ютерна інженерія*, *2,* 12-17. <http://nbuv.gov.ua/UJRN/Itki_2012_2_4>.

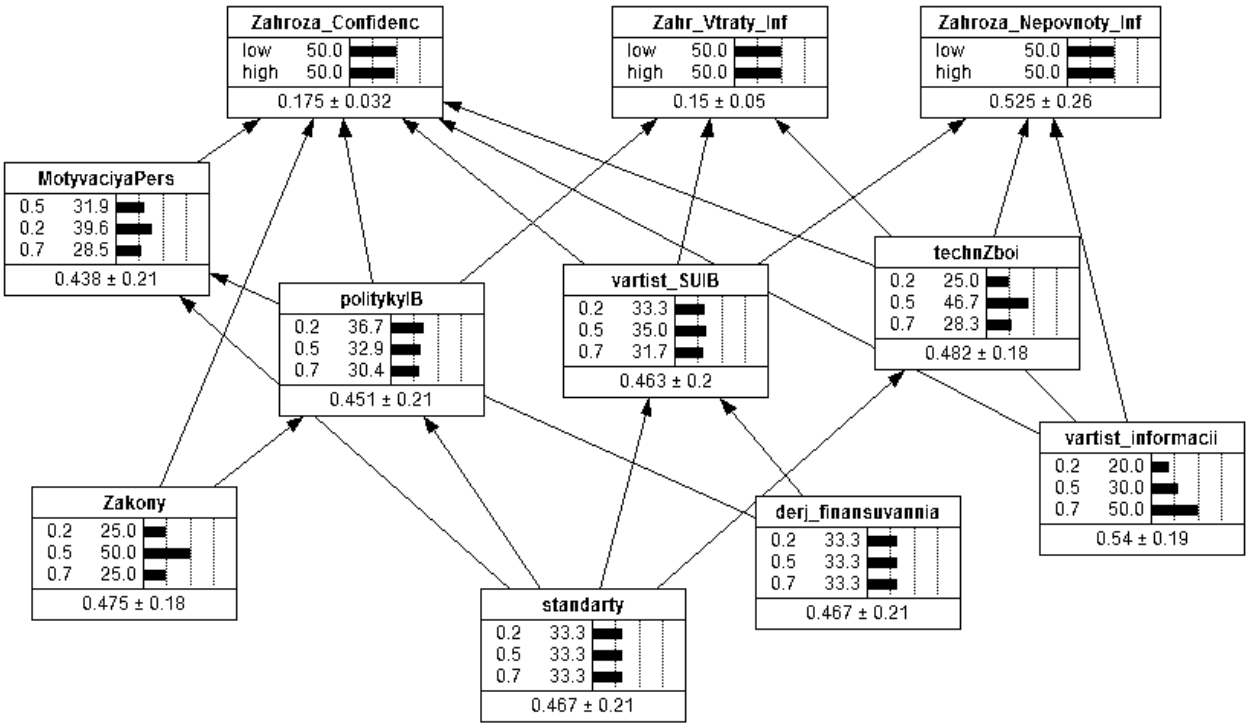

Рис. 1. Фрагмент байєсової мережі для оцінки ймовірності загроз інформаційній безпеці

За допомогою програмного забезпечення Netica було побудовано модель впливу показників інформаційної безпеки на ймовірність виникнення загроз інформаційній безпеці. Задавши величини впливу чинників на загрози ми отримали ймовірності виникнення загроз інформаційній безпеці.

Як видно з рис. 2 ймовірність виникнення загрози конфіденційності за урахуванням рівня мотивації персоналу, політики інформаційної безпеки, вартості СУІБ, збоїв у роботі технічних засобів та нормативно-правових актів складає 0,175, а загроза неповноти інформації складає ≈ 0,52.

При виникненні чинника, що впливає на загрозу ми можемо спостерігати зростання ймовірності реалізації цієї загрози.

Так, наприклад, якщо показник рівня мотивації персоналу знижується, тобто зростає ймовірність впливу показника на ймовірність виникнення загрози конфіденційності, ймовірність реалізації загрози конфіденційності зростає до 0,177. А при зростанні рівня двох чинників (рис. 3) ймовірність виникнення загрози збільшується до 0,179.

На основі даних розрахунків вже можна оціни найкритичніші загрози та бачити показники впливу на загрози, що покращує управління інформаційною безпекою, а також дозволяє уникнути економічних збитків, які могли б настати в разі реалізації загрози.

Висновок. Діяльність наукоємного сектору не можлива без використання новітніх інформаційних технологій задля створення нових інформаційних продуктів, отримання інформації необхідної для діяльності, обміну інформацією та її продажу. Тому інформаційна безпека наукоємного сектору економіки має бути винесена на перший план серед пріоритетних напрямів розвитку і є темою, яка потребує подальших досліджень.

Мережі Байєса є основою для створення досить простих і швидких інформаційних технологій побудови прогностичних економічних оцінок. Результатом моделювання є мережа, що вказує на показники, які потребують регулювання задля мінімізації ймовірності виникнення загроз інформаційній безпеці наукоємного сектору. Серед них: вартість інформації, вартість системи управління інформаційною безпекою, рівень мотивації персоналу, політики інформаційної безпеки та інші.

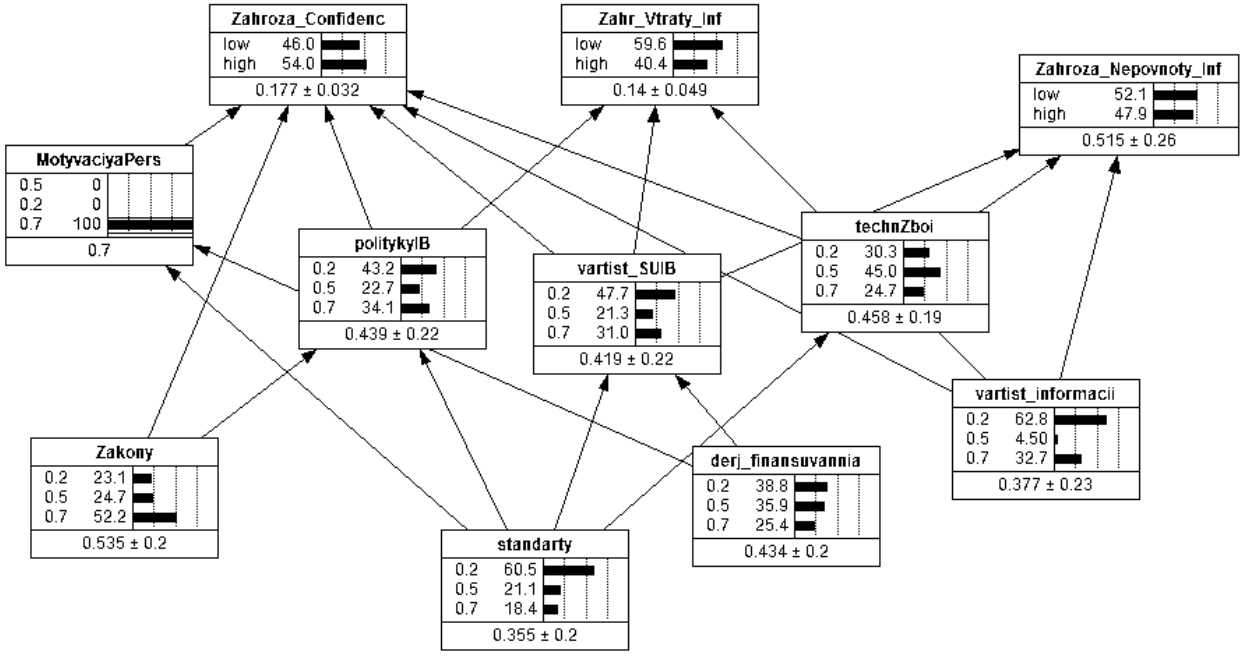

Рис. 2. Ймовірності виникнення загроз інформаційній безпеці при зростанні впливу одного чинника

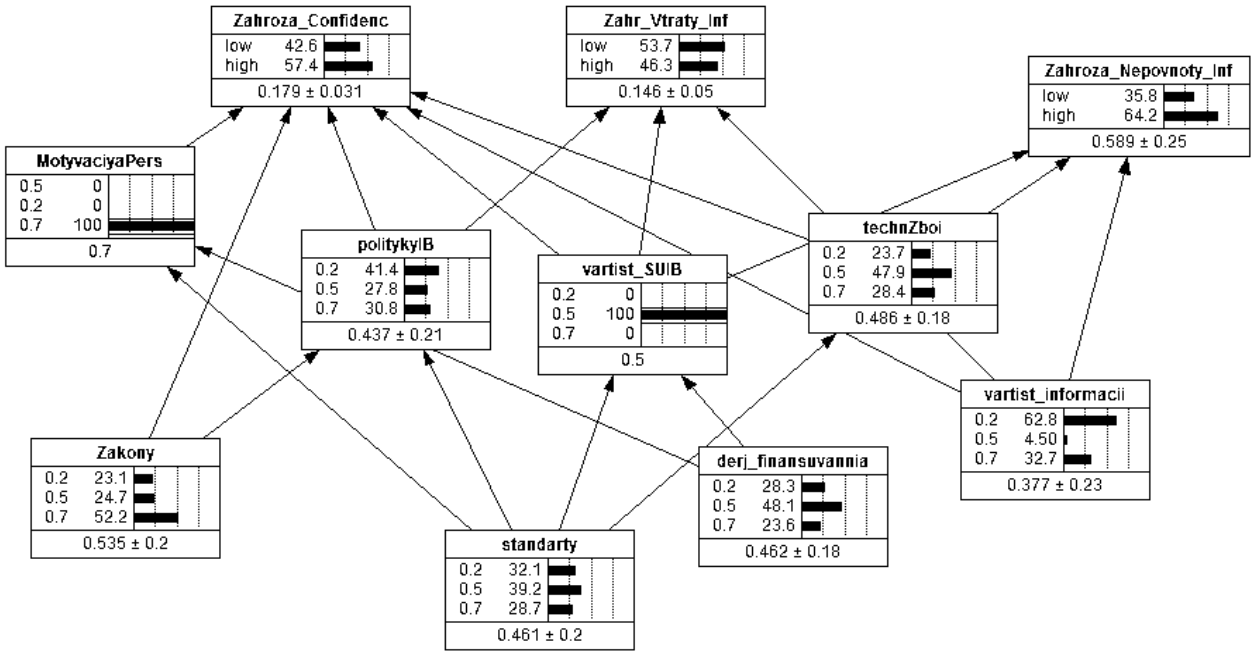

Рис. 3. Ймовірності виникнення загроз інформаційній безпеці при зростанні впливу двох чинників

References:

1. Lipkan, V.A. (2008). *Nacionalna bezpeka Ukra'ny* [National security of Ukraine]. Kyiv: Kondor. [in Ukrainain]
2. Cymbaljuk, V. (2004). Okremi pytannja shhodo vyznachennja kategorii' «informacijna bezpeka» u normatyvno-pravovomu aspekti [Some questions concerning the definition of "information security" in the legal aspect]. *Pravove, normatyvne ta metrologichne zabezpechennja systemy zahystu informacii v Ukraini* [Legal, regulatory and metrological support of information security system in Ukraine], *no.8,* 30-33 [in Ukrainain].
3. Glushak, V.V., Novikov, O.M. (2012). Pidhid do analizu zagroz informacijnoi bezpeky z vykorystannjam bajjesivskyh merezh [The approach to the analysis of threats to information security with use of Bayesian networks]. *Informacijni tehnologii ta kompjuterna inzhenerija* [Information Technologies and Computer Engineering], *no.2,* 12-17 [in Ukrainain]. <http://nbuv.gov.ua/UJRN/Itki_2012_2_4> (2017, April, 03).
4. Gorbatjuk, O.M. (1999). Suchasnyj stan ta problemy informacijnoi bezpeky Ukrainy na rubezhi stolit [Current state and problems of information security in Ukraine at the turn of the century]. *Visnyk Kyiv'kogo universytetu imeni T. Shevchenka* [Bulletin of Taras Shevchenko National University of Kyiv], *no. 14,* pp. 46-48 [in Ukrainain].
5. Manojlenko, O.V., Kravchenko, S.M. (2014). Teoretyko-metodychni aspekty vdoskonalennja derzhavnoi' investycijnoi' polityky z rozvytku sektora naukojemnyh vyrobnyctv [Theoretical and methodological aspects of improving of state investment policy for the sector of knowledge-intensive industries]. *Problemy ekonomiky* [Problems of Economics], *no. 4,* pp. 104-109. <http://nbuv.gov.ua/UJRN/Pekon_2014_4_14> (2016, November, 23).
6. Borysenko, P.A. (2008). Metodychni pidhody do vyznachennja ponjattja „naukojemne vyrobnyctvo" (na prykladi aviacijnoi promyslovosti) [Methodological approaches to the definition of "high-tech production" (for example in the aviation industry)]. *Skhid* [East], *no.5 (89),* 27-32. [in Ukrainain].
7. Koshevyj, M. (2013). *Formuvannja organizacijno-ekonomichnyh umov rozvytku naukojemnyh vyrobnyctv u promyslovosti Ukrainy* [Formation of organizational and economic conditions for development of high-tech manufacturing industry in Ukraine]. *Ekonomist, no.8,* 58-60.<http://nbuv.gov.ua/UJRN/econ_2013_8_15> (2016, November, 23).
8. Makarov, V.L., Varshavskij, A.E. (2001). *Nauka i vysokie tehnologii Rossii na rubezhe tretego tysjacheletija (socialno-jekonomicheskie aspekty razvitija)* [Science and High Technology in Russia at the turn of the third millennium (the socio-economic aspects of development)]. Moscow, Nauka. [in Russian].
9. Mochernyj, S.V. (ed.). (2001). *Ekonomichna encyklopedija v 3-h t.* [*Economic encyclopaedia in 3 volumes*], *Vol.2.*, Kyiv: Akademija. [in Ukrainain].