UDC 005.332.4:005.921.1

Ya. Ya. Pushak,
DrHab (Economics),
Z. B. Zhyvko,
PhD (Economics),
Lviv State University of Internal Affairs

COMPETITIVE INTELLIGENCE AND COUNTER-INTELLIGENCE: THE ADJACENT PLANE OF SECURITY OF THE ENTERPRISE

Statement and relevance of the problem. Inteligence activities are being conducted by most domestic enterprises. Undoubtedly, a need to obtain reliable information about the competitive environment is as relevant and important as is the issue of protecting their secrets. The question of effective and well-functioning of counter-intelligence becomes especially important. Security and sustainable develeopmnet of enterprise depends on obtaining reliable information in a timely manner. Equally important if protection of confidential commercial information.

Analysis of the research problem. From ancient times to the present there are clearly formed principles of intelligence, which are as important and worthy of attention today as they were many years ago. Namely, there is a direct proportional relationship between the gathering of intelligence about competitors, partners, suppliers, and protection of its own data, which contains commercial secrets.

The subject of economic security of enterprise, credit and banking system, economic and competitive intelligence, protection of trade secrets and proprietary information has been researched by a number of Ukrainian and foreign scientists: B. V. Gubskiy [6], N. V. Vashenko [9], A. Derevytskyy [7, p. 8], L. I. Donets [9], Z. B. Zhyvko [10 – 11], V. I. Muntiyan [15], V. K. Senchahov [17], A. I. Sukhorukov [16], V. I. Yarochkin [18].

However, a comprehensive study of counter-intelligence issues in today's information society is not investigated adequately because counter-intelligence issues are closely intertwined with information security, information technology, and competitive intelligence.

The purpose of the article. To investigate the interaction of intelligence and counter-intelligence of enterprise and their role in the protection of an enterprise.

The main material. According to a a definition by Ivchenko, "counter-intelligence is protection of confidential information from espionage" [12]. Economic counter-intelligence got its legitimate status only after the development of market relations. This market makes entrepreneurs not only study business relations with partners, peculiarities of signed agreements, intentions and contacts competitors, but also conceal their own plans, development programs, and support staff.

We agree with the author that preventing the disclosure of information sources (even if they are public information) is a priority in traditional counter-intelligence, as well as methods of gathering information for competitive counter-intelligence [12].

This system is especially well-developed in the US, where American specialists of this profile have developed a number of techniques to protect commercially important intelligence from leakage and theft by competitors. At the initial stages of building security systems, domestic businessmen typically borrowed experience of Western experts on competitive intelligence and readily attracted to former employees of the Ministry of Interior Affairs, Prosecutor's Office and the Security Service.

In general terms, the process of competitive intelligence and counter-intelligence in the system of economic security consists of three stages: (1) internal monitoring, (2) external monitoring and (3) analytical work.

Internal monitoring suggests that security staff aim to protect a company against the penetration by "spies", as well as to monitor compliance of company employees with internal policies regarding disclosure of confidential information [5]. General information and communication systems and special information systems are extensively used for these purposes. One of the most common is IPC (Information Protection and Control), which protects information by encrypting information, as well as full control of possible media channels through which, from a technical point of view, sensitive information may be leaking. Such a system becomes particularly valuable given the fact that up to 75% of confidential corporate information is disclosed unintentionally, by mistake, or negligence of staff [5].

External monitoring in accordance with the abocе-described objectives is a competitive intelligence in the most general sense. It involves collecting the full amount of information about competitors: technology, management, sales volumes, factors of competitive advantage, strategic plans for the future strategy of market penetration, possible threats to a company, process optimization techniques, innovation and so on.

Analytical work involves conducting comparative performance, identifying strengths and weaknesses, develop specific recommendations for management in order to prevent damages, loss of market share, etc. [5].

In order for information that belongs to an enterprise to gain grounds for legal protection, it should be presented

as information that contain trade secrets and confidential information which are property of the subject of commercial activities. This aspect facilitates the work of counter-intelligence but also makes it more difficult because it demands a particular procedure to identify information as trade secrets.

According to the rights established in Part 5. Article 30 of the Law of Ukraine "On Information", a firm defines in its regulations the procedure for obtaining, using, distributing, and storing trade secrets [1]. It is important to note that the process of design and implementation of restricted access to trade secrets must be economically and legally justified and carried out in several stages, which logically follow from one another [11, p. 202].

First of all, it should be noted that according to Article 36 of the Commercial Code of Ukraine [2], data of an economic entity that is related to production, technology, management, financial and other activities and disclosure of which may harm the interests of an entity can be considered as its trade secrets. According to Article 505 of the Civil Code of Ukraine [3], trade secret is information that is secret in a sense that it is generally or in a particular form and set its components is unknown and not readily accessible to persons that normally deal with the kind of information to which it belongs to, and therefore has commercial value and has been the subject of adequate circumstances existing measures to preserve its secrecy taken by a person lawfully controling information. The composition and amount of information constituting commercial secret, as well as methods of its protection, are determined by an economic entity according to the law [11, p. 203].

According to the current legislation, information is a trade secret if it meets the following characteristics: 1) it has actual or potential commercial value due to not being utilized by the third parties; 2) there is no free legal access to it; 3) an owner or his authorized representative take specific measures to preserve its confidentiality. Information that is a trade secret must be fixed on a physical medium (paper, magnetic or optical media, photo negatives or other material objects) and be provided with details that allow its identification. In some circumstances, information constituting commercial secret may be embodied in objects – clothes, blocks, units, devices and substances. However, in this case to establish information embodied in objects, trade secret requires that information has been previously documented in due course.

In addition to the concept of "trade secret", "banking secrecy" has a separate definition and governed by separate laws. Banking secrecy is information on the activities and financial condition of a client, which became known to the bank in the customer service and relationship with him or a third person in the provision of banking services and the disclosure of which might cause material or moral harm to a client. Banking secrecy includes: 1) information about bank accounts of clients, including banks correspondent accounts with the National Bank of Ukraine; 2) operations that were carried out for or on behalf of a client, or agreed by a client; 3) financial and economic conditions of customers; 4) health of a bank and its customer; 5) information about the organizational structure of the legal entity – clients, its directors, and activities; 6) information regarding business clients or trade secrets, projects, inventions, designs and production of other commercial information; 7) information reported by individual banks except that which shall be publicly disclosed; 8) code used for bank protection, 9) Information on banks or customers, collected during the banking supervision [11, p. 204], [7].

There are three common methods of criminal attacks on information of commercial or banking secrets: 1) illegal collection of information constituting commercial or bank secrets; 2) the illegal use of such information; 3) the intentional disclosure of such information [11, p. 207].

Illegal collection of information can take place via: 1) stealing of relevant information or objects that it contains from the premises where they are stored. Such theft can be both open and concealed when items actually sought (documents, products that contain trade secrets) are being stolen along with others thus creating a false impression about the real objectives of criminals; 2) secret criminal penetration of the premises and copying information on paper or electronically. To record and transmit information, perpetrators can use mobile phones with integrated cameras and MMS service; 3) bribing employee of a company that had or has legal access to information. Employee can copy and send information in exchange for certain material or other benefits. If a person has resigned or currently does not have a legal access, but information available to this person earlier has not lost its commercial value, ihe/she simply reports such information; 4) bribery of intermediaries in the negotiations which have certain information; 5) illegally obtaining information from law enforcement or regulatory authorities, which collected such information while performing their direct duties; 6) threats of physical violence against a person or his close relatives to whom information has been authorized as a work responsibilities; 7) blackmail an employee who is on the "hook" because of certain circumstances , 8) installing a spy as a member of staff of an enterprise; 9) recruiting an active employee or using an incentive to disclose information by a laid off person on the grounds of ethnic, racial, religious affinity, to avenge manager for illegal dismissal, transfer to another job, dismissal; 10) using various technical devices that record and transmit information. Using special technology, rooms are being monitored and information is being collected from transmitting channels. For this purpose are often used microphones of directed impact, laser devices for reading information from windows, scanners

detecting and decoding the electromagnetic radiation from office equipment, miniature cameras and camcorders. Such devices can be installed or used a specially trained person or a recruited employees of the company; 11) penetrating the computer networks. To do this, criminals use special computer programs that allow them to seek out relevant data and copy it.

Illegal use of commercial or banking secrets means implementation into manufacturing or taking into account when planning and carrying out business activities certain information without the permission of the owner or authorized person. In particular, the illegal use can have the following forms: 1) presentation of the property or other requirements to an owner of the business or bank secrecy for refund or non-disclosure of relevant information. Such requirements may apply to return to work, appointment to a higher position, firing another employee, providing services, etc.; 2) sale of information to third parties (electronic databases of telephone operators, traffic police, real estate regulators and others.); 3) exchange of information that has commercial or banking value for other tangible assets; 4) adjusting its actions when entering into contracts with owners of such secrets.

Illegal use of information constituting commercial or banking secret, it is possible in other forms, such as intentional disclosure of information [13]. Disclosure can be done orally, in writing, using the means of communication and media, computer networks, and so on. Such disclosure is committed by a person to whom such information became known due to professional or official duties. It can be done by employees of enterprise, institution, organization, or law enforcement or regulatory agencies that have received this information, using their official positions. The objective of counter-intelligence is to deal with above-described crimes of illegal acquisition and use of information. We believe that crime prevention is by far much more effective way to address this matter than dealing with the consequences. The above is justified because of internal monitoring to determine the set of bottlenecks in advance will lead to elimination of a large number of threats.

A. A. Mitrofanov made a significant contribution to the formation of structural units of enterprise security [14]. The organizational structure of competitive intelligence of American corporation Motorola can be used as an example. Motorola was the first organization ot use such a structure. The hybrid structure consists of a central intelligence department and one or two other employees who are assigned to maintain communication with the department of intelligence. Taken together, the corporation Motorola competitive intelligence department employs up to 30 people. Properly constructed interaction between departments provides significant savings.

We offer a model of counter-intelligence of an enterprise (Fig. 1).

The model does not take into account the specifics of a particular company, but is consistent with the essential positions of the prevailing concept of economic security and advanced tasks that relate to the economic security of domestic business entities.

Conclusions. Summing up the results of this study, it is necessary to take into account the scientific contributions of W. Mack Mack, a renowned specialist in firm security, who not only included intelligence department into organizational, managerial, and legal aspects of organization chart of enterprise, but also added to a general description of activities specific provisions about intelligence unit developed by him intelligence. is very important Enterprise competitive intelligence activities , external and internal monitoring of team morale, identifying risk factors, timely receipt and processing of information, cooperation with law enforcement and security agencies are very important for counterintelligence division of the enterprise. Only a systematic and comprehensive approach to enterprise security will lead to developing a common approach and mechanism of protecting business.

References

1. **Конституція** України прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року // Відомості Верховної Ради України від 23.07.1996. – 1996 р., № 30, стаття 141. 2. **Кримінальний** кодекс України прийнятий 5 квітня 2001 // Офіційний вісник України, 2001. – № 21. 3. **Закон** України "Про інформацію" від 2 жовтня 1992 // Відомості ВРУ, 1992. – № 48. 4. **Закон** України "Про Службу Безпеки України" від 25 березня 2002 // Голос України від 13.05 1992. 5. **Господарський** Кодекс України // Редакція від 25.08.2013, підстава 399-18. [Електронний ресурс]. – Сайт ВРУ. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/436-15 6. **Цивільний** кодекс України // Редакція від 11.08.2013, підстава 406-18 [Електронний ресурс]. – Сайт ВРУ. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/435-15 7. **Про банки** і банківську діяльність : Закон України від 7 грудня 2000 р. № 2121-III // Відом. Верхов. Ради України. – 2001. – № 5 – 6. – Ст. 30. 8. **Абрамов В.** Деловая разведка в системе обеспечения предприятия / В. Абрамов // БДИ. – 2002. – № 2. – С. 22 – 26. 9. **Андрощук Г. А.** Экономическая безопасность предприятия: защита коммерческой тайны / Г. А. Андрощук, П. П. Крайнев. – К. : Вид. Дім "ІнЮре", 2000. – 398 с. 10. **Бруксбенк Д.**, Уилсон Дж. Руководство по безопасности / Пер с анг. – М. : ЮНИТИ-ДАНА, 2003. – 319 с. 11. **Губський Б. В.** Економічна безпека України: методологія виміру, стан і стратегія забезпечення / Б. В. Губський. – К., 2001. – 122 с. 12. **Деревицкий А.** Искусство "боевого говоруна" / А. Деревицкий. – Спб. : Питер, 2006. – 192 с.: ил. 13. **Деревицкий А.** Коммерческая разведка / А. Деревицкий. – Спб. : Питер, 2006. – 208 с.: ил. 14. **До-**

нець Л. І., Ващенко Н. В. Економічна безпека підприємства: навч. пос. / Л. І. Донець, Н. В. Ващенко. – К. : ЦУЛ, 2008. – 240 с. 15. **Живко З. Б.** Конкурентна (ділова) розвідка в системі в системі економічної безпеки / З. Б. Живко. – Монографія. – Львів: АПРІОРІ, 2008. – 192 с. 16. **Живко З. Б.** Особливості кадрового забезпечення служби конкурентної розвідки в економічній безпеці фірми / З. Б. Живко, М. О. Живко, О. И. Хомин // Науковий вісник ЛДУВС: Серія економічна, випуск 2. – Львів, 2006. – С. 306 – 327. 17. **Живко З. Б.** Регламентація конкурентної розвідки в інформаційно-правовому просторі / З. Б. Живко,

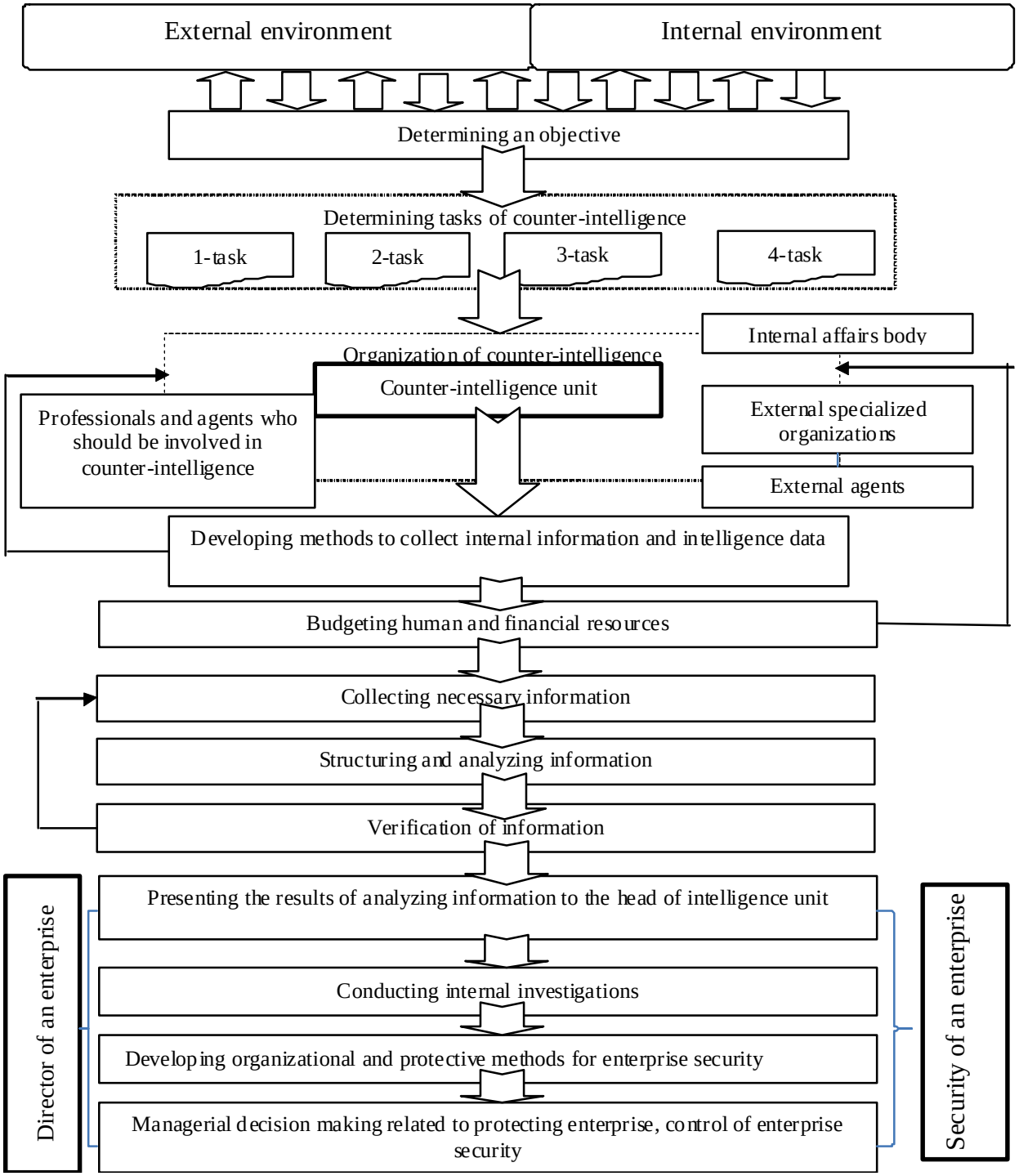

Fig. 1. Structural model of counter-intelligence of the enterprise (authoring)

М. О. Живко // Науковий вісник ЛДУВС: Серія юридична. Збірник наукових праць. – Львів, 2007. – Вип. 2. – С. 211 – 219. 18. **Живко З. Б.** Основні аспекти впливу конкурентної розвідки на недобросовісну конкуренцію / З. Б. Живко // Збірник тез Міжнародної науково-практичної конференції "Розвиток підприємництва в Україні та економіко-правове забезпечення". – Львів, 2007. – С. 88 – 91. 19. **Живко З. Б.** Економічна безпека підприємства:сутність, механізми забезпечення, управління. Монографія / З. Б. Живко. – Львів : Ліга-Прес, 2012. – 256 с. 20. **Жуков А.** Все о защите коммерческой информации / А. Жуков, М. Маркин. – К., 2002. – 120 с. 21. **Задорожний Г. В.** Економічна безпека і тіньова економіка. Монографія / Г. В. Задорожний, П. О. Іщенко, С. В. Тютюнникові. – Х. : ХІБМ, 1999. – 208 с. 22. **Збірник** методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та комп'ютерних технологій / Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь та ін. ; за ред. О. М. Джужі. – К. : ДДСБЕЗ, 2009. – С. 56 – 58. 23. **Івченко О.** Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка [Електронний ресурс] / О. Івченко. – Режим доступу : //www.justinian.com.ua/article.php?id=707. 24. **Кримінальне** право України: особлива частина : підруч. / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. ; за ред. В. В. Сташиса, В. Я. Тація. – [4-те вид., переробл. і допов.]. – Х. : Право, 2010. – С. 229. 25. **Митрофанов А. А.** Экономическая безопасность коммерческих предприятий и деловая разведка [Электронный ресурс] / А. А. Митрофанов. – Режим доступа : http://www.bre.ru/security/22843.html. 26. **Мунтіян В. І.** Економічна безпека України / В. І. Мунтіян. – К. : КВІЦ, 1999. – 463 с. 27. **Настільна** книга слідчого : наук.-практ. вид. для слідчих і дізнавачів / М. І. Панов, В. Ю. Шепітько, В. О. Коновалова та ін. – [2-ге вид., перероб. і допов.]. – К. : Ін Юре, 2007. – С. 179. 28. **Подлужная Н. А.** Выбор критерия экономической безопасности предприятия / Н. А. Подлужная // Сб. статей ДонНТУ. – № 5. – 2002. – С. 10 – 16. 29. **Сухоруков А. І.** Фінансова безпека держави: навч. посіб. / А. І. Сухоруков, О. Д. Ладюк. – К. : ЦУЛ, 2007. – 192 с. 30. **Шепитько В. Ю.** Криминалистика : курс лекций / В. Ю. Шепитько. – Х. : Одиссей, 2003. – С. 249. 31. **Экономическая** безопасность: производство – финансы – банки / под ред. В. К. Сенчагова. – М. : Финстатинформ, 1998. – 621 с. 32. **Ярочкин В. И.** Система безопасности фирмы / В. И. Ярочкин. – М. : Ось-89, 1998. – 192 с.

Пушак Я. Я., Живко З. Б. Конкурентна розвідка та контррозвідка: суміжна площина економічної безпеки підприємства

У статті розглянуто площину перетину функцій конкурентної розвідки та контррозвідки підприємства як складових системи економічної безпеки підприємства. Доведено, що документальне забезпечення правового статусу комерційної таємниці та конфіденційної інформації на підприємстві сприятиме надійному її захисту як у випадку розголошення відповідних відомостей працівниками підприємства, так і цілеспрямованими діями конкурентів щодо її викрадення. Виділено три групи типових способів злочинних посягань на відомості, що становлять комерційну або банківську таємницю та запропоновано шляхи їх локалізації; розроблено структурну модель контррозвідки підприємства.

Ключові слова: економічна безпека, конкурентна розвідка, контррозвідка, система економічної безпеки підприємства, конфіденційна інформація, комерційна таємниця.

Пушак Я. Я., Живко З. Б. Конкурентная разведка и контрразведка: смежная плоскость экономической безопасности предприятия

В статье рассмотрена плоскость пересечения функций конкурентной разведки и контрразведки предприятия как составляющих системы безопасности предприятия. Доказано, что документальное обеспечение правового статуса коммерческой тайны и конфиденциальной информации на предприятии будет способствовать надежной ее защите как в случае разглашения соответствующих сведений работниками предприятия, так и целенаправленными действиями конкурентов по ее похищению. Выделены три группы типичных способов преступных посягательств на сведения, составляющие коммерческую или банковскую тайну и предложены пути их локализации; разработана структурная модель контрразведки предприятия.

Ключевые слова: экономическая безопасность, конкурентная разведка, контрразведка, система экономической безопасности предприятия, конфиденциальная информация, коммерческая тайна.

Pushak Ya. Ya., Zhyvko Z. B. Competitive Intelligence and Counter-intelligence: Adjacent Plane of Security of the Enterprise

The article discusses the intersection of competitive intelligence and counter-intelligence of enterprise as components of economic security. It proves that the documentation of the legal status of trade secrets and confidential information reinforces its protection. The article describes three common methods of criminal attacks on information of commercial or banking secrets and discusses ways of their localization. The article also develops structural model enterprise counter-intelligence.

Key words: economic security, competitive intelligence, counter-intelligence, the system of economic security of enterprise, confidential information, trade secrets.

Received by the editors: 01.10.2013
and final form 04.12.2013