Journal of Security and Sustainability Issues *www.lka.lt/index.php/lt/217049/*
ISSN 2029-7017/ISSN 2029-7025 online
2014 Volume 3(3): 23–44
http://dx.doi.org/10.9770/jssi.2014.3.3(3)

SECURITY OF BUSINESS: COMMERCIAL SECRET'S LEGAL REGIME AND METHODS OF PRESERVATION

Aleksandrs Baikovs[1], Ivars Zariņš[2]

[1]Daugavpils University, LV-5400, Daugavpils, Latvia
[2]University Turiba, LV-1058, Riga Latvia
E-mails: [1]aleks_baikov@inbox.lv; [2]ivars@orions.lv

Received 2 October 2013; accepted 10 January 2014

Abstract. In the article, on the basis of comparative-legal analysis, there is explored the content of concept "commercial secret", considered the organisational, administrative (management), and legal measures of ensuring the safety of commercial secret, and criteria of referring information to commercial secret. The conditions of ensuring the confidentiality safety of commercial information, the methodology of selecting data constituting commercial secret, and information protection measures are sequentially analysed; the evaluation of the role of administrative information in competitive activity and authorization-based information access system is provided. In the article also the legal nature and kinds of agreements about confidentiality, as well as the content of some of them, measures of protection of commercial secret from disclosure, among which the main place is occupied by liability measures applied on law-breakers, and also basic questions on protection of commercial secret after termination of labour relationship with employee, are studied in details.

Keywords: Information, protected information, commercial (trade) secret, state secret, list of data considered to be the commercial secret, confidentiality regime, forms of confidential relationships, commercial secret regime, protection mechanism of commercial secrets.

Reference to this paper should be made as follows: Baikovs, A.; Zariņš, I. 2014. Security of business: commercial secret's legal regime and methods of preservation, *Journal of Security and Sustainability Issues* 3(3): 23–44. DOI: http://dx.doi.org/10.9770/jssi.2014.3.3(3)

JEL Classifications: K1, K2, K4, K12

1. Introduction

Efficiency of commercial activity largely depends on skills and abilities to manage such a valuable commodity as information. However, you can take advantage of only the information that is required by the market, but is unknown to competitors. Therefore, under conditions of increased competition, success of business, prospects and real profit opportunities are largely determined and depend on the extent of ensuring preservation of secrets of industrial, financial, commercial, and scientific and technical activities, based on intellectual potential, technologies and innovations of production, management, and social processes at the disposal of merchant (Grybaitė 2011; Dudzevičiūtė 2012; Lankauskienė, Tvaronavičienė 2012; Giriūnas, Mackevičius 2014). But emergence of market and development of market relations spawned unfair competition (Totyev 2000), one of the manifestations of which, according to clause 4 part 3 Section 18 of the Law of the Republic of Latvia *On competition* of 4 October 2001, is illegal acquisition, use or dissemination of information constituting a commercial secret of merchant (other market participant). Although the problems of legal regulation of information relations associated with the processes of formation and development of the information society, has become the subject of scien-

tific research, starting with the 70s, and recent years have seen tutorials on the information law (Tedeyev 2005), published monographs, doctoral researches, devoted to the analysis of the use of legal means in the Internet (Malakhov 2001), the concept of commercial secret, which is a form of information resources, is still among the least developed categories of jurisprudence. Adoption in different countries of legislative acts, which defined the legal regime of information resources, became a basis for justification of independent complex branch of law – information law, subject of which, according to the proponents of this idea, includes public relations related to the legal regulation of information turnover, its creation, storage, processing and use on the basis of communication technologies, its protection. They also, which seems to be more than justified, observed that in certain forms information is an element of any public relations, and legal norms themselves are, above all, information about the possible and proper behaviour, about the positive or negative consequences of legal and, accordingly, illegal conduct, i. e., contain legal information (Kudryavtsev 1981).

We should also note that agreeing with acceptance of information law as a complex branch of law, is quite difficult. Indeed, the very idea of separation of complex branches of law can hardly be deemed suitable, since construction of the legal system in general and allocation of one or another structural element thereof is primarily based on objective factors, first of all – economic factors. The idea of complex branches was once suggested by V. K. Raicher (1947), and was later supported by a number of scientists. Subsequently, it was repeatedly subjected to justified, quite convincingly grounded criticism. Thus, taking into account more than debatable nature of a concept of complex branches of law, as well as the fact that, in theory of information law, information, depending on its functional task, is divided into mass, industry and professional information, in structure of industry legal information one may not ignore its specific varieties – civil, commercial, labour information, etc. Each of them, of course, should be inherent in both general and specific (industry) signs of legal information. The latter are predetermined by particular subject composition (who information is about) and target orientation thereof. Taking this into account, it seems reasonable to talk about information as only an object of legal regulation of existing traditional branches of law.

Reference point of active work on legal regulation of public relations, related in one way or another to information, on international (universal) level is, obviously, approval of YUNSINTRAL Standard Law *On legal aspects of electronic data interchange and related means of communication*, which since 1996 is called *On electronic commerce*. Should be also noted here: Agreement designed to liberalize basic telecommunications (Telecommunications Annex) adopted on 15 February 1997 within the framework of the General Agreement on Trade in Services (GATS), Recommendations No 26 *Commercial use of interchange agreements in electronic data interchange* adopted on 23 June 1995 by Working Party on Facilitation of International Trade Procedures of the UN Economic Commission for Europe, EU Commission Recommendations 94/820/EC of 19 October 1994 concerning legal aspects of electronic data interchange.

2. Concept, signs, and legal nature of commercial secrets

In theory of information law, information is traditionally subdivided into proprietary information, information for official use, restricted access information, information for free use. Law *On transparency of information* of the Republic of Latvia of 29 October 1998 marks out publicly available information and restricted access information (Sec. 3). Sec. 8^1 of the same legislative act mentions information for official use. Proprietary information is usually only available for a very narrow circle of enterprise's officials. Information for official use may not be transferred by employees possessing it to other enterprise's employees, as well as to third parties. Restricted access information assumes existence of certain persons, who have limited or denied access to information, which constitutes or may potentially constitute enterprise's commercial secret.

Commercial secret is a form of security provision for the most important commercial information, which provides for limitations of its dissemination. From legal point of view, it is generally accepted that enterprise's commercial secret is a means of protection against unfair competition in the framework of realization of intellectual property rights. Minimum international standards for protection of commercial secret are established in some conventions and in Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), which is the largest

multilateral international agreement aimed at ensuring protection of commercial secret. The need to establish measures of legal protection of information of commercial value has led to the emergence in Latvia of institute of commercial secret protection. However, unlike such countries as the USA, Germany, China, Ukraine, etc., which have adopted separate legal acts of almost the same name, norms of this institution are scattered across different legal acts. However, literature has repeatedly expressed opinion on necessity of a special law on commercial secret protection. According to Sec. 19 of The Commercial Law of the Republic of Latvia of 13 April 2000 (hereinafter – CL), commercial secret is understood as things of economic, technical or scientific nature related to merchant's enterprise and information, recorded in written or other form or not recorded, with actual or potential property or non-property value, which, at disposal of other persons, could harm merchant, and in respect of which merchant takes reasonable measures for maintenance of secrecy. Thus, concept of commercial secret, formulated in this Section of CL, generally coincides with definitions contained in legal acts of Russia (cl. 1 Sec. 139 of The Civil Code of Russian Federation) and other industrial developed countries. Descriptively, not pointing to constitutive signs and focusing on possible adverse effects of its disclosure, commercial secret is interpreted by Sec. 7 of the mentioned law on openness of information. According to norm-definition laid down in it, a commercial secret is information created by and belonging to a merchant, disclosure of which could have significant negative impact on merchant's competitiveness. Commercial secret is characterized as one of the types of restricted access information except when a procurement contract in accordance with the Law on Public Procurement of the Republic of Latvia of 6 April 2006 or other contract on disposition of public funds or municipal funds and property is concluded (cl. 3 part 2 Sec. 5).

Carriers of commercial secret are material objects, including physical fields, in which information constituting a commercial secret is reflected in form of symbols, images, signals, technical solutions and processes. In order to be considered a commercial secret, information must simultaneously satisfy the following three criteria: (1) information must have actual or potential commercial value when it's unknown to third parties, (2) it must not have access on a lawful basis, and (3) information owner takes measures to protect its confidentiality. Subject of commercial secret is information related to enterprise's commercial and economic activities: industrial and technological information, management information, financial information and information on other activities. This can be documents of enterprise's commercial negotiations and pricing methods, documents related to marketing research, information on work organization and selection of employees, information on conditions of document storage, i. e. information with commercial value.

Commercial secret is one of the objects of intellectual property, to a certain extent being the result of creative activities and having a number of specific features, most notably: (1) de facto monopoly of commercial secret owner to a certain body of knowledge, (2) the highest, in comparison with other objects of intellectual property, versatility, since the volume of concept of commercial secret is so vast, that it can include any information related to production, management, finance, commercial activities, innovation etc., (3) unlimited period of its protection. Title to a commercial secret lasts as long as person's de facto monopoly to information, which it consists of, is maintained and statutory conditions for its protection exist. This condition makes selection of this form of protection attractive to merchants in cases where they are not satisfied with urgency principle of patent protection, and (4) necessity of official recognition of its eligibility, public registration or settling any other formalities, etc. We should agree with A. P. Sergejev (2003), who claimed, commercial secret has all the properties of an object of intellectual property and is a special kind thereof. Scientific literature expresses a point of view, according to which objects of intellectual property rights are essentially objects of property law (Kulagin 1992). However, a more appropriate to the nature of intellectual property rights is its understanding as of not a corporeal, but a kind of absolute right. As V. F. Popondopulo (2006) rightly writes, use in this case of the term "property" emphasizes not so much identification of creative result with the thing (it is not a tangible good), as quality of absoluteness inherent in intellectual property right. At the same time, owner of intellectual activity result owns right of possession, use and disposal of information constituting its content. This fact does not imply the identity of property right. Features of intellectual property right are expressed differently: if objects of intellectual property right are usually subject to special registration, they are characterized

with temporary and spatially limited nature of legal protection, then objects of property right are in most cases not subject to special registration, and property rights themselves are not limited in time or any territory of their validity.

Besides commercial secret, we should mention state secret, official secret and bank secrecy. According to Sec. 2 of the law *On state secret* of the Republic of Latvia of 17 October 1996, state secret is a secret information of military, political, economic, scientific, technical or other nature, disclosure of which may cause damage to interests of the state in the field of security, economy and politics. One of the specific types of commercial secret is banking secrecy. More precisely, nowadays legislator, obviously, taking into account complex nature of relations in connection with ensuring confidentiality and non-disclosure of information constituting a secret, as well as guided by desire to extend regulations, which govern relations in this connection, to all types of credit institutions, does not use this term, using a broader concept of *limited access information* in legislative acts, such as the Law *On credit institutions* of the Republic of Latvia of 5 October 1995 (Sec. 100[1]), the Law *On Financial and capital market commission* of the Republic of Latvia of 1 June 2006. It is information, access to which bank, in accordance with the law, is entitled to restrict. Banks usually work with many clients, depositors, correspondents whose interests may be negatively affected by disclosing information about their operations, transactions, accounts, etc. Moreover, threats may come from both competitors and criminal organizations. In this connection, there is a need to protect information held by banks, including information about activities of persons using their services.

Features of legal regime of banking secrecy lie in the fact that (1) analysis of part 5 Sec. 62 implies that it is information not subject to disclosure and not constituting state secret, and (2) list of information to be included in it is defined not only by law. Moreover, banks themselves may include some of the information they possess in the category of bank secrecy (if it does not contradict the law). According to part 1 Sec. 62 of the Law *On credit institutions* of the Republic of Latvia of 5 October 1995; credit institution's duty is to guarantee privacy of clients, their accounts, deposits and transactions. Employees of the bank must maintain banking secrecy, respecting the so-called *rule of the wall*. Information constituting bank secrecy may only be provided to clients themselves or their representatives. State bodies and officials thereof may only be provided such information in cases and according to procedure provided for by law.

Banking secrecy has traditionally been viewed in two senses: broad and narrow. In broad sense, information constituting bank secrecy is a specific kind of commercial secret, i. e., confidential information owned by the bank. But if it is viewed in narrow sense, it appears in form of bank's duty to keep accounts and transactions of its customers and correspondents secret and not to allow banking operations to become known to improper parties and, above all, to competitors of its clients. Said above indicates very significant differences between banking secrecy, in its narrow concept, and commercial secret. It appears that these differences may be summarized as follows:

1) absolute nature of relationships in connection with ensuring maintenance of commercial secret (right holder, carrier of information constituting commercial secret, on one part, and unlimited sections of public not entitled to familiarization with this information), and relative nature of relationships in connection with ensuring confidentiality of information constituting banking secrecy (bank being obliged person and client as entitled person);

2) information constituting commercial secret is purchased for performance of certain activities, usually on the basis of a license agreement. In turn, provision of client with information constituting bank secrecy is carried on the basis of an accessory agreement (additionally to the basic one);

3) with respect to commercial secret, it is crucial to ensure inaccessibility of third parties to it as such, i. e., to create conditions that rule out possibility to familiarize with information constituting it per se, and in relation to bank secrecy – to ensure non-disclosure of existence of the very fact of such secret, i. e., existence of the fact of relationship between the client and the bank;

4) transfer of information constituting commercial secret to third parties is performed to obtain some benefit, and transfer of information constituting bank secrecy (client to the bank, and bank to third parties) has coercive nature;

5) right holder of commercial secret is taking measures to ensure its non-disclosure in order to obtain

competitive advantage and, ultimately, profit. Banking secrecy is protected by the bank by virtue of the assumed obligation to ensure its safety, failure to fulfil which results in liability;

6) information containing commercial secret may be disclosed to persons interested in receipt thereof on contractual basis for a fee. In contrast, purchase or sale of information containing banking secrecy is always illegal;

7) information containing commercial secret retains its status (secret status) in respect of all persons. In turn, banking secrecy only retains this status in respect of persons, to which person, which entrusted confidential information to the bank, has not communicated it.

Considering the said above, banking secrecy in narrow sense cannot be considered as a kind of commercial secret. In V. Zemljanovs (2005) opinion, it is more correct to qualify it as a kind of professional secret. It is interesting to note that special legislative acts aimed at protection of interests of manufacturers, their owners and states from a possible leakage of secrets were adopted even in antiquity. For example, in ancient Rome a law was adopted, which provided for a penalty equal to twice the value of caused losses for forcing somebody else's slaves to disclose secrets of their master (Novickiy 1996). Legal norms providing for liability for disclosure of valuable confidential information were contained in Russian Penal Code of 1845. Chapter VIII of the Code *On crimes and misdemeanours against social order and decorum* included sections dedicated to liability for disclosure of classified information (Sec. 1157, 1187, 1355). Criminal Code of 1903 included Chapter XXIX *On disclosure of secrets* consisting of 6 sections, dedicated to liability for disclosure of various kinds of secrets, three of which concerned, respectively, factory, commercial and credit secrets. Code did not specify content of commercial secret concept, but apparently it concerned secret of trade books, constituting, in G. F. Shershenevich's words, *undiscloseable commercial secret*. Moreover, except in cases listed in the law, including: (1) disputes in partnership issues, (2) disputes in inheritance issues, and (3) insolvency, no one, under any pretence, could claim disclosure of these books (Shershenevich 1994).

Information used in commercial activities is traditionally divided into two types: industrial and commercial. Industrial information includes information about technology and method of production, technical discoveries and inventions, know-how, design documentation, software, etc. Commercial information is information about financial and economic situation of the enterprise (financial statements), credits and banking operations, concluded contracts and contractors, structure of capital and investment plans, strategic marketing plans, analysis of competitiveness of own products, customers, plans of production development, business correspondence, etc. On the basis of function and target, the following necessary components of commercial secret can be specified: (1) business information – about contractors, competitors, consumers, business negotiations, commercial correspondence, concluded and planned contracts, (2) scientific and technology information – content and plans of scientific research, know-how, rationalization proposals, implementation of new technologies and products, (3) manufacturing information – technology, product roadmaps, scope of work in progress and inventory, plans of investment activities, (4) organizational and management information – information about firm's management structure not contained in articles of association, original methods of management organization, labour organization system, (5) marketing information – market strategy, plans of promotional activities, provision for competitive advantages in comparison with products of other companies, methods of working in markets, plans of production distribution, analysis of competitiveness of products, (6) financial information – planning of profit, cost, pricing (calculation methods, structure of prices, discounts, possible funding sources, financial projections), (7) information on firm's personnel – personal files of employees, plans to increase (reduce) personnel, content of tests for new employees, and (8) software – programs, passwords, access codes to confidential information in electronic data carriers.

Usually, competitors, partners, banks, criminal communities are most interested in the mentioned information. Information constituting commercial secret may exist in paper form, on floppy disks, CD's, hard disk drives, in memory of enterprise's employees. Regulation of relations connected with use of confidential information must begin with the main document of the Company owning respective enterprise, with articles of association, which give the concept of commercial secret and establish liability for failure to observe it. All this information has dif-

ferent value for merchant, and its disclosure may cause adverse effects of varying degree on enterprise's economic security.

Let us examine criteria of protectability in more details. According to the first criterion, information must have actual or potential commercial value due to the fact that it is unknown to third parties. In this regard, it should be noted that (1) as a commercial value, literature understands ability of information to be object of market turnover, (2) commercial secret itself includes information, use of which gives its holder certain economic benefits due to the fact that its competitors do not have such information, (3) commercial secret includes information of interest to third parties, which could get specific benefit in case of having this information. As third parties in this case should only be understood persons carrying out commercial activities, and (4) information constituting commercial secret must have not only actual, but also potential commercial value.

The next criterion, which information must comply with, in ordered to be considered a commercial secret, is that this information must not be legally freely accessible by third parties. This means that information must not be generally known. As *generally known* is to be understood what is known to indefinite sections of public and available for perception of anyone interested. Generally known information, even if it has a great commercial value, in principle, cannot be considered commercial secret. However, it seems, in exceptional cases such information will still be recognized a commercial secret, if secret is the fact that enterprise uses this very method or device and therefore achieves the greatest success. At the same time, emphasis may be placed on words *free access*. Legitimate way of obtaining information is its obtaining from publicly available sources (advertising brochures, periodical publications, scientific presentations, etc.). However, free access possibility does not mean that as soon as one or another piece of information is made available for third parties, it loses status of commercial secret. The very fact of free access does not automatically mean loss of status of commercial secret. Due to free access possibility, noteworthy is the question of whether combination of generally known data can be considered a commercial secret. There are different opinions in this regard. According to one of them, sometimes a new combination of already generally known data is sufficient for commercial secret. Another is that simple combination of obvious and well-known data does not meet the requirement of not generally known information and is not protected, even if such set of data can be valuable and useful. On one hand, indeed, generally known cannot become not generally known by the will of one person, and if any information is known to everyone, commercial benefit from use thereof is questionable. But if, for example, someone discovers that specific combination of generally known data gives unexpected positive results, it appears that such combination may still be considered a commercial secret. Commercial value of using such combination of data can be quite great, on the other hand, the fact that exactly such combination can give certain effect is not generally known. You can draw here an analogy to patent law, where as invention, in particular, is recognized use of known substances, combinations thereof, for a new purpose (part 4 Sec. 5 of *Patent Law* of the Republic of Latvia of 15 February 2007. Thus, in passing verdict, court of an American state pointed out that, although all essential elements of the process were known previously, combination making use thereof economically feasible was not known (Shamkhalov 1993).

Concept of *access* can be seen in broad and narrow sense. In broad sense, access means availability of information, possibility of free obtaining thereof by anyone. In a narrow sense, access can be understood as possibility of obtaining information constituting commercial secret from their owner, based on legislative or contractual norms for using for a particular purpose, which must be specified in these norms (Kuzmin 1993). This kind of access is some kind of removal of subject to information from the monopoly. Access can be based on voluntary or mandatory basis. Holder of commercial secret can voluntarily provide access to classified information to his contractors under contracts. In particular, this may occur when information is transferred under contract to interested persons. Mandatory provision of access is connected with possibility of reclamation of information constituting commercial secret by various public authorities in course of performance of their duties.

It appears that demands of public authorities to provide information constituting commercial secret are legitimate to the extent they are claimed in course of performance of their functions entrusted to them by law and in scope justified for implementation thereof. Simultaneously, right of public authorities, as well

as municipal authorities, to reclaim information constituting commercial secret, must only be provided to respective authorities by law or legal act defining status of such authorities, their competence, basic rights and duties. Possibility of obtaining information constituting commercial secret by public authorities and their employees shall not cause loss by this information of status of commercial secret: information must not become publicly accessible due to this, since only specific persons in specific amounts have access to it, and it does not make it available to general public.

The third criterion, which information constituting commercial secret must comply with, is measures to protect its confidentiality taken by the owner. These measures are three-fold: (1) officers and employees of the company - right holder must be obliged to observe commercial secret, should be notified of their obligation not to disclose information about it to third parties, of classifying respective information as commercial secret, and of liability for non-observance; (2) contract with its contractors, by which right holder transfers respective information, must provide for their duty to refrain from transferring this information to third parties, inform them that this information constitutes commercial secret, and establish liability for breach of this secret; (3) right holder must take measures to prevent unauthorized access to commercial secret by third parties, in particular, to prevent industrial espionage. Failure to comply with these conditions can be an obstacle to recognition of protection as existing. Existence of protection measures is perhaps the most important criterion for protectability. For example, US courts, in disputes concerning infringement of commercial secret, require plaintiff to prove that he was taking measures to protect information. When implementing protection of confidentiality, requirements of reasonableness must be respected. Moreover, all measures to maintain secrecy of information can be conditionally divided into three major groups: technical, organizational and legal.

However, not all information held by merchant can be categorized as commercial secret. Commercial secret is not: (1) constituent documents (articles of association, memorandum), (2) documents giving right to engage in commercial activities (registration certificate, licenses, certificates, patents), (3) information on prescribed forms of financial statements necessary to verify correctness of calculation and payment of taxes and other mandatory payments to the state budget, (4) documents on solvency; (5) documents on payment of taxes and mandatory payments, (6) information on compliance with norms of labour protection; (7) information on compliance with environmental protection norms, (8) information on violation of the antimonopoly legislation, (9) information on sale of products that caused harm to human health, and (10) information on involvement of company's officials in other companies engaged in commercial activities. But this information also is not intended for public access to all interested. For example, information on remuneration of enterprise's employees, financial statements may only be submitted on request of public authorities, management, regulatory and law enforcement authorities, sworn auditors, eligible in accordance with the current Latvian legislation. At the same time, firm's clients may get acquainted with its articles of association, registration certificate, licenses, certificates, patents. Merchant himself defines list of objects of commercial secret and methods of protection against availability to third parties.

2. Subjects and content of subjective right to commercial secret

Commercial secret, as object of intellectual property protected by law, does not exist outside of activities of enterprises owned by merchants and is inseparable from them Accordingly, subjects of a right to commercial secret are merchants, i. e., physical persons (individual merchants) and legal entities (personal companies and capital companies), engaged in commercial activities, i. e., open economic activity for profit (Sec. 1 of CL). In general theory of law, subjective right is most often represented as a unity of three authorizations: (1) on own positive actions, (2) requirement from obligated person of performance of their responsibilities, and (3) on protection, which is expressed as the possibility to appeal to competent authorities for application of state enforcement measures in case of violation of subjective rights. However, as much interesting is the point of view that the entitlement to protection is a separate subjective right only arising for a right holder at the moment of violation or challenge of his right and realized in the framework of protective relationship appearing on this basis (Pokrovsky 1998).

Subjective right to a commercial secret is owned by its owner – a natural person or legal entity lawfully

possessing information constituting a commercial secret and associated right in full. Specificity of a right to commercial secret is that this right simultaneously is a duty, because the very possibility to protect information constituting a commercial secret depends on presence or absence of measures for its protection. Circle of entitlement to own positive actions includes authority to use information constituting a commercial secret, which suggests possibility of undertaking any actions by the owner of commercial secret for its use and application in their commercial activities. Owner of a commercial secret holds authority to disseminate information, i. e., to open access to information to third parties. Transfer of the right to use information to confidant of a commercial secrets (natural person or legal entity, who by virtue of official position, contract or legally knows another person's commercial secret) takes place on the basis of license agreements, which are agreements of a special kind (*sui generic*), but not devoid of similarities with purchase, lease contracts. Finally, holder of a commercial secret has the right to dispose of confidential information belonging to him. This can be expressed in ending regime of secrecy of this information – holder of a commercial secret may at any time disclose information constituting a commercial secret to the public, if it does not violate rights of third parties, which entails termination of existence of commercial secret as an object of right. In addition, holder of a commercial secret may at any time destroy information belonging to them: by destroying documents, material carriers, on which information are recorded, etc.

Authority to require from third parties to refrain from misappropriation of information constituting a commercial secret shows another specificity of rights of holder of a commercial secret: protection is only provided against appropriation of information by illegal means. If information is received by third parties legally, they will not be deemed violators of rights of holder of a commercial secret. Legal protection of a right to commercial secret arises from the establishment of de facto monopoly of the holder to information constituting a commercial secret (in accordance with requirements established by law), and is valid indefinitely for the entire period of compliance with these requirements to a protected secret. Protectability of rights to a commercial secret does not require state registration and is only checked when rights to a commercial secret are violated (challenged).

Thus, holder of a commercial secret has the following rights and duties: (1) to determine independently criteria for classifying newly obtained information as a commercial secret, duration and scope of measures necessary to ensure regime of commercial secret regarding information already received and being received, including registration and removal of classification *Commercial secret CS*, definition of procedure of access to commercial secret, selection and use of means and methods of protection, storage and transmission of information constituting a commercial secret (except as permitted by applicable law), (2) to establish, modify and cancel regime of commercial secret (if it does not violate obligations assumed under contract), including with regard to know-how. Rights to know-how, as to an unconventional object of intellectual property, which are not subject to exclusive rights, must also be protected in regime of commercial secret, (3) to require provision of regime of commercial secret from persons, who gained access to commercial secret legally to ensure their de facto monopoly to this commercial secret (including consolidation of such obligations in license agreements and other agreements, special confidentiality agreements), and (4) to allow (cancel) access of employed person, with their consent, to a commercial secret on contractual basis.

Admission of the employee to information constituting a commercial secret involves: (1) familiarization of employee with norms of applicable legislation on commercial secret, providing for liability for violation of regime of commercial secret, (2) familiarization of employee with employer's developed and approved list of information constituting its commercial secret, which employee will have right to access in order to fully carry out their work function, (3) adoption by employee of commitments to employer to comply with established regime of commercial secret, including on non-disclosure of commercial secret after dismissal during period established by law or contract, and (4) determination of employee's wage, providing for compensation for a duty to comply with regime of commercial secret. Amount of such compensation may be established by a separate agreement. Simultaneously employee may seek judicial review of measures taken by the holder to ensure regime of commercial secret regarding information, which is known to him (may become known because of his employment relationship with employer).

Subject of a right to commercial secret is entitled to (1) insist on compliance with regime of commer-

cial secret by persons who gained access to it in result of circumstances, which right holder could not foresee or prevent. Simultaneously, party, which has taken obligation not to disclose commercial secret, is entitled to receive remuneration in money from holder of commercial secret, (2) ask for protection of commercial secret when received lawfully by officials of government bodies and local authorities in regime of official secret in accordance with the law, for the whole duration of its legal protection, (3) to dispose of commercial secret in sole discretion, including use thereof in own production, transmission to other persons on the basis of contracts, issue to other persons of licenses to use commercial secret in own commercial activities, as well as other ways to incorporate the mentioned confidential information in civil circulation, and (4) require from third parties to refrain from improper obtaining of confidential information, illegal access and use of commercial secret (industrial espionage, bribery, threats, misrepresentation of employees, theft of documents, interception of negotiations, review of correspondence, violation or instigation (coercion) to violation of obligations of complying with regime of commercial secret, as well as other illegal means of transferring commercial secret to third parties without permission of the holder of commercial secret. Part 2 Sec. 200 of The Criminal Law of Latvia provides for imprisonment for up to 5 years, or arrest, or compulsory labour, or a fine of up to 100 times minimum monthly wage. German law on unfair competition provides for criminal liability of up to three years of imprisonment for disclosing to unauthorized persons of information constituting commercial (industrial) secret (Bergmann, Dubovickaja 2005). When exercising rights, holder of commercial secret must comply with the following conditions: (1) not to violate the legally protected rights and interests of other persons, (2) not to use for protection of commercial secret means that can cause harm to human life and health, (3) to take measures to ensure confidentiality of information constituting a commercial secret, (4) to provide information constituting a commercial secret to public authorities, local governments, law enforcement agencies upon their request within their competence established by law under penalty of administrative liability, and (5) to take measures to classification of information, which used to constitute a commercial secret, but is classified in accordance with the law as a state secret (with the right to receive appropriate compensation). Responsibility to prove right to a commercial secret and illegality of violator's actions in respect of such information rests with the holder of this commercial secret. If he cannot prove these circumstances, his subjective right is not subject to protection.

In civil proceedings, holder of a commercial secret independently determines ways to protect right to a commercial secret and is entitled to require violator to: (1) recognize right to a commercial secret (if this right is challenged), (2) indemnify for disclosure on part of employees and contractors, contrary to provisions of employment or civil contract, or on part of persons, who gained access to commercial secret illegally, (3) pay, on discretion of court, compensation in case of impossibility to determine amount of damage or injury caused by violation of a right to commercial secret, (4) annul act of public authority or local government, and (5) take other measures provided for by valid legislation protecting their rights. If rights of the holder of a commercial secret are violated by public officials (of tax, regulatory, law enforcement authorities, etc.), who have access to such information in cases provided for by law, norms of administrative responsibility must apply.

3. Legal regime of commercial secret in the enterprise. Sources of confidential information

Number of issues must be resolved in organization of protection of commercial secret, the first of which is definition of information constituting a commercial secret, as well as the possible distribution thereof by categories of importance, depending on value thereof to the enterprise, nature and extent of the damage that may be caused to him by disclosure of this information. As a result, company develops a commercial secret, which is a system of legal, organizational, technical and other measures taken by the holder of a commercial secret and confidant thereof to provide limited access to respective information.

All available information may be distributed by degree of confidentiality, depending on extent of negative consequences that may arise in case of its loss, as follows: (1) the highest degree of confidentiality – information is key in activities of enterprise, loss or disclosure of this information usually causes an irreparable damage, a consequence of which may be its liquidation, (2) strictly confidential information, leakage of which can cause very severe conse-

quences. This is information on strategic plans, prospective agreements, etc., (3) confidential information –disclosure thereof inflicts damage to society, comparable to current costs, but in a relatively short time, it can be overcome, (4) limited access information – leakage thereof has a slightly negative impact on the economic situation of the company (job descriptions, management structure), and (5) public information – dissemination thereof does not threat economic security of the company. On the contrary, absence of such information can have a negative impact on economic situation of the company.

For differentiation of information that needs to be protected, one can use the following criteria: (1) likelihood of threat to economic security of the firm. In case where competitors gain such information, firm will suffer economic damage. In case of disclosure of such information, firm will face serious economic difficulties, (2) possibility to protect information. If, for example, information is not included in mandatory list of public nature, one must define if there is a possibility to protect it by general or special means of protection, and (3) the economic feasibility of protection of information.

Sources of information constituting a commercial secret and, hence, potential sources of leakage thereof can be: staff of the enterprise, enterprise documentation, technology processes, communications, etc. Staff of the enterprise is the most vulnerable source of confidential information. Exactly staff of enterprise has invaluable commercial information, disclosure of which leads to a loss of competitive advantages, hard to restore negative consequences. Migration of specialists, especially those who have dealt with confidential information, is the main and difficult to control channel of information leakage. Quantitative and qualitative characteristics of personnel allow interested parties by using analytical calculations to draw conclusions on some of its other parameters – on labour productivity and, thus, level of production, on availability of contacts with suppliers or customers who purchase products or use services of the company. Such risks must be assessed depending on the nature of commercial activities. Perhaps, in some industries information openness of such kind may have rather positive than negative consequences. No secret that most part of losses of the enterprise is by the fault of employees or with their participation. In addition to purely criminal interests, employee can use knowledge of internal structure to solve their personal problems, such as revenge to superiors, promotion due to discredit of opponent or provision of stable workplace not burdened with responsibilities. In this regard, safety of confidential information largely depends on proper selection, placement and training of personnel.

Second most important channel of leakage of confidential information is documentation of the enterprise (incoming, outgoing, orders, business plans, business correspondence, various publications in mass media, deposited manuscripts, monographs, information on financial activities). Obtained information about principles of enterprise management provides insights into applied and, possibly, prospective methods of production management, facts of negotiations, objects and purposes of conferences and meetings of competitor's controls, enterprise's plans to expand activities of execution of works, provision of services and production, conditions of merger, acquisition, spin-off and associations of companies related to the whole enterprise. Methods of production management are know-how in the field of self-management. And because efficiency of the entire enterprise directly depends on how efficiently administration performs operative management and enterprise management, since principles and methods of management are object of commercial secret, which is most highly exposed to leakage to competitors or contractors in form of concentrated information. Enterprise's products are a special source of information, characteristics of which are very actively sought by competitors. Particularly noteworthy are new products being in preparation for production. It is considered that there are certain stages of *product life cycle* for products: idea, model, prototype, testing, mass production, operation, upgrading and removal from production. Each of these stages is accompanied by specific information manifested by a variety of physical effects, which in form of camouflaging signs may disclose protected information. Volume and assortment of manufactured products or specifics of provided services is one of the most important economic characteristics of the enterprise.

Marketing research performed by enterprise, as well as experiments related to attracting potential customers to manufactured products or provided services are of interest as a finished product of information obtained in course of economically costly activities. Information of this kind must be protected especially carefully,

because exactly with the help of this information enterprise can achieve substantial increase in profitability of its activities, increase its share in commodity markets and service markets. Technical means as a source of confidential information is a broad and capacious group of sources in terms of information. Group of means of ensuring production activities includes a variety of means, such as, in particular, telephones and telephone communications, televisions and industrial television equipment, radio receivers, radio broadcasting system, public address system, amplification systems, security and fire safety systems, etc., which, by their parameters, can be sources of transformation of acoustic information into electric and electromagnetic fields capable of forming electromagnetic channels of leakage of confidential information. It is also necessary to mention safety of data circulating in enterprise's internal computer networks, both wired and wireless. Network security objectives may vary depending on the situation, but usually there are three main objectives: (1) integrity, (2) confidentiality, and (3) availability of data. Priority is confidentiality of data being object of protection.

The next possible source of information leakage can be partners, contractors or customers, who are using or have used company's services and often hold important secrets. Therefore, when analyzing protection system, they deserve special attention. Special channel of information leakage, at least, its commercial value, are collaborations with other firms, contacts with customers and investors, where negotiations occupy a special place (Bellanger 2002). Contrary to stable misconceptions, most of information is extracted from indirect sources (garbage, advertising, publications in press). This source is usually not given much attention, consequently, it is the most accessible. For example, production waste, as well as various publications, can tell a lot about the materials used, their composition, production peculiarities, and technology. Among other pieces of information, which are object of enterprise's commercial secret, can be directly distinguished: (1) important elements of security systems, codes and procedures for access to information networks and centres, and (2) principles of organization of protection of commercial information and commercial secret in the enterprise.

4. Problems of functioning of legal mechanism for protection of commercial secret in the enterprise

The main factor contributing to protection of information circulating in the enterprise, are classified, i. e., special measures aimed at preventing diversion of specific information. Special measures aimed at protection of intellectual property depend primarily on the holder (holders) of information competitive circumstances emerging in environment of their activities, value of manufacturing or commercial information, and other factors. Certainly, to keep a secret, when it is only known to holder thereof, is not difficult and costly. Information carrier (document, floppy disk, and object) must have adequate storage place (safe or other place inaccessible to other persons). Slightly more complicated is protection of this information, when presence thereof becomes known to interested parties. It becomes necessary to restrict access of unauthorized persons to the place of storage of classified materials.

Enterprises, firms, associations, where there are several holders of information, especially where there are employees not admitted to production, commercial secrets, are a more difficult object of protection. It raises a question of the necessity to provide for internal and external security. In order to solve it, one can use commercial firms providing security services and, of course, own security service. Important place in the system of organizational, administrative, legal and other measures, which allow solving tasks of information provision for scientific and commercial activities, physical safety of material carriers of classified information, prevention of their leakage, preservation of commercial secret, is occupied by licensing system of access of performers to classified documents and information. Access is understood as obtaining a written permission of enterprise's manager (or, under his authority, other senior officials) for issuance of specific (or all pieces of) classified information to an employee, taking into account their duties (of authorities). Provision for preservation of confidential commercial information requires compliance with the following conditions: (1) determination (identification) of information constituting enterprise's commercial secret, (2) development of procedures for protection thereof, and (3) ensuring compliance with such procedure.

5. Methodology for separation of information constituting a commercial secret

Procedure of allotment of the most valuable pieces from the total volume of enterprise's own information for subsequent protection is closely linked to process of production of goods (services) and derived from the practice of competition. Factors determining competitiveness of the enterprise can only bring positive results if they are hidden from economic rivals. Therefore, assignment of such information to a commercial secret is a form of protection, economic security of the enterprise by decree of the manager. This decree lists information relating to commercial secret. Essence of forming methodology of allocation of valuable information lies in logic of actions and features characterizing a commercial secret.

After deleting information constituting state secret, as well as publicly known information, from information sources two types of information can be distinguished in the remaining information volume: (1) technology, management, and (2) business (financial and commercial) information. Some information, taking into account feasibility and commercial benefits, is secured by the Patent Law of the Republic of Latvia of 15 February 2007 and the law *On copyright* of the Republic of Latvia of 6 April 2000, as well as by major international conventions governing these provisions. After consistent performance of the mentioned actions, object of analysis and evaluation is a part of information unprotected by patents and copyright, as well as commercial and financial data. Key to understanding, protection of what information as a commercial secret is instrumental in specific period is competition (price and non-price based). That is why it is advisable to classify information, which gives (can give) significant advantages in competition, as a commercial secret. Disclosure of this information causes economic damage due to loss of competitiveness of enterprise's goods and services. American businessmen believe that loss of 20% of information leads to firm's ruin within a month in 60 cases out of 100 (Solovjev 2002).

Further is performed analysis and evaluation of spheres and cycles of production of goods, in which innovations are possible: product, service, marketing, production, distribution, financing, management, social sphere. In each of these areas, based on the analysis, amount of innovations required for successful operation is determined in percents. The largest volume of information constituting a commercial secret (innovations affecting competitiveness) lie in the following areas: product, marketing, production, service, management. Considering production cycle from the perspective of protection of commercial secret, it should be noted that most firms can achieve dynamic growth and financial and commercial success by successive improvements. Taking into account market peculiarities, commercial secret must include information on improvements of manufactured products, including technology and other issues (and not just significant innovations). Arrangements for protection of information must include problem of differentiation of product quality compared to competitors' products. At the stage of product development, specific value will be represented by information about its properties, providing a significant difference from products existing on the market. This is the most valuable information of the enterprise (firm) constituting a commercial secret. In purchases, one is guided not only by price, but also by indicators of product differentiation achieved by efficient design. Efforts of enterprises are aimed at improving price significance of own products in customer's eyes and at intensification of the differences between own products and competitor's products. In this regard, it is advisable to make an exhaustive list of own product properties, and then to ask which of these properties after improvement would provide it with the most competitive difference. Exactly these facts are more likely to be classified as a commercial secret.

Assessment of the role of management information in competition for obtaining advantages over economic rivals allows including range of information from these activities of the enterprise in the list of data constituting a commercial secret. Significant economic damage may be caused by disclosure of a commercial secret on the stage of testing the developed product on the market. The most important in the process of market testing is to assess attractiveness of the product for consumers. It is necessary to ensure protection of such information that would facilitate the adoption of appropriate countermeasures by competitors. Usually, at this stage should be protected product trademark, name of the company conducting tests, test results, time of start of product mass production, etc. To hold or gain enterprise's market position, actively is used advertising, in which it is important to prevent disclosure of valuable information, since, after gaining it, competitors can make necessary adjust-

ments in the process of competition. Proven method of advertising, providing for protection of a commercial secret, is the so-called black box method. Simultaneously, problem is being described, achieved results, gained advantages are shown, but how this is achieved is disclosed in truncated form, with extreme caution. In recent years, in industrialized countries, security services began to take measures to protect information, which rival firms may obtain in the analysis of waste products entering disposal or market. The main form of protection is to keep secret information on enterprises supplying raw materials by firms specializing in sale of industrial waste.

Particular attention should be paid to protection of contracts concluded by merchant. Most of them belong to a commercial secret. Moreover, in certain cases protected is not only text of the contract, but also fact of conclusion thereof. Not disclosable is information, disclosure of which may lead to adverse effects (home phone numbers, addresses of employees, work plans, information on conflict situations in a team). The first step to be made by merchant, who wants to keep production or technological secrets, is to develop a list of information constituting a commercial secret of the enterprise, as well as to approve Regulations on procedure for securing commercial secrets of the enterprise. Documented commercial secret of the enterprise, expressed in a certain volume of data, acquires, under part 1 Sec. 83 of the Labour Law (hereinafter LL), status of *information constituting a commercial secret of the employer* and is employer's property.

In order to make a decision on inclusion of data on enterprise's activities in the list of information constituting a commercial secret, it is advisable on the first stage to define possible negative consequences in the event of disclosure. Negative consequences include: termination of business relations with partners, failure of negotiations, loss of possibility to conclude a lucrative contract, reduction of level of cooperation with business partners, failure to fulfil contractual obligations, necessity to perform additional market research; rejection of decisions that have become inefficient in result of information disclosure and necessity to take additional measures related to financial costs, use of obtained information by competitors to improve efficiency of economic competition, loss of possibility of patenting and licensing; improving technology; reduction in product prices or decline in sales; damaging firm's credibility, reduction of economic security; advance by competitor of output of similar product to the market; worsening of crediting conditions, emergence of difficulties in supply, purchase of equipment, dismissal of enterprise's leading specialists.

To avoid errors, it is necessary to take into account additional criteria for classifying information as a commercial secret. The most common of these are: time gain for the enterprise in comparison with competing firms, unique design, novelty (new consumption function, new technology, application in new areas); advantages in technical and economic characteristics of the product over competitor's products, original use of materials, technologies; advantages in price competition; significant labour costs in obtaining information; enterprise's monopoly to information in this direction of industrial and commercial activity; degree of evidence of use of information by competitors in case of its publishing; prospect to obtain information, hidden by competitors, independently and term of obtaining; emergence of opportunity to enter the international market; degree of influence on formation of positive image of the company by consumer; ability to ensure safety of information in the enterprise in the case of its classification as a commercial secret.

Structure and content of the list of information constituting a commercial secret depends on characteristics of the enterprise. List should specify terms of revision of information constituting a commercial secret and transfer thereof into the category of publicly known information. After making a list of technologies and business information according to acceptable scheme, first of all, it is necessary to provide for provision of valuable information, leakage of which can cause damage exceeding cost of its defence.

Practice shows that this issue is better addressed collectively. To develop a list, committee of the most qualified and competent specialists of main divisions and representatives of security service are created by decree of enterprise's manager. One may not use classification of any information as a commercial secret, in order to evade taxes, conceal facts of damaging human health, as well as other illegal activities. Result of work of experts should be a list of information constituting enterprise's commercial secret. Quite naturally, that this list should be reviewed, modified and supplemented, when necessary. In the list, if possible, it is desirable to specify a time period for which some information is classified as a commercial secret. List is communicated to structural units and sub-

contractors in part concerning them, for guidance in work and according classification of works (it is advisable to apply classification of *commercial secret*), documents and products. Contractor and manager signing the document evaluate, during its preparation, information constituting a commercial secret contained in it.

6. Development of procedure for protection of commercial secrets

Organizational and legal protection of commercial secret is realized by establishing of regime of confidentiality in the enterprise. Confidential relationship is a fundamental category characterizing mechanism of protection of commercial secrets. Three forms of confidential relationship can be distinguished: (1) between employees and employer as a legal entity, arising from the moment of particular person's employment and continuing throughout the period of his work in the enterprise, (2) between a particular employee and other employees of the enterprise, created and developing both vertically and horizontally, and (3) between customer and contractor, created by work performance or service provision contract.

As noted above, right to establish regime of commercial secret has holder of a commercial secret. Confidant of a commercial secret must respect regime of a commercial secret established by its holder or establish regime of a commercial secret if it follows from obligations contained in agreement concluded with holder of a commercial secret. Access to commercial secret can be granted in accordance with manager's approved regulation on access system, where authorities of enterprise's officials for distribution and use of information are legally fixed. Enterprise's manager may allow use of any protected information by any employee of this enterprise or by a person, who has arrived at the site from another organization to deal with any issues, if no restrictions are set in respect of this information to acquaintance on part of production and commercial partners in joint production, etc.

In small enterprises with limited amount of classified works (documents and articles), manager has opportunity to personally distribute all classified information coming from outside and created inside the enterprise between employees regardless of their positions. In this case, so-called direct distribution of classified information is performed. However, direct distribution becomes impossible in the enterprise with large amount of classified works scattered among different structural units and divisions with employees of various job categories. In order to perform quality management functions, enterprise's manager may transfer a part of their rights to dispose of the motion of classified information to managers of lower levels. Manager usually reserves the right to dispose of the most valuable information constituting a commercial secret (confidential contracts with firms, reports of the results of work on promising products, etc.).

Effective work of permit system is only possible under certain rules: (1) permit system as mandatory rule includes a differentiated approach to permit for access taking into account importance of classified information in respect of which access issue is addressed, (2) documentation of issued permit to specific protected information. It means that manager, who gave permission to use, must fix it in writing in respective document or in accounting form of the enterprise. No verbal instructions and requests for access for someone else (except for the enterprise's manager) have legal force and are required for security service personnel. This requirement also applies to managers of all levels, working with classified information and carriers thereof, and (3) principle of control should be strictly observed by security services. This means that any permit to acquaintance with classified documents, information and objects must be security service manager. Permit must include: date of registration and issue, surnames, positions of persons, specific classification documents and products, to which they may be admitted.

Permit system must meet the following requirements: (1) apply to all types of classified documents and products available in the enterprise, regardless of their location and capacity, (2) determine order of access for all categories of employees who qualify to work with commercial secrets, as well as specialists, temporarily attending the enterprise and related to joint classified orders, (3) establish a simple and reliable procedure for issuing permits for access to protected documents and products, allowing to react immediately to changes in the area of information in the enterprise, (4) clearly distinguish rights of managers of different job levels in documentation of access for respective categories of contractors, (5) exclude possibility of uncontrolled and unauthorized issue of documents and products to anyone, and (6) not allow persons working with classified information and objects to make changes in account-

ing data, as well as substitute accounting documents.

Classification of *commercial secret* of certain documents usually contains phrase *commercial secret*, indicating attribution of information to commercial secret. The mentioned classification is marked on information carrier or accompanying document. In the upper right corner of the document is written *CS* (or completely – *Commercial secret*), *Confidential*. Such indication is classification of secrecy, but merely shows that ownership of this information is protected by law. On documents containing commercial secret and submitted to public authorities, other government agencies and local government authorities, classification *Commercial secret* must be marked on information carriers. Person establishing regime of commercial secret independently determines criteria for classifying newly obtained information as a commercial secret, validity of regime of commercial secret and set of measures to ensure regime of commercial secret regarding obtained information, including classification and declassification of commercial secrets, procedure of access to commercial secret, selection and use of means and methods of protection, storage and transmission of information constituting a commercial secret, except in cases provided for in the contract.

In developing permit system, special attention should be given to allocation of the most important information most valuable for the enterprise, which would allow providing strictly limited access to it. If there are joint works with other enterprises (organizations), foreign firms or individual representatives thereof, it is necessary to provide for a procedure for access of these categories to enterprise's commercial secret. Regulation of firm's permit system should indicate that transfer of classified documents and products from contractor to contractor is only possible within a structural unit and with permission of its manager. Transmission, return of such documents, products is made according to procedure established in the firm and only during normal business hours of this day. Regulation of firm's permit system must indicate that closed meetings on business issues are only conducted with permission of firm manager or their deputies. Special requirements may apply to meetings of academic council, meeting on reviewing results of research and financial and commercial activities, etc. It is recommended to document mandatory permit lists for such activities and only include those enterprise's employees, which are directly related to planned activities and have a duty to participate. As noted above, employees of other firms may only participate in closed meetings with personal permission of firm's management. Lists are usually prepared by the person responsible for organizing the meeting in contact with interested managers of structural units. List is the basis for organization of control over admission to this meeting. Prior to the meeting, security service officer warns those present that the disputed information is confidential and not for distribution outside the sphere of circulation established by the firm, and gives instructions for the conduct of business records.

Validity of regime of commercial secret is established within regime of a commercial secret and is determined by validity of conditions necessary and sufficient for recognition of certain information as a commercial secret. Necessary measure to ensure regime of a commercial secret is conclusion of properly executed confidentiality agreements or other supporting obligations not to disclose commercial secret of contracts by holder and confidant of a commercial secret. Confidant of a commercial secret, who obtained commercial secret by virtue of a civil contract and permitted its disclosure, must immediately notify holder of a commercial secret. If his actions do not contain a crime, confidant of a commercial secret is civilly liable in accordance with applicable law. A prerequisite for establishing regime of a commercial secret in conclusion and execution of a civil contract is conclusion of written confidentiality agreement by the parties along with contract or inclusion of respective conditions in labour contract. According to part 1 Sec. 83 of the Labour Law (hereinafter – LL), employee is obliged to keep secret information at his disposal constituting enterprise's confidential information.

Confidentiality agreements may be unilateral or mutual, i. e., binding by obligation to remain silent either for one party thereof, or for both the employee and employer. Unilateral confidentiality agreement is most often found in practice. Unilateral is usually confidentiality agreement concluded with an employee. Mutual confidentiality agreement is concluded usually in case where an employee, more often high-level manager or senior technical specialist, comes in a large company with a ready business plan or development, and company provides data on its marketing, financial and other possibilities. Any confidentiality agreement must, first of all, accurately and with the highest possible degree of detail and

specificity define its object and a complete list of the information, which parties will deem confidential.

It is necessary to keep in mind that not every information, although secret, on the basis of local regulations of this enterprise, may be recognized as such under confidentiality agreement concluded with specific employee. For example, if company employs developer, who created a new technology, similar to that already used in your plant, you can hardly extend his obligation of confidentiality to information on this development. The most important condition of any confidentiality agreement is its validity. The most urgent question is, whether confidentiality agreement is valid after termination of employment contract. Confidentiality agreements are used to prevent leakage of any confidential information, from production secrets to personal data. Its use is required by law in most developed countries, and claims related to it are accepted by the courts unconditionally.

A characteristic feature of confidential relationship is documentation thereof. This raises another problem – issue of assigning a document appropriate confidentiality classification and development of a system of regime measures providing for protection of confidential information. Analysis of available domestic and foreign publications allows a number of authors to recommend, in relation to business structures, a following approach. Define two classifications of marking information relating to a commercial secret: (1) *strictly confidential* – when loss (disclosure) of information creates preconditions for possible catastrophic consequences, most often bankruptcy, and (2) *confidential* – when loss (disclosure) of information causes economic or moral damage to the enterprise, but cannot lead to its death. However, it should be taken into account that use commercial secret non-disclosure agreements are not an independent measure of protection. By offering employees to sign such agreement, firm's management warns employee that a whole system of measures to protect information comes into play: legal, organizational, and technical. Agreement provides a legal basis to prevent potential wrongdoing. Principal also seems reflection of issues of compliance with commercial secret in the agreement concluded with firm's manager, when the latter is elected as provided for by law. By law, manager is granted exclusive rights to determine composition and content of information constituting a commercial secret, and procedure for protection thereof. However, he is imposed certain obligations for appropriate provision of preservation of commercial secret and responsibility for state of affairs in this area.

Therefore, agreement with enterprise's manager should reflect the following: (1) he should be obliged to strictly keep enterprise's commercial secret and not use it to engage in any activity at the expense of the company, (2) it should be emphasized that enterprise's manager is personally responsible for creating necessary conditions to provide for preservation of enterprise's commercial secret, and (3) as well as members of the personnel, enterprise's manager must be warned that his violation of requirements in part of organization and procedure of protection of commercial secret may result in termination of the contract, as well as criminal, administrative, civil liability in accordance with valid legislation. The presence of the mentioned documents gives opportunity to speak about the presence of legally enforceable procedure of protection of commercial information in the enterprise. This creates opportunity assume responsibilities for preservation of customer's commercial secret, relating it to classified information. Contracts with customer must clearly and unambiguously indicate information relating to protected information. Holder of commercial secret has the right to change or cancel regime of commercial secret, if it does not violate responsibilities assumed at conclusion of confidentiality agreement or other contract. In case of changing or cancelling regime of commercial secret, holder of a commercial secret must notify confidant of commercial secrets, which concluded corresponding agreement or contract, thereof in written. In case of liquidation of legal entity, holder of a commercial secret, liquidation commission (liquidator) makes a decision on possibility and procedure of further use and protection of information constituting a commercial secret of liquidated legal entity.

7. Ensuring compliance with the established procedure for protection of commercial secrets

Of course, issue of legal protection of commercial secret exists not only in Latvia, but also in other countries, such as the UK, Germany, USA, and France. It is worth noting that legislation in industrialized countries formulates concept of commercial secret fuller and wider. It mentions trade, commercial and official secret. For example, English law understands

information, disclosure of which could harm interests of the enterprise, as a commercial secret. Concept *interests of the enterprise* broader defines circle of responsibilities for violation of regime of commercial secret, since it does not bind value of enterprise's commercial information only to monetary equivalent.

If we compare Latvian legislation on protection of commercial secret with foreign legislation, a conclusion on feasibility of development and adoption of legislative act on commercial secrets in Latvia arises. It makes no sense to supplement existing laws, which, though containing reference of commercial secret, do not provide for complex regulation of all problems associated with it. Adoption of a separate law on commercial secret is also favoured by almost complete absence of jurisprudence on claims for indemnification of damages incurred in result of disclosure of confidential information.

Importance of information and awareness of individual enterprise on the market grows every month. If enterprise's secret, secret information, which gives it an advantage over competitors, will not be defined and restricted by law; *fair competition* will hardly exist in a complete form, since lawful acquisition of valuable information on the market is its main element. Questions related to protection of confidential information of commercial nature involve not only legal entities, but also individual specialists. Legislative protection of know-how is a necessary element of legal protection of their accumulated knowledge and experience, as well as intellectual property in general.

Among the ways of protection against disclosure of commercial secret, main place is occupied by sanctions applied to violators. Unlike other cases of infringement of rights of holder of a commercial secret (such as illegal receipt or use), where it is possible to prevent or terminate respective violations, in case of disclosure of valuable information, right holder usually is already put at already accomplished fact of disclosure and, in the best case, can only rely on material compensation of losses. Disclosure of commercial secret may be committed by employees of the holder of a commercial secret. This, of course, does not mean that every employee is a potential violator; however, literature indicates that disclosure of commercial secrets by employees is the most common case of violation of commercial secrets. According to Sec. 86 of LL, employee is liable for damages, which he caused to employer. In interpretation of Sec. 1770 of The Civil Law of the Republic of Latvia (hereinafter – CL), as losses are understood any damages subject to property assessment. Every loss except for occasional losses is refundable (Sec. 1775 of CL). Loss is a decrease in actual property of the victim. The law also mentions loss of anticipated profit (Sec. 1771 of CL). With regard to employee's civil liability, these legal subjects are regulated by Sec. 79, 80, 81, 83, 86, 87-89 of LL. Thus, according to LL, employee must submit to internal labour regulations, which, in essence, are an expression of employer's power. Unlike civil relations, participants in which are persons independent from each other, in employment relationship employees are in subordination to the employer. Clause 1 Sec. 83 of LL provide that employee must not disclose information constituting employer's commercial secret at his disposal. As previously mentioned, in order to make employee liable for disclosure of a commercial secret, necessary is a contract with such employee on non-disclosure of a commercial secret, which becomes known to employee in course of employment. In terms of improving legal regulation of preservation and protection of commercial secret, considerably interesting is legislative experience of Western industrialized countries. Thus, for example, in British commercial practice, contractual provision for safety of commercial secret is the main means of successful protection. British courts adhere to a literal interpretation of confidentiality clause and consider rights and obligations of parties in accordance with specific provisions of agreement (oral or written). Usually, broader interpretation of the contract is not permitted. However, this rule is supplemented with possibility of using implied terms, which are derived from conclusive action in accordance with concluded agreement. What is important in such a contract? First, determine what exactly constitutes a commercial secret. It is important to give a fairly clear definition without disclosing, at the same time, the secret itself. Usually such an agreement includes a list of information not subject to disclosure. Second, clear contractual establishment of obligations of a party, which is informed on or otherwise obtains commercial secret. In most general sense it is obligation to keep confidential information secret, as well as not to use commercial secret in unauthorized purposes. As important as a duty *not to disclose*, is a duty *not to use* legally obtained confidential information. It is clear that by using commercial secret for personal purposes, employee (partner or another person) still

harms interests of the holder of commercial secret, though actual disclosure does not take place. Therefore, it is very important that agreement determines, how commercial secret is permitted to use, and provides that any other use is prohibited or requires a special permission. Third, contract must establish period of validity of a duty to respect confidentiality of information, because, as a general rule, it is not limited to the period of validity of employment contract or other relationships. Very often, such agreements do not provide for any time limit, but simply contain phrase *...as long as the relevant information is a commercial secret*, i. e., still valuable, unavailable to a wide range of people, and protected. To clarify and not create grounds for possible future disputes, whether information is a commercial secret or not, you need to set a specific period of restriction, for example, 3, 5, or 10 years. Defining this term, try to imagine, how valuable confidential information will be after expiration of set time intervals.

One of the most complexes is an issue on amount of employee's liability for violation of confidentiality. Losses from disclosure of secret information can be calculated in considerable amounts. It is clear that no employee has enough money to compensate them to the employer. In this regard, it is clear how important is a careful selection of employees and establishment of reasonable restrictions for access to classified information within the enterprise. Since damage caused by disclosure of enterprise's commercial secret is very difficult to estimate in property, it must be acknowledged that recovery from guilty employee of indemnification for losses incurred in this regard, would hardly compensates leakage of confidential information about the enterprise to third parties.

Basis of civil liability of employee is mandatory existence of the following conditions: (1) direct (real) damage, (2) wrongfulness of behaviour of employee, who caused damages, (3) guilt of employee in causing damage, and (4) causal connection between employee's actions (inactivity) and damages. Unlike indemnification of damages in civil law, civil liability of employees according to norms of labour law has its own peculiarities. First, civil liability of employees occurs for causing damages to the enterprise. Based on the meaning of respective sections of LL, we can conclude that property in this case is understood in a narrow sense, namely *actual, really existing property*, that is, everything understood in civil law as a concept of *thing*. Second, employee is only civilly liable according to norms of labour law in case of existence of a direct actual damage. As direct actual damage is understood decrease in actual property of the enterprise as a result of loss, deterioration or decrease of its value, as well as need to bear costs of restoration, acquisition of property or other assets, or make unnecessary payments (Sec. 1770 of CL). Third, in assigning liability to worker, only direct actual damages are considered, loss of earnings is not included here (unless it is a malicious wrongdoing). Fourth, amount of liability is limited to the size of caused damage and, as a general rule, must not exceed 20-50% of employee's monthly wage, but in any case with preservation of minimum wage, in accordance with Sec. 594 of The Civil Procedure Law (hereinafter – CPL). Thus, holding employee to civil liability according to norms of labour law for disclosure of a commercial secret is only possible if (among other prerequisites of holding to civil liability, such as wrongfulness and guilt of employee) employee's actions caused real damage to property of enterprise, institution, organization. Furthermore, there must be a written agreement of parties (contract), governing list of enterprise's information of confidential nature and legal regime thereof. However, in most cases, disclosure of a commercial secret does not entail direct damages to real, actual property of the enterprise. For example, disclosure by employee of marketing research results constituting commercial secret of organization he works in, has no effect on the property of the organization, organization essentially only loses those opportunities it could use, taking into account de facto monopolistic possession of such information. In other words, we can talk about loss of profits, and it is not to be recovered from employee by virtue of direct guidance of clause 2 Sec. 86 of LL. In addition, due to the limited size of employee's civil liability for damages caused to employer's property (not more than one average monthly wage), interests of the holder of commercial secret in case of violation of a commercial secret by its employees, remain virtually unprotected.

Nevertheless, in some cases, interests of the holder of a commercial secret can still be protected. Here we talk about cases of full civil liability of employees. Employee is liable for all damages caused to employer, in accordance with clause 3 of Sec. 86 of LL, in cases of causing damages with malice or due to such his illegal, guilty actions, which are not related to performance of work provided for by employ-

ment contract. For collection of damages caused by fault of the employee, employer must obtain written consent of employee. If employee disputes basis or amount of claim for compensation of employer's damages, he may file respective claim in court within two years (Sec. 79 of LL). Taking into account that Sec. 200 of Latvian Criminal Law (hereinafter – CL) provides for criminal liability for illegal disclosure or use of information constituting a commercial secret, employee's full civil liability according to norms of labour law in this case seems to be quite real.

Under the current law, amount of liability of a person, who disclosed a commercial secret, practically is not defined. It is clear that damage caused to employer can be calculated differently. By and large, it would be enough to create a precedent. But there is still no such practice. Moreover, most specialists in corporate law had never faced similar cases. Large companies prefer to agree with employee independently, and usually dismiss him voluntarily. In case of recovery of damages through the court, competitors can get even more information on activities of affected merchants. And explaining why certain information is confidential is quite difficult for merchants. British procedural law, unlike Latvian, provides for the possibility of closed trials in case, where there is a threat of disclosure of commercial secret in course of proceedings. In addition, court decision may limit access to materials of the case. Very important is the requirement to plaintiff to provide the court with maximum clear information on what information he considers confidential. Plaintiff cannot be limited only with a general description, since content of the judgment must be precise restrictions and prohibitions addressed to defendant (Kiselev 1998). It should also be noted that in jurisprudence concerning protection of a commercial secret became widespread temporary (interim) remedies. Disclosure of a commercial secret may entail significant damage (and even termination of victim's commercial activities), and disclosure, of course, cannot be re-classified. In this regard, objective of many claims filed in British courts is to prevent misuse of confidential commercial information or disclosure thereof even before it would entail property damages. Court's task in this case is to establish a proper balance between rights and obligations of the parties, without making final decision substantively.

With regard to liability for damage not at the time of performance of employment duties, in this case there is uncertainty about the delimitation of moments, when employee was acting in the performance, and when – not in the performance of employment duties. Literature offers to consider disclosure of a commercial secret, committed not in the performance of employment duties, when violation is performed outside of working hours, i. e., labour regulations. Let us consider such problem as duty of preservation of commercial secret by employee after termination of employment contract between him and the holder of a secret. Employee may use information in form of issue, transfer, disclosure, etc., of a commercial secret of the former employer during employment with another employer or on own enterprise. LL provides for protection of a commercial secret also after termination of employment relationship (Sec. 84, 85 of LL). Agreement of employee with employer on limitation of competition after termination of employment contract is only permitted if such agreement meets the following criteria: (1) its purpose is protection of employer against such professional activity of employee, which can create competition in commercial activities of the employer, (2) period of limitation of competition is no more than two years from the date of termination of employment contract, and (3) employer undertakes to pay employee a monthly fee for compliance with condition of limitation of competition. Amount of such remuneration may reach very high values. This agreement must be concluded in writing, specifying type, amount, location, time of limitation of competition and amount of compensation paid to employee. After termination of employment contract, employee may not use commercial secrets of former employer (for example, list of very important customers). When defining scope of such limitations, court conditionally evaluates whether contested information can be considered part of professional experience and knowledge of employee with *medium level of integrity and ability*. It should be noted that British courts often deny employers in their demands, seeing attempt to limit competition in their respective claims.

The most important conditions of satisfying claims on protection of a commercial secret are the following circumstances established by the court: employee intentionally copied, memorized or moved documents; employee acted by deception or fraud; information is definitely owned by employer, and its use is beyond the scope of employee's professional expe-

rience; employee was specifically warned that information is classified and pledged to comply with this requirement; employee occupies managing position. Current LL gave opportunity to employer to actually prohibit dismissed employee to work in enterprises with identical activities or create such own firm operating in the same market sector, for two years. Prohibition of competition to some extent could be considered means of keeping people in the enterprise, if not statutory opportunity to challenge validity of this agreement, citing the fact that it is unjust restriction of further professional activities of employee (part 3 Sec. 84 of LL). Inclusion of restrictions in employment contract is only possible when they protect legitimate interests of employer and, in particular, their right to industrial and commercial secrets of the company, lists of customers. Protection of these interests in the contract must be reasonable and logical. Of course, in any case, employee, who was fired or resigned from the firm, may not use information he received while working, but he may continue performing the same kind of activities (Kuzmin 1993).

In the above case, reviewed before the Supreme Court, judge decided that, since technician did not use customer lists of the firm, where he worked before, and customer contacted him by ad, competition did not take place. The fact that the person, after quitting former place of work, continues working in the same area does not mean that he is competing with former employer. He has the right to work in the same industry, and any limitation thereof will be considered a limitation of constitutional rights. All of the above concerns very different spheres of activities – trade, intellectual labour, etc. Interesting also is the opposite example from the US practice. Three former employees of Novell created a new company developing cluster technology for a competitive Windows NT Server platform. Novell representatives were quick to apply to court, accusing the new company of stealing commercial secrets. Court imposed a temporary limitation on use of cluster technology of the latter. Police seized computers, floppy disks and other materials from founders of Wolf Mountain Group. According to the lawyer, all three deny their guilt, and their activities will not be affected by court prohibition to use Novell cluster technology. Contract prohibits disclosure of commercial secrets, – he said. – But it says nothing about prohibition of competition, which, in fact, is sought by Novell (Laura 1997).

In foreign practice, all these issues are dealt with in different ways. For example, in Estonia the law follows the principle that employer's prohibition on former employee's work in a competing enterprise after termination of employment relationship greatly limits its employee's freedom of choice in activities in their profession, and therefore it should be ensured that his economic situation is not worsened in result of application of prohibition. To do this, period of limitation of competition is limited – it may not exceed one year. In addition, employer must, within this period, pay monthly compensation, which may not be less than 60% of the average wage of the former employee. In Germany, in accordance with decision of the Federal Court on employment disputes, law enforcement practice recognizes employee's duty to preserve employer's commercial secret after completion of employment relationship. Prohibition to use information constituting enterprise's commercial secret, after termination of contractual relationship between employee and holder of the secret is only set when employee obtained mentioned information in bad faith. If respective knowledge is obtained in good faith, there is no such prohibition. In determining good faith or bad faith of obtaining information while working in enterprise, German jurisprudence comes from duty to consider all circumstances of particular case, including importance of employee's activities for the enterprise, his position, participation or non-participation in development of information constituting a commercial secret, compliance of his behaviour to *good manners* (*guten Sitten*), i. e., usual modus operandi for entrepreneurship (Kuzmin 1993).

In addition, German and US legislation includes mandatory provisions requiring employer to pay employee compensation or provide him with special advantages and benefits in case of conclusion of respective agreement. Thus, paragraph 74a of German Commercial Code establishes duty of the employer to appoint and pay employee a monthly cash payment in case of signing agreement on prohibition of subsequent competition, period of validity of such agreement, as a general rule, may not exceed 2 years. US legal doctrine includes principle, according to which employee, who signed respective agreement, must be provided with commensurate benefits and advantages, but provision thereof is usually based on the agreement between parties and is purely contractual in nature. According to the definition given above, another important feature of a commercial secret

in accordance with US legislation is the condition on its holder's need to take reasonable measures to ensure confidentiality of information. The law does not require absolute secrecy – amount of necessary measures is determined by specific circumstances and must comply with the principle of reasonableness.

In practice, *reasonable effort*s mean, for example, message to employees about the necessity to observe confidentiality, signing by employees of agreements on non-disclosure of commercial secrets, storage of classified documents *under lock and key*, etc. Usually, resigning employee notify organization about undertaken obligations on preservation of commercial secrets in writing. Manager of the organization of resigned employee may notify new employer on employee's awareness in the area of commercial secrets. By preventing possible violations by hired personnel, employer may offer employee to notify him about existence of commitments on non-disclosure of commercial secrets.

In French law, in case of a dispute concerning the disclosure of a commercial secret, jurisprudence establishes absolute priority of rights and interests of entrepreneur in relation to a former employee. Courts rely on the fact that after the termination of employment relationship, former employee is obliged to keep former employee's commercial secret, even if there is no corresponding legislative clarification on this issue.

In British practice, commercial secret is to be fully (but more rarely) protected after completion of employment on the basis of the former employee's work. Be that as it may, centuries-old legal doctrine *of restraint of trade* is based on assertion that, after termination of employment relationship, employee is not civilly liable to former employer. It seems that occurrence of such optional obligation as obligation to keep information after termination of the principal obligation not only undermines accessory nature of its origin, but also leads to unilateral restriction of rights and interests of subjects of civil relations and contradicts the main idea – provision of balance of their rights and legitimate interests.

It seems preferable not to establish a general proclamation norm prohibiting use of commercial information by former employee for two years, but provision to former participants of guarantees to settlement of civil obligation upon its completion. In this case, it would not only emphasize the main feature of the civil law – dispositive orientation, but also reflects the very idea of dispositive regulation – provision of balance of rights and interests of members of civil relationship. In this regard, Western legal practice uses agreements on non-disclosure by former employee of former employer's commercial secret. In accordance with the Italian Civil Code, employee must to observe the so-called *duty of loyalty*. The law prohibits exercise by employee of competitive activities, transfer or any use of information about the enterprise or manufacturing processes, if it might harm the enterprise. It should be noted that the law does not set expiry date of *duty of loyalty,* and prohibition to disclose former employer's commercial secret is established, regardless of how employee acquired respective knowledge. In Belgium and the Netherlands, any use by employee of information constituting former employer's commercial secret, regardless of method of obtaining, is prohibited.

We should note that the jurisprudence of many industrialized countries has many cases of denying companies in their claims against former employees, considering such as an attempt to limit individual's ability to obtain employment. For this reason, most courts insist that non-competition agreement had *reasonable* limits, both in time and geographical spread. For example, in the US agreements are recognized valid if: (1) they are suitable and necessary for protection of commercial information, (2) scope of activities covered by the agreement is clearly defined and is not too wide, (3) they are reasonable by period of validity (no more than 2-3 years), (4) they are reasonable by area of validity (within 1-2 states), and (5) they provide for commensurate remuneration/compensation to employee.

Conclusions

Summarizing the above, it should be noted that in order to ensure safety of a commercial secret, it is necessary to create such system of protection of information circulating in the enterprise that includes: (1) implementation of measures for development of a legal regime ensuring effective protection of a commercial secret in the enterprise, (2) acquisition of audio and video surveillance equipment, (3) hardware and software security solutions of corporate computer networks that will protect them from illegal actions by third parties, (4) ensuring continuous monitoring of compliance with confidentiality of

information in the enterprise; and (5) selection and training of personnel.

Most small and perhaps medium enterprises in Latvia today are not able to afford the entire complex of corporate security protective equipment due to high cost. And all it can be useless, given constant action of the human factor, which is the most vulnerable link in any system. Therefore, basic means and efforts at organization of and compliance with enterprise security should be aimed at personnel – from hiring to dismissal, including a two-year period of limitation of competition after termination of employment relationship. Security system can, more or less reliably, stand and reflect an attempt of intrusion from outside.

But if this invasion will be performed by enterprise's employee, in most cases system will fail and sensitive information will leak. Practice shows that the leading role in preventing these violations belongs to prevention thereof. Only when level of sense of justice of the majority of members of civil society (personnel of the enterprise), coupled with constant monitoring system is high enough, one can hope for positive results.

But we should not forget about other protection mechanisms available to the merchant: law enforcement norms of copyright and patent law, which are closely connected with problems of protection of enterprise's commercial secret, norms of competition law. For maximum effect, it is necessary to use the entire arsenal of legal means and methods.

References

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS agreement)//International protection of intellectual property. Compilation of international legislation acts. Conventions. Agreements. Contracts. 2006. Biznesa informācijas birojs, Riga.

Bellanger, L. 2002. *Negotiation.* 5th edition. Neva.

Bergmann, V; Dubovickaja E.A. 2005. *Trade regulation of Germany. Join stock company Law. Limited liability company Law. Production and economic cooperatives Law = Deutsches Handelsgesetzbugh, Aktiengesetz, GmbHGesetz, Genossenschaftsgesetz.* Wolters Kluwer, Moscow.

Dudzevičiūtė, G. 2012. Conceptual approaches towards sustainability, *Journal of Security and Sustainability Issues* 1(4): 261–272. DOI: http://dx.doi.org/10.9770/jssi.2012.1.4(3)

Giriūnas, L.; Mackevičius, J. 2014. Evaluation of frauds in public sector, *Entrepreneurship and Sustainability Issues* 1(3): DOI: http://dx.doi.org/10.9770/jesi.2013.1.3(3)

Grybaitė, V. 2011. Towards measurement of sustainable development: systems of indicators, *Journal of Security and Sustainability Issues* 1(1): 17–24. DOI: http://dx.doi.org/10.9770/jssi.2011.1.1(2)

Kiselev, I.J. 1998. Foreign labor right. Learning book for universities. NORMA-INFRA*M, Moscow.

Kudryavtsev, J.V. 1981. *Rules of rights as social information*. Legal literature, Moscow.

Kulagin, M. I. 1992. *Business and right: experience of west*. Delo, Moscow.

Kuzmin, A. E. 1993. Problems of accessibility of commercial secret, *Pravovedenie* 4: 20–28.

Lankauskienė, T.; Tvaronavičienė, M. 2012. Security and sustainable development approaches and dimensions inn the globalization context, *Journal of Security and Sustainability Issues* 1(4): 287–297. DOI: http://dx.doi.org/10.9770/jssi.2012.1.4(5)

Laura, D. 1997. *Computerworld*. Available on the Internet: <http://www.osp.admin.tomsk.ru>.

Malakhov, S.V. 2001. *Civil-right regulation of relationship in world wide web: Abstracts of doctoral dissertation.* Moscow.

Novickiy, I.B. 1996. *Roman right.* 2nd edition stereotypical. TEIS, Moscow.

Pokrovsky, I. A. 1998. *Basic problems of civil right.* Statut, Moscow.

Popondopulo, V.F. 2006. *Commercial (business right).* Jurist, Moscow.

Raicher, V. K. 1947. *Social-historical types of insurrance*. AN USSR, Moscow.

Sergejev, A. P. 2003. *Intellectual property rights in Russian Federation.* Learning book, 2nd edition. TK Velbi, Prospekt, Moscow.

Shamkhalov, F.I. 1993. *American management. Theory and practice*. Nauka, Moscow.

Shershenevich, G.F. 1994. *Learning book of trade right.* SPARK, Moscow.

Solovjev, E. 2002. *Commercial secret and its protection*. 2nd edition. Osj-89, Moscow.

Tedeyev, A.A. 2005. *Information right: Learning book.* Eksmo, Moscow.

Totyev, K.J. 2000. *Competition right (legal regulation of competition). Learning book.* RDL, Moscow.

Zemljanovs, V. 2005. *Commercial secret and safety of business*. Jumava, Riga.