TRADE SECRETS - SECURITY AND LEGAL ASPECT

Branko MARKOVIĆ
Aksiom Softver Development, 11000, Serbia
markovic_m_b@yahoo.com
Milica OSTOJIĆ
Lawyer, 11000, Serbia
milica.ostojic.adv@gmail.com
Dejan T. ILIĆ
Faculty of Strategic and Operational Management, 11000, Serbia
dejan.ilic@fpsp.edu.rs

Abstract
The struggle for the dominance of competition is increasingly being transferred from physical to virtual arena, and therefore the application of new technologies is becoming an increasingly important basis for faster development, but it is becoming increasingly important weapon in the struggle for the dominance of competition in the new (digital) economy. The aforementioned trends in the foreground are even more emphasized than they were in the past years, the need to improve the protection of intellectual property, and the enhancement of the protection of trade secrets from increasingly intense industrial espionage and increasingly frequent cyber attacksIt is this trend that has been mentioned and initiated to pay special attention to the analysis of the possibilities and potential possibilities for improvement of the security and legal system of protection of sent secrets as an integral part of the intellectual property.

Key words: *trade secret, intellectual capital, strategy, data protection system*

JEL Classification: O34; O31; O32; O17; L84.

I. INTRODUCTION

Trade secret is the most common form of intellectual property. Because of its nature, or minimum formal protection measures in terms of registration and protection from a state or international authority, this form of intellectual property is most exposed to cyber attacks and industrial spies (Pooley, 2013). Trade Secret (Trejd Secret) means information that is not publicly known and accessible to the public, which as a result has or may have economic value and which, according to its value, is subject to confidentiality or security protection measures. UPSTO (United States Patent and Trademark Office) defines confidential information as information that may contain a formula, pattern, compilation, program, device, method, technique, or process. In order for the information to become a trade secret, it must satisfy the requirement that it is useful for business and provides and creates opportunities to gain an economic advantage over competitors who are not familiar with it and are not using it (USPTO, 2017). The extent to which trade secrets are important for modern business is best illustrated by the fact that 75% of companies in the EU believe that trade secrets are crucial for their business (Oldeskop, 2016).

According to UPSTO, the minimum preconditions that some information must satisfy in order to be considered a trade secret:

- A trade secret is information that has value if it is not known to others;
- This information has value to those who can not get it in a legitimate and legitimate way;
- The information is subject to reasonable protection measures.

The most common reasons and motives why companies are increasingly opting to protect their intellectual property by using the mechanisms to protect trade secrets are (Davis, 2009):

- The loss of secrecy in trade secrets leads to: a reduction in profits; loss of comparative advantage and loss of advantages in knowledge and skills directly related to the core business,
- Patent Law protects the idea for 20 years, and the trade secret for as long as the one who owns it succeeds to preserve it as a secret,
- Trade secrets are not registered, so they are free of charge, but they must be arranged and covered by all internal company documents. The company must clearly define trade secrets with its internal documents. In the event that this is not done, the non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), has no legal force,

- Trade Secrets are used as a safeguard against all of the business key information to which Trade Mark, Patents, Copy Right or other well-known and recognized intellectual property protection mechanisms can not be applied,
- Patent rights can not relate to abstract ideas, so it is a question of how the idea for a new type of software or additional functionality could be patented at all - in such cases, the most common way to protect new business ideas is through a trade secret,
- Processes (natural, business, social) can not be patented. Algorithm, especially in terms of algorithmic trade, can not be patented,
- Mechanisms for protecting intellectual property through trade secrets are also applicable to presenting ideas to investors because they do not require the innovator to have high costs if he had tried to patent the idea. Under this type of trade secret application, NDA is applied as a form of protection - if you have a business idea that you want to make to potential investors, you must first protect it in such a way that it asks potential investors to sign the NDA in connection with the ideas outlined before presenting the idea. In this case, it is also important to know that the case-law has roughly shown that this kind of protection can not be applied infinitely long on the idea, and that it is limited to the same period of time for 1-2 years, that is, depending on the type of secret and much shorter.

II. TRADE SECRETS - ANALYSIS OF APPLICATION IN MODERN CONDITIONS

In modern economics you are increasingly faced with the question: For which organizations are the most appropriate measures for the protection of intellectual property are trade secrets? Trade secrets can be applied in virtually any form, and form of business, and are most often used as a measure of protection of intellectual property in the sphere of new technologies and business processes. A general overview of where and how different types of trade secrets can be applied can be seen from the table below.

Type	1950-2007	2008
Formula	4% (12)	9% (11)
Technical information and know-how	46% (126)	35% (42)
Software or other types of computer programs /algorithms	11% (29)	10% (12)
List of customers /users	32% (86)	31% (38)
Internal business information	31% (84)	35% (42)
External business information	2% (5)	1% (1)
Combined trade secrets	2% (5)	1% (1)
Negative trade secrets	1% (2)	0
Other	5% (14)	9% (11)
Table 1: types of trade secrets at the level of disputes conducted before the US courts for the period 1950-2008		
Source: Almeling D. S., Snyder D. W., Sapoznikow M., McCollum W. E., Weader J. (2010), A Statistical Analysis of Trade Secret Litigation in Federal Courts, Almeling Gonzaga Law Review, Vol. 45:2, 2010, pp. 304, on line: https://www.omm.com/files/upload/AlmelingGonzagaLawReviewArticle.pdf		

Also, from the documents published by NSF and NCSES, BRDIS can partially answer the question.

Number	Industry	Percentage of trade secrets in the total protection of intellectual property companies by sector
1	All industries	58,8
2	Production	62,1
3	Chemical production	69,7
4	Machine industry	53,0
5	Electronics and computers	70,6
6	Traffic - transportation and systems	47,8
7	Not a production company	54,3
8	ICT	63,6
9	Professional, scientific and technical services	49,9
Table 2: Trade Secrets in Total Protection of Intellectual Property		
Source: Barbe, A., Linton K. (2016), Trade Secrets: International Trade Policy and Empirical Research, Draft Version: August 5, 2016,		

Trade secrets are most often used in companies that belong to the group of innovators and those business systems that are market leaders in terms of innovation. The application of intellectual property protection through commercial secrets is particularly reflected in technology start up companies in the field of software and companies that conduct digital transformation of their business. A frequently applied business protection strategy in an industrial segment is to build a defensive wall. Building a defense around a certain technology is possible in the following way through the patentability of products and /or technology that we do not even plan to sell, which will ultimately limit or disable competition for a period of maximum 20 years. What is lacking in this patenting strategy is the fact that when you patent something if you do not manufacture or apply it, you are conditioned to continue to market patents through licensing at a reasonable price in order to be profitable. The said patent method of constructing the defensive technological wall has shown numerous deficiencies, so it is increasingly less applied. In modern business, the measures of protecting the technology of the corsage of trade secrets with the balanced publishing of the technically correct but not the complete information that keeps the competition in constant financial effort are used more in order to keep pace with the technological progress in the sphere in which the competitor does not try serious business. This strategy has proved to be very successful in the short term, especially in the digital sphere of business.

III. TRADE SECRETS - SECURITY AND LEGAL ASPECT

In the direction of closer determination of trade secrets and the possibilities of handling them in terms of protection and management of security incidents, it is necessary to properly define the security and legal framework for the handling and management of trade secrets as well as their protection. However, before further analysis of the mentioned topic, it is crucial at the outset to point out what can not be considered a trade secret. It is often the case that right here there is a problem in dealing with trade secrets because there is no awareness of confidentiality and the possible channels of leakage of secrets. It is necessary to clarify that under confidential information, information can not be regarded as accessible through the independent research of a company or an individual who processes the same domain from which the trade secret is. Under confidential information, information that is publicly available or can be accessed without breaking security measures can also not be considered. It should also be noted that there is no obligation to register trade secrets, and therefore there is no ban on their commercial use in cases where competing companies have legally and legitimately obtained information that someone considered the subject of trade secrets. The said legitimate ways of obtaining such information are: independent discovery or creation; the process of observing, disassembling or testing products and facilities that are accessible to the public; engaging specific professional staff or consultants in the field and applying "some other business practice" that is considered to be a fair commercial activity.

Regarding the security aspect of trade secrets, it is also necessary to remove a significant dilemma concerning the violation of business secrets through security penetration. Namely, it is wrong to observe any security breakthrough malicious and, therefore, easily proved in court. Not all security breaks are malicious and not all breakthroughs are easy to prove during the trial. Namely, it can not be considered a security breach or disclosure of confidential information by an act of disrupting a business in cases where information representing a commercial secret has become public due to respect for the freedom of expression or the obligation of public availability of information or justified action of whistleblower. Persons or firms that are familiar with confidential information can, or are required, disclose to the same legal authority according to the law procedure. In this case, depending on the NDA and the business policy and the relationship they care about, they are required to inform the other party about this in order for this to take appropriate steps. Also, the collection of information by competitors through reverse engineering is also permitted. Data leakage by reverse engineering in terms of market assessment, or state of competition, etc., is based on the exploitation of security vulnerabilities caused by, for example, regular numbers (Schrenk M., 2015). Namely, reverse engineering is allowed in business both for products and technologies as well as for applied business models. From the successive series or parts of the series, it is possible to reconstruct the size of the market, and the participation of a particular company in the market, its sales volume, prices, profit margin, and the business strategy, and all this is not only allowed but the usual practice that modern business requires.

However, despite numerous determinants that indicate what is and what is not a trade secret, and that not all security penetrations are malicious, numerous studies nevertheless point to an increasing number of industrial espionage cases and injuries and theft of trade secrets. The number of cases related to industrial espionage which are directly related to the violation of trade secrets in the period 2009-2013, increased by 60% and to continue to grow exponentially (Coleman R. C., 2014). Center for Responsible Enterprise and Trade (CREATe.org) suggested that the economic loss attributable to trade secret theft is between 1% to 3% of U.S. Gross Domestic Product (PwC & CREATe.org, 2014). That is precisely why the Federal Bureau of Investigation (FBI) has defined illegal trade in trade secrets as the second most important security threat. In terms of jeopardizing general security, the threat of trade secrets is the second security goal of security agencies, immediately after the

fight against terrorism. Also, in terms of engaging internal security forces in the United States, there is an internal threat number one (Rogers M., 2012).

How often in reality are the allegations of trafficking in trade secrets to be allegations that the allegations are easy to make, but it is difficult to prove them, and the evidence that some information that can be considered confidential or secretly used does not mean by automation and proof that a company or individual has obtained and exploited trade secrets inappropriately. In the sense of initiating charges based on violation and misuse of trade secrets by an employee or former employee, it is necessary for the organization that raises the lawsuit to provide a case before the initiation of the lawsuit in the manner in which its internal documents have defined what is the subject of a secret and that the employees meet the same document. This set of system documents must include the following: what is the trade secret for which the specified level of security is required (if there are more with different levels of risk and required security), as defined as a trade secret and which are unauthorized ways in which the defendant could come into possession of the same, and in the case of a lawsuit which is the specific way in which the defendant came into possession of the same and used it, and how he hurt the company. In order to ensure the passage in terms of preliminary case submission to national or international investigative and judicial authorities, and a consensual court judgment that would justly punish the perpetrator and compensate the victim of a security breach in connection with a trade secret, all traces and evidence must be placed in the appropriate context, respectively, causally consequently connected, both to each other and with the perpetrator, and presented all the measures that the business organization did in order to provide their business and trade secrets in a reasonable way.

Although not directly related to intellectual property protection measures, the best practices related to the application of the General Data Protection Regulation (GDPR) can be useful here, and represent an adequate methodology for preparing the necessary information for the judicial process. This methodology involves monitoring information of importance (what is transmitted to whom, when and why, and who is the source of information, and how information is stored) (Critical Action Ltd., 2017). Also, for each security incident, it is necessary to create a map of events and information flows, and to link the movement of information with external events (events in the market and work environment for which there is a reasonable suspicion that a security breach and the emergence of confidential information, ie abuse and trade in industrial and trade secrets). This methodology also implies the interpretation of all security breaches, which is significant from the standpoint of the preparation of the trial.

Although, due to the different nature of trade secrets in different industries, it is impossible to provide a unique algorithm for dealing with and proving the validity of its own allegations in court, what is possible from the previous case-law is to draw up a series of guidelines in which the legal strategy should move. The legal strategy should consider the above-mentioned topic for consideration in analyzing whether it is a defense or allegation that someone unauthorized breakthrough and abuse of trade secrets or whether he has trafficked unauthorized with them. The interpretation of the chain of events is as clear from the previous analysis as the central issue of the dispute. Without a clear narrative and linking facts with a time-flow, no abuse of trade secrets can be demonstrated. The fact that a person was familiar or has come into possession of some industrial secret does not in itself represent an act of abuse, especially since for most industrial secrets, as we have shown earlier, reverse engineering can come to almost all the information and information that companies consider confidential in his business.

Some legislation of certain countries clearly defines the time limits in which it is possible to ask the court to determine the facts and define the penalties for possible perpetrators. For example, in China, it is not possible to raise a claim for infringement of intellectual property in the sense of the disappearance and misuse of trade secrets beyond 2 years from the day the security breakdown and /or unauthorized trade is detected by specific trade secrets (Bai B., Healey P., 2014). In case this is a constant activity, we can seek protection of the right in court, but only for the last two years. In addition to the above, it is necessary to prove and make all the measures taken by the prosecutor in order to preserve his trade secrets, that is, measures taken to prevent a breakthrough in security, as well as the measures he has taken to prevent further leakage of information and address security vulnerabilities, all within the legal deadline.

Also, some legislation prescribes that in cases where the financial value of goods or money acquired through the misuse of trade secrets exceeds a certain amount, the case changes the character and becomes a criminal offense prosecuted ex officio, but in such cases it is usually necessary before transferring the burden of investigative actions, and proving, to state authorities, to build a clear case, which is basically the starting point of the state security body. It is necessary to prove the losses and clearly show that they result from the abuse of trade secrets, not the market situation or the bad internal business of the claimant. It is precisely in the above that lies the notion that is called the "counter-proof strategy". Namely, if the defense attorney succeeds in proving or at least sufficiently contradicting the allegations of the prosecutor regarding the losses caused by the misuse of trade secrets and bringing them into relation with real problems in the prosecutor's business, the likelihood is that the whole case will be dismissed as unfounded. Interpreting the chain of events and associating it with business

results is critical to the outcome of the case. The mere fact that someone has come into possession of an industrial or other business secret does not automatically mean guilt in connection with the abuse of the same.

The next problem in terms of proving a violation of business secrets is the fact that they do not approve all legislation a legal attack on the "third party". A legal attack on a third party implies the following situation: if the attack is carried out by professional hackers, even if you know who the customer is without specific evidence, it is not possible to sue it. However, some legislators like the Chinese provide the option that it is nevertheless possible to initiate a dispute in the mentioned situation. Another provocation problem relates to the use of forensic techniques and tools that most often vary from country to country. In the above sense, crucial importance is to ensure the integrity of digital evidence by monitoring and proving the equality of Hash Value parameters on the source and destination file, that is, the system (Ozkaya E., 2017), (Hash Value is a feature of an electronic document that determines whether it is identical or not with another document).

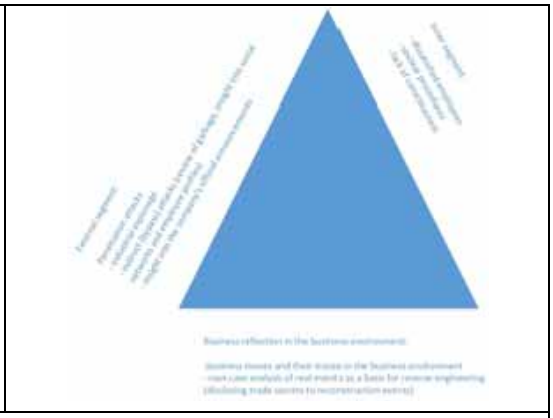

Figure 1: Vectors of a security attack that includes an attack on trade secrets;
Source left: Passmon, P. (2017). Trade Secret Protection: The Reasonable Steps Requirement,
The Center for Responsible Enterprise and Trade, Published on July 28, 2015, video, on line: https://www.youtube.com/watch?v=EY8eghzYKGg (04.09.2017).
Source right: Authors

IV. TRADE SECRETS - THE VECTOR OF ATTACKS

The reasons that lead to increased abuse of business secrets can generally be grouped and presented in the following way: accelerated development of the global market; fragmented value chains; digitization of information, accelerated labor mobility and more frequent work environment mobility (Yeh T.B., 2016,.) In addition to the mentioned factors that influence the frequency and intensity of the attacks, it is necessary to highlight and consider the issue of motivation. The issue of motivation is often skipped considering that the only valid motivation for discovering and downloading other trade secrets is the economic motive. Practice on the other hand points to the fact that in addition to economically represented and other motives for czber attacks such as: personal ego, ideology, detection of illegal activity - whistleblowers, moral disagreement and awareness of the protection of natural, historical and cultural values. All of these motives are not equally represented, and the proportion of ideological and moral motives grows, especially in the case of breakthroughs by third parties from other countries (usually Third World countries and China) which in a sense foster culture that everything is allowed in terms of strengthening the position of one's own countries and peoples.

As the most common vectors of attacks on trade secrets in the previous period (prior to the IT revolution) were the classic methods of industrial espionage and infiltration. Today, the most common methods used to create trade secrets are related to IT security techniques, especially digital penetration, and men in the midle attacks and attacks based on social engineering. Since all of these attack vectors are closely related to the operation of hacker groups in terms of preserving security, it is imperative that the company adhere to the best world practices in the field of IT security technology and to regularly conduct penetration testing and security audits.

In order to improve security, it is also necessary to use technical tools and security protection based on Active Directory, LDAP, Firewall, SIEM technologies, as well as all other legally prescribed measures and technical and organizational security measures.

V. TRADE SECRETS - EXISTING AND POTENTIAL MEASURES OF PROTECTION

Organizations in a modern environment should have clear and written measures for the protection of business and trade secrets that are both efficient and at the same time harmonized with the law. It is also necessary to prescribe clear procedures for dealing with other trade secrets as well as procedures for dealing with cases where their own trade secrets have been discovered and abused (UPSTO, 2017). The company's program of confidential information protection, in particular trade secrets, should contain the following protection measures (Dohmen L., Fortier L., 2017):

- Polices, procedures and records;
- CDA, NDA and other confidentiality agreements;
- Management system of security management and confidentiality of information;
- Risk management;
- Capabilities for building competencies and training in the field of security of confidential information;
- Audit: measurement and monitoring;
- A plan of corrective actions and improvements.

Depending on the level of organization and the field of business, the protection measures involve the following:

- Development and application of security measures for employees;
- Regular training of employees and decision makers;
- Procedures for termination of employment with staff members. Namely, when leaving the company, all employees leaving the company as well as former employees must recall the obligation to keep confidential information with the obligation to return all technical devices by abolishing and prohibiting all corporate profiles that had previously been used;
- Information is provided and shared only on the principle of minimum required set of information, and only to those who need to know them (these rules apply especially to buyers and suppliers);
- In order to ensure confidentiality with all customers and suppliers, there must be a contract regulating the obligation to store confidential information to which these partners come in their work;
- At the company level, the business system must create and maintain a campaign to raise awareness of the problem of trade secrets and other confidential information;
- At the level of the business system, the company must provide physical and electronic data access restriction, and technical audit and monitoring of employees' activities related to attempts to prohibit unauthorized access to protected data and information.

Another protection measure that is often applicable in the case of direct communication when communicating by any third party for information that is the subject of a trade secret, or could be related to it, is the application of pre-prepared phrases with which the employees are familiar with and which they are used in all cases when in communication with business partners (or in the public) a question arises in the area of trade secret (Salem S. 2012). It is important to note that, depending on the legislation, legislation is applied differently to the definition of "reasonable protection measures", and that the mentioned steps in the legislation of USA, GB, and the EU are only descriptive, while in the Russian legislation it is required that the company adheres to the "protection regime" in Japan, the legislator went a step further and demanded that companies that call for the protection of trade secrets should carry out within "reasonable security measures" and has a certificate that it has passed security testing in this area. In other legislation, these measures also include strict security of the facility, facilities, and evidence of the restriction of physical access to objects, or parts of an object or plant in which the trade secret is protected and defended.

AGREEMENT ON COMPETITION AS A MEASURE

The "Non-Competition Agreement" (CDA, NDA, NCA) is the most widely-used method of protecting trade secrets applied to employees in terms of maintaining business secrets and after termination of employment in a chaired company. The NDA is now a mandatory integral part of any top and middle management contract, but it is applied in practice to all employees who come into any contact with trade secrets. The aforementioned type of contract envisages the obligation of keeping the secret, but it is also used as a measure of protecting the business against unfair competition, as well as for preventing the employment of an employee in the competition in areas that could represent direct competition to the parent company. The NDA usually implies a measure of prohibition of work in the same industry for a certain period of time. The NDA has practically two possibilities

for activation: in the form of out-of-court settlement and judicial settlement. Today, this type of practice has become so common (due to the hyper competitiveness of the global market) that the same firms appear in both roles and prosecutors who persecute their former employees and companies that employ people in the NDA regime. Prior to initiating this type of dispute, it is necessary to assess how such a process is working on the total business, and towards which it is directed - as a warning measure for its own employees or as a measure of protection of key trade secrets. Also, it is important to note that in this kind of dispute, the company almost never performs its best witnesses because they are usually business partners (Fog S., 2012). Also, firms must be aware that judges favor the former employees, since the NDA basically violates the right of an employee to work. In the event that the company decides to go to court in an attempt to impose NDA, it is important that the construction of the case does not rest on the NDA itself, but in fact the company's business largely depends on specific classified information (trade secrets) that the employee had access to secrets and that his the new engagement is detrimental to the company's business (Gallagher J., 2014). Even if the company succeeds in imposing strict adherence to the NDA, it should be emphasized that judicial decisions are limited to a maximum of 1-2 years and are much shorter due to the development of technology at exponential speeds. This practically means that former employees will become your competition within a maximum of 2 years, so that the settlement strategy is probably more appropriate in most cases.

INTERNAL AUDIT AS MEASURES TO PROTECT TRADE SECRETS

One of the mandatory and easily applicable measures for the protection of trade secrets is the regular risk assessment with the audit. In the context of a security audit related to the safeguarding of this type of intellectual property, the auditors must ask the following key questions (Haris D., 2014):

- What information do you have in a company that your competition could use against you;
- How much of a breakthrough or swelling of this information will hurt (in a competitive and financial sense);
- To whom the above questions are asked (top management, middle management, employees working with confidential information);
- Whether employees are aware of the fact that the protection of trade secrets is the protection of their jobs;
- What policies and methods used to ensure and preserve trade secrets;
- How is a trade secret protected by applied policies;
- What are trade secrets about performances (business), which are of a temporary nature, and which are absolutely untouchable and never are disclosed to anyone;
- How to provide absolutely untouchable secrets (double key, individuals know only a part of the secret and can not complete without others, measures of physical and technical protection, ...);
- In terms of protection of intellectual property, it is prohibited from downloading, mobility, BYOD, so that it is secured from unauthorized access;
- Have educational measures been taken to educate employees regarding the confidentiality of confidential information;
- Is there a policy or SOP to manage and handle confidential information.

Outside of this formal audit, it is necessary in the context of an audit, but also for the needs of a possible litigation, to collect all information on how the company and at what price has provided its trade secrets, as well as the estimated values of the secret during the previous period. All these metrics are indispensable as a possible evidence applicable in a court that the company would prove that it had applied reasonable security measures for confidential information.

VI. OPEN IDEA

If one looks at the essence of trade secret as a mechanism for protecting the market advantage that is derived from an abstract idea or algorithm or another methodology that enables the creation and maintenance of a comparative advantage, it is very important to define and what is completely contrary to the idea of trade secret. In this sense, we can define the concept of open and publicly available ideas. It is also important to note that many publicly available ideas are used as Open Ideas, and are not as defined by those who have put that idea out. Although, for now, there is no clear legal regulation that would regulate this type of intellectual property in terms of preventing abuse, there are basic moral principles that define this area. Namely, in the world of shared knowledge and information, it is considered immoral any attempt to patent some idea above publicly available knowledge. For example, open source software tools offer the ability to see the source code, but not the ability to use it in commercial software tools without the special permissions of those who created and published the

specified code. Defining a given information or information as an open idea deletes any possibility to establish a certain level of secrecy subsequently or apply security protection mechanisms to the secrecy of trade secrets.

VII. CONCLUSION

From all of the foregoing it is clear that the protection of trade secrets is one of the key measures to achieve and preserve the competitiveness of modern business systemsDue to the nature of trade secrets and the nature of the way in which they are today, it is necessary to define and dismantle a range of activities and measures to define and protect trade secrets as such as the organization and its representatives would have prepared to protect them both within the company parameter and in the within the court process if it comes to it. These protection measures represent the basic working framework for the preparation of defense, that is, security operations to defend the most important trade secrets, and with them the benefits that the company realizes on the market. Due to the dynamic development of new attack vectors and the certainty that in the future companies will surely encounter both industrial espionage and secret sales, it is necessary to apply dynamic models of protection at depth that would imply all three types of protection - organizational, technical and legal, and constituted a single working framework for protection of the company's intellectual property.

VIII. REFERENCES

1. Pooley, J. (2013), Trade Secrets: the other IP right, Wipo Magazine, June 2013, dostupno na mreži: http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html (05.09.2017).
2. UPSTO, (2017), Trade Secret Policy, on line: https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy, (05.09.2017).
3. Oldekop, A. (2016) The newly adopted EU trade secrets directive, EU-Japan Technology Transfer Helpdesk, webinar 2016, part 3, video, online: https://www.youtube.com/watch?v=YA14C4XMTqs (04.09.2017).
4. Davis P.(2009), Intellectual Property: Patents, Trademarks, and Copyright, DardenMBA, Published on Jun 15, 2009, video, , on web: https://www.youtube.com/watch?v=qFRaamWjYGo, (01.12.2017)
5. Almeling D. S., Snyder D. W., Sapoznikow M., McCollum W. E., Weader J. (2010), A Statistical Analysis of Trade Secret Litigation in Federal Courts, Almeling Gonzaga Law Review, Vol. 45:2, 2010, pp. 304, on line: https://www.omm.com/files/upload/AlmelingGonzagaLawReviewArticle.pdf
6. Barbe, A., Linton K. (2016), Trade Secrets: International Trade Policy and Empirical Research, Draft Version: August 5, 2016,
7. Schrenk M. (2015), DEF CON 23 - Michael Schrenk - Applied Intelligence: Using Information Thats Not There, DEFCONConference, Published on Dec 11, 2015, video, On line: https://www.youtube.com/watch?v=UJeKNl461d8, (02.09.2017)
8. Coleman R. C., (2014), Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism Washington, D.C., May 13, 2014, Combating Economic Espionage and Trade Secret Theft, 04.09.2017, on line: https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft
9. PwC & CREATe.org, Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, at 3 (February 2014), available at http://www.pwc.com/en_US/us/forensic-services/publications/assets/economic-impact.pdf
10. Rogers M., (2012), CNBC - Cyber Espionage: The Chinese Threat, Rep Mike Rogers, Published on Jul 10, 2012, video, on line: https://www.youtube.com/watch?v=Js52FjOsgPA , (04.09.2017)
11. Critical Action Ltd., (2017) GDPR - ideas for analysing your data, CriticalActionLtd, Published on Apr 3, 2017, video, On line: https://www.youtube.com/watch?v=eJBXUajwK_U, 31.08.2017
12. Bai B., Healey P., 2014, How to Protect Your Trade Secrets while doing Business in China, Helpdesk TV, Published on Feb 6, 2014, video, on line: https://www.youtube.com/watch?v=e3hFyEON-Uo, (04.09.2017)
13. Ozkaya E., (2017), Windows Forensics, Microsoft Virtual Academy, on line: http://www.microsoftvirtualacademy.com, , (04.09.2017)
14. Yeh T.B., (2016), Protection od Trade Secrets: Overview of Current Law and Legislation, Congressional Reasrch Service 7-5700, R43714, April 12. 2016,
15. Passmon, P. (2017). Trade Secret Protection: The Reasonable Steps Requirement,
16. The Center for Responsible Enterprise and Trade, Published on July 28, 2015, video, on line: https://www.youtube.com/watch?v=EY8eghzYKGg (04.09.2017).
17. UPSTO, (2017), Trade Secrets, USPTO video, Published on Mar 1, 2017, video, on line: https://www.youtube.com/watch?v=1dXA5A4l0Rg, (30.08.2017)
18. Dohmen L., Fortier L., 2017, Why Trade Secret Protection is Powerful and How to Set up an Effective Program, Schwegman Lundberg & Woessner, P.A., Published on May 12, 2017, video, on line: https://www.youtube.com/watch?v=YN3fWx_Xeyo, (31.08.2017)
19. Salem S. (2012), Protecting trade secrets, Published on Jun 8, 2012, video, on line: https://www.youtube.com/watch?v=QodgIZ5thsg, (04.09.2017)
20. Fog S., (2012), STRATEGIC POINTERS FOR NON-COMPETE AND TRADE SECRET LITIGATION, Network Trial Law Firms, Published on Aug 30, 2012, video, 0n line: https://www.youtube.com/watch?v=Das96yzybck, (05.09.2017)
21. Gallagher J., (2014), Is My Non-Compete Agreement Enforceable? Non-Competition Contract Lawyer, John Gallagher, Published on Jun 24, 2014, video, on line: https://www.youtube.com/watch?v=rQWVKhtHC6I, (05.09.2017)
22. Haris D., (2014), Trade Secret Audits: Protecting and Valuing Your Company's Secret Know-How, Network Trial Law Firms, Published on Aug 14, 2014, video, on line: https://www.youtube.com/watch?v=UsnSo7TASdg, (04.09.2017)