Peculiarities of cyber security management in the process of internet voting implementation

Tadas Limba, Konstantin Agafonov, Linas Paukštė, Martynas Damkus, Tomas Plėta

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Publisher
http://jssidoi.org/esc/home

PECULIARITIES OF CYBER SECURITY MANAGEMENT IN THE PROCESS OF INTERNET VOTING IMPLEMENTATION

Tadas Limba[1], Konstantin Agafonov[2], Linas Paukštė[3], Martynas Damkus[4], Tomas Plėta[5]

[1,2,4] Mykolas Romeris University, Ateities g. 20, 08303 Vilnius, Lithuania
[3] Cognit consult JSC, Kareivių st. 6-509, 09117 Vilnius, Lithuania
[5] NATO Energy security center of excellence, Šilo g. 5a, 10322 Vilnius, Lithuania

E-mails: [1]tlimba@mruni.eu; [2]ka1979@gmail.com; [3]linas.paukste@gmail.com; [4]martynas.damkus@gmail.com; [5]tomas.pleta@enseccoe.org

Received 20 August 2017; accepted 14 November 2017; published 29 December 2017

Abstract. The modern world could not be imagined without the information and communications technology. Today's society, its life and social relations are deeply influenced by the virtual space, and that stands as a reason why the world's Information Technology specialists and representatives of various branches of science have been focusing on solving the problems in the sphere of cyber security. Software and technological solutions used in reorganization of the activity of private sector nowadays are widely used in the public sector as well. By using technologies, countries put their effort into involving their citizens into the process of governance and direct participation in various political processes inside the state itself, and one of the most widespread tools to motivate the citizen-to-state political participation and resident's direct interaction in political processes is internet voting. Authors of scientific literature investigate how cybersecurity management is being comprehended and analyzed in technological, legal, management, economical, human resource management and other aspects; how cyber security is analyzed in the context of services provided by institutions of public administration; which means of cyber security management are essential, in order to speed up the processes of establishing e-voting systems. In this article the authors investigate the theoretical aspects of cyber security management in internet voting, analyze the global experience in the sphere of cyber security management implementation with the help of already established e-voting systems, evaluate the properties of cyber security management in the process of implementation of internet voting in Lithuania, as well as present audience with an in-depth analysis of the opinion of the local population, cyber security and voting system specialists, concerning the matters and possibilities of establishing internet voting in Lithuania. The authors also propose a cyber security management model, which could be used in the process of implementation (both preparation and establishment) of the internet voting system in Lithuania.

Keywords: internet voting, e-voting, cyber security, cyber security management, cyber security model

Reference to this paper should be made as follows: Limba T.; Agafonov K.; Paukštė L.; Damkus M.; Plėta T., 2017. Peculiarities of cyber security management in the process of internet voting implementation, *Entrepreneurship and Sustainability Issues* 5(2): 368-402. http://doi.org/10.9770/jesi.2017.5.2(15)

JEL Classifications: D72, D80, H83

Additional disciplines: information and communication; informatics

1. Introduction

Approximately 50 countries (for example, Switzerland, the United States, Canada, Kazakhstan and others) in the world allow their citizens to vote via the internet, but undoubtedly Estonia is the country that could be named as

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

the leader in e-voting, being the first country to launch internet voting (Vegas, Barrat, 2017; Shahandasht, 2017). Most states allow the usage of e-voting systems only in local (municipalities) elections, meanwhile internet voting is available in all types of elections in Estonia since 2005. However, internet voting has not been critically acclaimed everywhere. The successfully functioning e-voting system of the Netherlands was banned in 2007 due to the vast amounts of cyber attacks. Germany and Norway have both shut down their e-voting systems, claiming the system failed to meet expectations and assure the privacy of the voting process, as well as meeting the appropriate security standards. The topic of internet voting in Lithuania has been very relevant in the past decade and is known for being the center of heated discussions before every upcoming election. There were five law bill packages concerning the possibilities of voting in elections and referendums that were debated in the committees of Parliament of the Republic of Lithuania. Today, when attacks targeting individuals and against corporations, banks or state sectors occur, precaution measures against these types of cyber attacks are becoming a strategic aim of numerous countries. Internet voting is a very specific and important expression of democracy, and it is crucial for this expression to be protected from both, inner and outer dangers. A successful cyber attack against a process as important to a country as elections, can not only be the reason for the election to be declared invalid, but can also discredit the country and destroy its citizens' trust in the state. This article will analyze the whole process of internet elections in the context of cyber security. The aim of this article is to investigate the properties of cyber security management, analyze the cyber security of certain e-voting systems and to present a model of cyber security management, which could be applied and used for internet voting.

2. Theoretical aspects of cyber security management in elections conducted via Internet

Issues with the definition of Cyber security in Lithuania. Modern life and organization management could not be imagined without information technology and internet access, and the influence of internet over everyday life and global economics has not ceased to grow (Limba, Plėta, Agafonov, Damkus, 2017; Štitilis, 2013). Today, our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. The phenomenal expansion of cyber space has brought the unprecedented development of economics and increasing number of new opportunities. However, that also conditioned the appearance of new risks (Erbschloe, 2017). The 2013 cyber security strategy of the European Union states, that 'Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace' and both scientists and experts of cyber security stated, that cyber security incidents can affect the supply of services, essential for the society (providing water, electricity, healthcare, mobile network etc.) and damage the critical infrastructure (Fuschi, Tvaronavičienė, 2013; Limba et al., 2017). Modern technologies and the global cyber space have created unprecedented conditions to commit crimes remotely on the separate parts the world, as long as they have the access to the internet; and both - private users and entire governments are exposed to risks in the cyberspace (Štitilis, 2013; Kohnke et al., 2016; Owen et al., 2017; Antonucci, 2017).

The definition of cyber security in Lithuania was often confused with the definitions of electronic data security, data security, safety of networks and information and security of data systems. Also, cyber security is defined differently in various laws and legal bills of the Republic of Lithuania: for example in the resolution of 'development of electronic data safety (cyber security) 2011-2019 programme' and 2012 Republic of Lithuania Minister's of Internal Affairs order on 'Affirmation of State's data resource concordance to electronic data safety (cyber security) requirement internal supervision', the definition of electronic data security and cyber security is though of as the same thing, while in the 2013 electronic data security requirement schedule, affirmed by the Government of the Republic of Lithuania, *electronic data security* is defined as assurance of confidentiality, integrity and accessibility of electronic data.

This problem was solved by the Cyber security law issued on 2014 December 11, which specifically defines the concept of cyber security as 'the whole of legal, data transmission, organizational and technical means, meant to avoid, discover, analyst and react to incidents, as to reconstruct the functioning of customary electronic

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

connection networks, data systems or industrial processes in case such incidents take place. It is worth noting, that scientists, when talking about the development of cyber security, mention not only the main groups of electronic data security (normative, administrative, procedural and programme-technical) (Kiškis, 2006) and dimensions of data security (strategical, human factor and technological) (Jastiuginas (2011), but also emphasize the essential integration of the governing aspect into the process of assurance of cyber security (Limba et al., 2017).

Cyber security management principles and e-voting. The Committee of Ministers of the Europe Council endorsed the Recommendation (2004) 11 of the Committee of Ministers of the Member States on the legal, operational and technical standards for e-voting at the 898th Ministerial Meeting on 30th of September, 2004. In regards to the relatively low turnout of voters in the Member States and noting that some Member States have already implemented or are planning to use electronic voting, the Committee encourages Member States to take into account the development of new information and communication technologies in their democratic practices. The recommendation emphasizes the need to maintain the principles of democratic elections and referendums when electronic voting systems are being implemented. Voters must be guaranteed universal suffrage, equal elections, free elections and secrecy of ballot (Recommendations Report to the Legislative Assembly of British Columbia, 2014; Goldsmith, 2017), and the electronic voting system must be designed to give the voters the possibility to vote with an *empty ballot* (Limba, Agafonov, 2012).

It should be noted that in order to organize electronic elections it is necessary to implement:

1. *Procedural e-voting security measures:* familiarize voters with electronic voting system and its operating principles; provide with the possibility to test and understand how to use e-voting system; provide initial, as well as periodic testing of the system; know the principles and function of the hardware and software used in the electronic voting system; develop the voting system in a way which allows the recalculation of the results of voting if it is necessary; ensure the security and reliability of the e-voting system and provide voters with alternative voting options;
2. *Organizational standards:* make adjustments to legislations in order to establish the legality of the use of electronic voting systems; create voter register and keep it up to date; provide mechanisms that allow voters to vote only once (only one vote must be recorded in the election results); ensure that information on electronical voting will be disseminated through various communication channels; present voting options for the voters following the principle of impartiality; strictly avoid affecting voters choice in electronic voting system; electronic voting bulletin must contain only information related to the voting; clarify that the vote casted through the Internet is calculated as an equivalent vote with the same value as the vote casted through ordinary ballot in the polling district; the electronic voting system should be configured in a way which does not provide the voter with the evidence of the choice in ballot; in case of violation of the integrity of the system, electronic voting results must be announces as ineligible;
3. *Technical measures:* ensure that e-voting software and services are public and easily accessible; include voters in the process of developing electronic voting systems, in particular into the testing of simplicity of the system; analyze the interoperability of the e-voting system with the technologies already used by the voters;
4. *Security procedures:* authenticity, availability and integrity of registers containing data of voters and candidates must be guaranteed; it is necessary to ensure that voters receive an authentic electronic ballot; sufficient measures should be employed to ensure that the e-voting system is protected from the effects that could change (influence) elections results; ensure that information on the voters decision is destroyed immediately after the voting has taken place and the results of the election are recognized as valid; restrict the voters from connecting to the e-voting system after the elections are over; ensure the integrity of the received data; perform the counting process and, if necessary, repeat it.

Cyber security issues related to Internet voting. Internet voting system is not only a technical but also a social entity that is created, supported and used by people and groups. These groups may make mistakes or try to abuse

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

the voting system for their own purposes. The ability to vote remotely provides with a possibility to attack the voting system from anywhere in the world using non-administrative, but information resources (Ramonaitė et al. 2008). Successful attacks against internet voting systems may lead to public mistrust in voting systems or influence the deployment and usage of these systems in the internet voting process. Therefore, it is extremely important to analyze all possible threats that could arise in regards to the internet voting system, identify potential parties and attack mechanisms (Limba, Agafonov, 2012).

Vulnerability of personal device. Personal computer, mobile phone or other device used by the voter is the least secure link in the chain of internet voting. Personal computers are most often poorly maintained and not protected from cyber threats. However, they will be used by voters to reach the internet voting system servers during the internet voting. Those devices cannot be controlled by the elections committee and election committee is unable to influence voters to draw attention to these issues (Elections BC, 2011; Wohlin C. et al., 2012).

Potential intruders are constantly scanning the Internet for vulnerable targets. Researchers have noticed that computers in internet cafes or public libraries are most insecure (Jefferson, 2004). They may contain spyware or vulnerable programs (Dykstra, 2017). Voters may encounter same risks at their workplace – operating systems and browsers may be vulnerable to malware that can be downloaded by voters or other users accessing the same devices (computers) due to negligence or lack of awareness. A malicious program, operating on the voters device, can change the choice of the voter during the internet voting period without the voters knowledge or consent. Voter needs to have the access to a trusted and secure device to participate in internet voting, as this is only option to reliably check what choice was made and received by internet voting system. However, this situation is problematic as it allows voters to have a solid proof of their choice and fuel corruption. If the malicious counterfeiting occurs before the ballot is sent (on users machine), representatives of the administration may not be able to distinguish between the incident and the users mistake (Elections BC, 2011).

Also, it is also possible that the voter may try to manipulate the use of the internet voting system: vote more than once and try to sell the proof of choice. Malicious behavior may also be anticipated – intentions to damage the voting system, influence or change the election result, create doubts and damage credibility of the election results.

To summarize, it can be stated that the security of voter's personal device is one of the biggest issues connected with the internet voting system. Personal computers are not well maintained and not protected against malware attacks and other vulnerabilities, while public resources like computers in the internet cafes or public libraries are even more insecure.

Analysis of the internal vulnerabilities of internet voting systems. Štitilis (2011) describes the internal threats to the system as *authorized users of the information system (or former ones) who unexpectedly caused damage to the organization*. Limba and Agafonov (2012) categorized internal users into three groups:

- *Users of internet voting systems* usually create minor problems; incidents are not complex often caused not by the technical violation of the system, but mostly through non-technical vulnerabilities (organizational policies, etc.). The main purpose of such criminals is usually financial gain, but not the damage to the organization (Štitilis, 2011). Internet voting systems sometimes could be at risk due to negligence or lack of competence by users;
- *Administrators* of the *internet voting systems* can be very dangerous for the system and cause the excessive damage due to the exclusive access rights. They can try to abuse the electronic voting system and civil servants to execute the attacks. Štitilis (2011) observes that the most common motive for these employees is the revenge, and less often – financial gain. In order to defend against the actions of unauthorized system administrators, there is a need for rules which limit the ability of system administrators to elevate their own privileges – this would require the approval of other administrators (Association for Computing Machinery, 2006);

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

- *Civil servants.* Some vulnerabilities of internet voting system relate to the civil servants who are not directly involved in internet voting system administration, but have access to a voting system (managers, project supervisors and etc.). These individuals can participate in or even manage the internal attacks on voting system. Most common motive for this group of people may be the financial gain (Limba, Agafonov, 2012).

In order to protect against internal users of the system, the system must ensure that no person, using their privileges or permissions, could undermine the secrecy of electronic votes. All votes (ballots) must be encrypted in a way, which ensures on a technical level that a single person is unable to decrypt them. The private key of the election committee, used to decrypt collected ballots, could be split into several parts and entrusted to different individuals or authorities (administrators, auditors, etc.). Only after putting together all parts of the key it would be possible to create the possibility to decode the ballots (Recommendations Report to the Legislative Assembly of British Columbia, 2014).

Analysis of the external vulnerabilities of internet voting systems. Voters can participate in the internet voting from anywhere in the world if they are able to use internet. This makes voting much more accessible and convenient for the voter. However, this also makes internet voting more vulnerable to threats of the global electronic environment which can emerge from anywhere in the world. Cybercriminals may disrupt or even takeover internet voting systems. Electronic crimes are committed by various parties: students, terrorists, members of criminal groups, etc. The goals of these groups may vary, but usually they attack systems for personal financial gain or political purposes (Štitilis, 2011):

- *Hackers.* This group is characterized by excellent knowledge of computer applications, networking processes and weaknesses of computers. Most often, hackers are computer fanatics who are looking for weaknesses in computer software or hardware, just from boredom or to demonstrate their abilities (Štitilis, 2011). Ramonaitė and others (2008) argue that internet voting systems can become a new entertainment or a good challenge for the hackers;
- *Typical criminals.* Criminal groups and individual criminals, in order to get financial profit are moving their *business* into the electronic space (Štitilis, 2011). Internet voting systems may be interesting for them because the private data stored inside the voting systems. Typical criminals could also include vote buyers, who are looking for ways to safely buy votes online;
- *Hacktivists* are members of groups which try to achieve their goals through the abuse of computers and computer networks. Their activities usually are protests or civil disobedience. To achieve these goals, hacktivists tend to target websites, steal and disclose confidential information, carry out DDoS attacks etc. (Hampson, 2012). Hacktivists may try to compromise internet voting systems, interfere with the work of the system or disclose confidential information stored in the voting system;
- *Foreign intelligence services* carry out their missions. In addition to gathering of information, foreign intelligence services are also seeking to influence the decisions of state institutions and influence the public opinion (Who, how and why are spying in Lithuania, 2014). Servers of internet voting systems can be attacked to show the influence of a particular country or to create public chaos. Depending on the goal, intruders may not try to conceal the unauthorized intrusion into the internet voting system. If the goal is to influence the outcome of the election, foreign intelligence could try to falsify the results of the internet voting during election in order to choose the most suitable political party or candidate. In this case, efforts would be kept secret (suspicion could be fueled only by an unusually high level of support for a certain political party or candidate). At last, foreign services could try to compromise the internet voting system in order to undermine the authority of the state itself and reduce the level of public trust (Ramonaitė, 2008; Limba, Agafonov, 2012).

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

It can be concluded that the biggest threat to internet voting system is the foreign intelligence services as they are well organized and have a high financial, technical and intellectual capabilities. There are also considerable risks from caused by hacktivists, who are moderately organized and the lack of financial resources is supported by a common goal. Typical criminals could try to abuse internet voting systems for financial gain, but it is likely that good protection may persuade them to not take risk. It is possible that unknown hackers could try to attack internet voting systems in order to show off their skills.

Possible attacks of internet voting system. There are numerous ways in which cyber attackers could try to break into the internet voting system (Halderman, 2017), disrupt its work, violate the integrity of votes or simply compromise internet voting. Limba and Agafonov (2012) stated that it's unlikely that individual user systems (PCs) will be an attractive target for cyber-attacks, but practice shows that this is one of the main targets for attack.

Internet-based attacks could be divided into three main groups:

1. *Attack against the environment of the voter* could be based on a low level of the security of personal equipment and social engineering. The most commonly used attack techniques are:
    - *Man in the middle* is a frequent attack in cyberspace, when the attacker interrupts communication between clients or client-server systems. Violation of the integrity of communication allows the attacker to control the flow of information. This attack may violate the voters' privacy and disclose the voting information. The attacker can also use this attack to deprive the voter of his right to vote by not allowing the vote to reach the internet voting system. In order to avoid this attack, it is necessary to ensure a secure connection throughout the entire internet voting process. Another way to deal with it is to check whether the voters vote has been counted. The fact of a large number of voters who connected to the voting server, but did not vote, would create suspicions of a man in the middle attack and could force the election to be recognized as invalid. The same attack could take place during the registration phase (Jefferson, 2004);
    - *Viruses.* Hackers could prevent internet voting by creating a virus that destroys the systems. An example of this could be the CIH (Chernobyl) virus, which was created to gently slip into the user's computer and remain dormant until a certain date. On a certain date it starts working and destroys the system. A similar virus could be created to work on the period of elections, damaging personal computers (Middleton, 2017) of voters and preventing them from voting. Of course, voters may try to find other computers, but this would complicate internet voting and create chaos;
    - *Spoofing attack* is a method of imitation of a legitimate message or resource which is being offered to a voter (through email or other means of communication). The voter may think that he is voting on the official website of the internet voting system. The fraudulent internet voting website may look and visually function as an official site, but does not connect to the system. During this attack, the attacker also receives voters identification data, which can later be used to connect to the real internet voting website. The attacker can use e-mail to send a web link to the voter and lure him to a malicious webpage or use this method to install the Trojan horse on the voters computer;
    - *Trojan Horse* is a destructive program that is often presents itself as a useful software, but secretly runs malicious functions which may violate the confidentiality and integrity of the data on the system of a user. This can result in user losing his login information, access to the system or imitated voting;
    - *Pharming attack* can redirect traffic from one website to another. This can be done by changing the settings of the voters computer or by exploiting domain name server (DNS). Attack on DNS may also be called DNS poisoning, when attacker falsifies DNS records and redirects voter to a specially prepared fake internet voting website. The voter, following the instructions on the website (which looks like an official one) casts a vote that is not being counted (and may also lose his credentials);
    - *Attack against the website.* A dangerous hybrid attack which could be accomplished by inserting a malicious code into a specially selected website. For example, an attacker who is an opponent of the other

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

candidate sets a trap on his website. This way, every visitor, who visits the website, loses the technical possibility to vote using the internet voting website. Such attack could take away several hundreds or even thousands of votes from the candidate and that might be enough to lose the elections (Jefferson, 2004).

2. *Attack during the ballot casting.* When the voter confirms the choice in a ballot, the ballot travels to the internet voting server. Data sent through open channels may be subject to change by third parties (integrity violation), stolen or disclosed (confidentiality violation). Therefore, it is necessary to ensure a secure connection between the voter and the internet voting system using secure protocols (e.g. TLS). The data, sent by the voter, should be encrypted with a secure encryption algorithm (Recommendations Report to the Legislative Assembly of British Columbia 2014).
3. *Attacks against the electronic voting system.* It may appear that only technical attacks against electronic voting systems are relevant, but the abuse of social engineering is also an issue that can cause problems for the system. The following list indicates the attacks which are most dangerous for the internet voting systems:
   - *Denial of Service (DoS) and Distributed Denial of Service (DdoS) attacks*. The purpose of these attacks is to create conditions that do not allow legitimate users (voters) to reach the resources of the internet voting system (attacks against availability of information). Exhausting resources on the internet voting server (ddos against physical infrastructure, software or communication protocols) may render the system unavailable thereby compromise the internet voting process. This type of attack may be accidentaly caused by legitimate system users if the system is technically weak and was not estimated to handle a high number of connections from users. Such accidental DDoS attack has happened in 2011 (Census of Inhabitants in Lithuania) when a large amount of users logged into the census system simultaneously;
   - *Zero-day attacks* are based on security vulnerabilities in applications or operating systems which are not known to the producer of the software. Traditional security measures like antivirus or firewall are unable to detect or prevent these types of attacks. Zero-day attack is classified as highly advanced and can be used as an entry point to the system;
   - *Social engineering attacks.* This type of attacks can not only trick voters into using fake websites, but also organize campaigns "against the internet voting" or scare people by suggesting that the internet voting is unsafe, which could lead to public losing trust in internet voting system (Limba, Agafonov, 2012). These ideas can be supported by other propaganda campaigns (publishing the fake internet voting results before the end of the elections or publically publish a fake list of voters). A similar situation occurred in Lithuania in 2015 when a fake list of conscripts was published earlier than the real one.

Cyber security management in Lithuania. According to Urmanavičiūtė physical, technical (logical) and administrative control measures are used in order to protect the information. Cyber security law (adopted in Lithuania in 2014) defines cyber security as a body of legal, information dissemination, organizational and technical measures which are intended to prevent, detect, analyze and respond to cyber incidents. The following are tools for managing cyber security in Lithuania:

- *Legal measures:* The main legal acts of the Republic of Lithuania that regulate the principles of cyber security assurance and management are the Cyber Security law (2014), Resolution of Government of the Republic of Lithuania On the Approval of the Program of Electronic Information Security (Cybersecurity) Development in 2011-2019 (2011), General Lithuanian Police Commissioner order On Approval of the Description of the Information Required for Cybercrime Investigations, Possessing, Police Instructions and Cybersecurity Investigation Procedures. According to the description of the general safety requirements for electronic information approved by the Government of the Republic of Lithuania, a description of the guidelines for the content of security documents and a description of the guidelines for the classification of state information systems, registers and other information systems and the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

determination of the importance of electronic information, each information system administrator must prepare and get approval from the Ministry of the Interior for these documents:

- Instructions for regulation of system security;
- Rules for safe electronic information management;
- Continuity plan for information system;
- User administration rules for information system.

- *Information dissemination measures:* One of the most important elements of the organization management is the ability to correctly communicate and to understand the value of the information received and its significance for the effectiveness of the organization's activities (Virbalienė, 2011).
  Legal documents do not establish a list to clearly determine if the information is a secret of the company or institution. Different subjects may consider very different information to be important. Therefore, organizations must have their own internal documents and lists of confidential data, also create rules and procedures for storage and administration of this data. According to the law on State and Service of Secrets of the Republic of Lithuania (1999), classified information is marked by the significance, potential damage that would be incurred by the state, its institutions or persons if this information should be lost or disclosed to persons without the right to know it. The law also sets out the principles that must be observed when working with classified information:
  - Information must be classified and declassified in accordance with the principles of legality, reasonableness and timeliness;
  - The classification of the information is established and the level of protection assigned to such information must be proportional to the importance of the classified information and the amount of damage that would occur from the unlawful disclosure or loss of such information;
  - Classified information must be trusted while strictly following the *need to know* principle. This principle says that classified information may only be entrusted with appropriate work permits or access to classified information held by persons who, in the course of their duties, are required to have access to classified information. A person may be entrusted only with classified information that is required for the performance of his duties.

- *Organizational measures:* Security measures may prove to be useless, unless all the employees of the organization contribute to the protection of the information. Personnel protection covers a wide range of organizational measures. Information security training increases the awareness of employees on what and why needs to be protected, what are the threats and vulnerabilities (Ministry of Internal Affairs of the Republic of Lithuania, 2005). The Center for Internet Security (2015) emphasizes that human factor has a significant impact on all system design, application, operation, usage and monitoring functions. The Association for Computing Machinery (2006) states that authorized users of the system need to know how to protect their passwords and to protect themselves against social engineering attacks. Therefore, it is very important to assess the specific skills and knowledge of a particular group and to develop a training plan that needs to be continuously updated to include the latest threats (Center for Internet Security 2015). The recommendations issued by the Ministry of the Interior on the protection of information (2005) refer to the determination of responsibilities and personnel protection measures. It also defines the internal organization rules and procedures that govern the organization's information security policies, procedures and instructions. The procedures define how to safely use the systems or behave in certain situations: creating and changing passwords, accessing the office outside of office hours etc. Resolution of the Government of the Republic of Lithuania (2013) focuses on the secure exchange, updating, introduction and destruction of electronic information; software and hardware replacement and upgrade; information system changes management.
  The Association for Computing Machinery (2006) states that it is necessary to ensure that the rights to administrate the system of internet voting system or its parts (servers) must be strictly controlled and granted only to those employees who are required to complete the specified tasks. Administrators should

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

not be able to elevate their privileges – this should require permission from another administrator. The rules may have an exception for an emergency, when the permission of is not required. Center for Internet Security (2015) notices that attackers may try to detect and exploit legal accounts (ex-employees, testers, attendees) that have not been deactivated and have retained their rights. Therefore, systemwide accounts must be monitored on a regular basis. It is important to ensure that all accounts have an expiration period, as well as the activation linked to the termination of the employment contract. Response to incidents and their management plans must be prepared in advance. After the incident occurs, it is too late to develop the necessary procedures, data collection, record keeping and other processes that could help coping with the situation during the incident. Chaotic response can help attackers capture more data and cause more damage, therefore it is essential to prepare incident response procedures. It is necessary to define phases of incident management, assign specialists who will make take the decisions and take the responsibility for them.

- *Technical measures:* Technical measures are divided into hardware (access control systems, firewalls, video cameras), software (protects computer systems against malicious programs and viruses, provides access to important data only to authorized system users and eliminates software vulnerabilities) and mechanical (locks, doors, groves, etc.) (Ministry of Internal Affairs of the Republic of Lithuania, 2005). Different solutions are developed to protect network resources from external factors and to ensure the control of user access to the system resources. Most popular of them are:
    - *802.1x standart.* Network access is controlled by verifying user identities in accordance with the 802.1x standard, which provides access control and the ability to check user profiles on the RADIUS server and grant them access rights from different places on the network (Urbanavičiūtė, 2010);
    - *DMZ.* Demilitarized zone is an access control tool that ensures the security of public servers. Public service or proxy servers (that act as an intermediary and establish two-step connections between remote users and enterprise servers to which the external users are connecting also help protect against attacks from outside) may be located in DMZ. Center for Internet Security (2015) emphasizes that, in order to increase security, DMZ systems should be allowed to communicate with the intranet only through applications on proxy servers or firewall applications;
    - *PKI*. Public Key Infrastructure is a set of hardware, software, specialists and procedures used to store, create, manage, provide, update, delete certificates using public key cryptography. Public Key Infrastructure can facilitate and speed up the exchange of information by changing paper based methods (Repečka, 2007);
    - *IDS*. Intrusion Detection System is a device that monitors traffic on the network and detects an attack-like traffic. They can act on the basis of signatures, behavioral analysis and other mechanisms. IDS controls and analyzes user and system performance, checks system configuration and vulnerabilities, evaluates system and data integrity (SANS Institute InfoSec Reading Room, 2001);
    - *WAF*. Web Application Firewall - software that checks the flow of data for a web-based application. WAF's solution helps with blocking attacks against Web server vulnerabilities, protects sensitive information from unauthorized disclosure and control access to it (Center for Internet Security 2015);
    - *SSL and TLS protocols* are commonly used to ensure secure communication (Repečka, 2007): • *SSL protocol* uses symmetric and asymmetric encryption methods. During the communication session between the client and the server symmetric session key is set at the beginning of the session, which is created by the client browser and encrypted with the public key of the server. Since asymmetric encryption has been implemented in this step, only the server can decrypt the session key with its own private key. Both the client and the server station already have an identical symmetric session key and can begin to securely interchange data. However, the usage

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

of SSL protocol is prohibited due to the vulnerabilities found back in 2014 (SSL 3.0 is vulnerable to POODLE attacks). The new version of the secure protocol (TLS 1.2) is currently recommended;

• *TLS* only performs the identification of the server and the client remains unidentified, but in case of internet voting, it is important to voter to identify with whom he is communicating. There is also a higher-level scheme called mutual authentication, but it requires a well developed PKI. The operation of the TLS is based on three steps:

- direct connection based on algorithm;
- transfer of public key and validation of the certificate;
- encryption using the symmetric key.

In conclusion, it can be said that in order to prevent, detect, analyze and respond to cyber incidents, a comprehensive set of legal, information dissemination, organizational and technical measures is needed. According to the legislation of the Republic of Lithuania, it is necessary to ensure secure communication and dissemination of information and to adopt the documents regulating the organization's information security policy, procedures and instructions. Technical security measures should be adopted in order to protect network resources from external factors and ensure the control of users' access to resources and secure communications.

3. Analysis of global experience of implementing cybersecurity management in internet voting systems

***Scytl* internet voting model.** *Scytl* is one of the largest organizations in the world offering various voting systems (traditional voting, phone voting, electronic voting machines and internet voting). The organization claims that its products cover over 87% of the voting systems used in the world and that the online voting system proposed by it is extremely reliable. *Scytl* is constantly looking for new technologies and techniques to ensure even greater security of electronic ballots. Technologies such as public key infrastructure, cryptography, have been approved by twelve countries and have been successfully used. Scytl's internet voting system was studied by independent experts who found that the technology used in system is accurate and reliable (Shah, 2013).

According to the *Scytl* voting model (see Figure 1), the encrypted votes are signed with the voter's electronic certificate and sent to the internet voting storage server. After the verification of the voters eligibility, voting server stores the ballot. At the end of the voting period all encrypted ballots are transferred to the ballots mixing server. Ballots are mixed and decoded and the results of the voting are counted.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

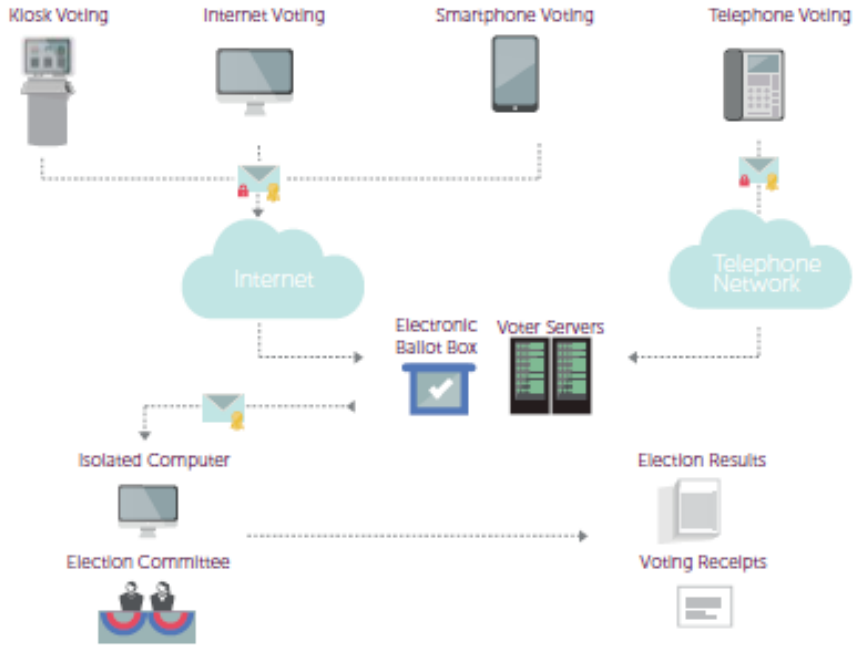

Fig. 1. *Scytl* principle internet voting scheme
Source: Scytl.com, 2017

In the *Scytl* model, voting system is provided is with personal and confidential voters data during the voter registration process. For the security reasons, this information is distributed to different internet voting system servers. The internet voting system requires authentication each time from anyone who attempts to obtain this data. These procedures ensure that personal data is provided only to an authorized user. *Scytl* company uses different voter identification techniques that can differ according to requirements of the different countries of the world. *Scytl's* cryptographic technologies and algorithms are easily compatible with Google, Android, Blackberry and Apple IOS operating systems and provide the same level of security as a cryptographic techniques used in standard personal computers. The *Scytl* voting system securely encrypts voting ballot on user's voting device before ballot is signed and only then sends it to the servers of electronic voting system.

Voters who voted on the Internet voting system get a confirmation voucher with a unique number that enables the voter to check whether his or her voice has successfully traveled to an electronic voting system and has been counted. With this unique code it is impossible to restore voice content and this measure could prevent the sale of voice during the elections. Additional measures that could prevent voice selling is an ability of voter to vote through internet voting system as many times as he wants – only the last vote will be counted. Voters also have the opportunity to vote with empty ballot and put his choice on internet voting system.

The encryption technology used in *Scytl* voting system provides the confidentiality and integrity of the voters' ballot. Ballots are encrypted before they are sent to electronic ballot boxes and only the election board can decrypt them. At the end of the election, ballots are transferred to a safe environment, mixed and decoded before counting procedure begins, thereby guaranteeing anonymity of voters (Puiggali, 2014).

The *Scytl* internet voting system has an ability to check ballots before, during and after the election. Election audit teams have the opportunity to check whether the electronic ballot server contains only the eligible voters' ballots (Puiggali, 2014).

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Audit system in *Scytl* internet voting system is integrated with the security information and notification of violations management system. This solution ensures that all data in system is properly processed and that security of this data is analyzed. Continuous scan of vulnerabilities ensures that system has a real-time opportunity to block security breaches even before they cause damage to the voting system (Scytl, 2015). *Scytl* has patented the technology of *static record* that protects system records from unauthorized change, also the encryption of those records ensures system integrity.

Cybernetica internet voting model. The *Cybernetica* organization develops various software, conducts researches and implements theoretical and practical security solutions. The company is ISO 9001: 2008 and ISO 14001: 2004 certified. *Cybernetica* has participated in several projects developed by the Estonian Government such as the Estonian National Identity Card (ID) and the creation of an internet voting system (cyber.ee). The *Cybernetica* internet voting system is used only by Estonia.

Before the beginning of each election in Estonia the election committee publishes sets of internet voting system applications (applications for Windows, Linux, Mac OS) that can be downloaded from the https://valimised.ee web page. Voter downloads the voting application and enters the identification key which is used to verify his identity. A secure connection (TSL) used for data transfer confirms the identity of the server using an encryption certificate. The server confirms the voter's eligibility (using voter's public key) and returns voter to the list of candidates. The voter can mark his choice and enter the signature key. For the voter registration the ballot forwarding server is used. It is a publicly accessible server that accepts an HTTPS connection from a voter's software and verifies the voter's eligibility. Ballot forwarding server acts as a subsystem for mediation with a ballot storage server that could not be reached from internet (Springall et al., 2014).

In *Cybernetica* internet voting model the identity of the voter is determined using a personal identity card with an integrated electronic signature. Each card has two keys: a user identification key and a signature key each of them has separate PIN code.

Another possibility for a voter to confirm his or her identity is to use the mobile signature (Mobile ID). The voter accesses internet voting web page www.valimised.ee using his computer, downloads and installs special internet voting application. When Mobile Signature Authentication Code (PIN1) is entered an SMS message with a control code is sent to the voter. After the identification voter can reach the list of candidates according to the voter's place of residence (list is displayed on the voter's device). The voter makes a choice and after entering the private key (PIN2) receives a control code via SMS message, which, after entering, signs the ballot. After that voter gets the popup message which indicates that the voter's ballot has been counted (Springall et al., 2014). The mobile signature allows the voter only to identify himself, but there is currently no possibility to use a mobile phone as a voting device. The computer with internet connection is required to participate in internet voting process in Estonia. For these reasons this method is not so popular in Estonia although the state encourages its use (Estonia.eu, 2015; Clarke, 2017).

Cybernetica internet voting system used in Estonia uses public key infrastructure to create a *double envelope* analogue that is used for postal voting (see Fig. 2.). The voter's vote is encrypted before being sent to the electronic ballot box using election committee's public key. An encrypted vote could be considered as an internal anonymous envelope as it is in the case of mail voting. The voter, who signs encrypted vote with electronic signature, adds his identification data to the outer envelope (Ramonaitė et al., 2008; University of Tartu, 2015). The outer envelope (digital signature) identifies the identity of the voter and the secret "voice" is stored in the inner envelope (public key encryption). When the voter's eligibility is confirmed, the signature is removed leaving only an anonymous encrypted vote that is transferred to separate ballot storage server (Springall et al., 2014).

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

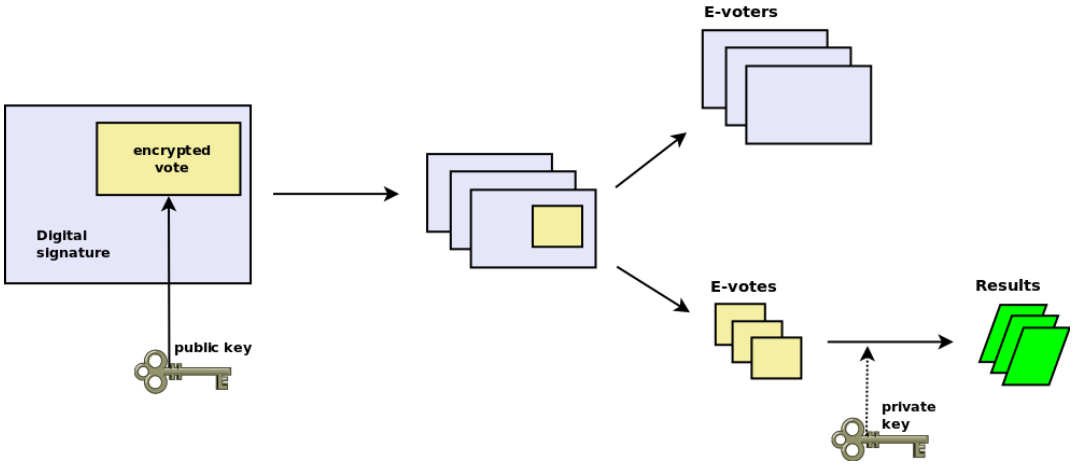

Fig. 2. Technical solution for internet voting in Estonia
Source: University of Tartu, 2015.

In order to avoid the possibility of selling votes, internet voting system allows voter to vote as many times as he wants, but only the last vote is counted. Internet voting system informs user that he has already voted, but it does not display how many times. If the voter is voting on the election day using the traditional voting method, the internet voting ballot is canceled (Springall et al., 2014).

Encrypted and signed ballot is sent to the server and linked to an unpredictable unique tag, and returned to the voter in the form of the QR code. The user can verify that his voice has been correctly recorded using the smartphone's application. The gadget scans the voter's QR code and contacts the voting system server, which returns the encrypted voice (but not the signature) and a list of potential candidates. The gadget, using a unique tag, encrypts the simulated vote for each potential candidate and compares the result with the encrypted voice sent from the internet voting server. If there is a match, the application displays the appropriate candidate.

Opponents of Estonian Internet voting say that this voice check method gives voters the opportunity to sell their voice because proof of voting content is proven. However, the election organizers reject thecomplains as, in their opinion, buyers can learn the content anyway (without voting control), as voting takes place in an uncontrolled environment. This mechanism simply gives the voter more clarity, and, moreover, vote can be verified only for a very limited time (University of Tartu, 2015).

Internet voting system server stores signed and encrypted ballots during the online voting period. Internet voting ballot storage server, after receiving a ballot from the ballot forwarding server uses certified external protocol to verify the voter's digital signature and confirms that the ballot is formed correctly. After the depersonalization of the votes, the election committee officials record all valid encrypted voices on the DVD and transfer them to the vote counting server. Vote counting server processes encrypted votes and re-checks signatures, afterwards, removes any canceled or invalid voices. The counting server is connected to a device that has the private key of the election committee for voice decryption. Election committee officials exports decrypted votes and record them on a DVD. The results are compared with the number of votes cast during the internet voting period and published. The counting server is not connected to the network, it is used only at the final stage of the election. Officials use the DVD to copy encrypted voices (with their digital signatures removed) (Springall et al., 2014).

During the internet voting *Cybernetica* voting system use authentication server to monitor system processes. This server is an internal authentication and monitoring platform that track events and collects statistics from the ballot

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

forwarding server and voice counting server. The server applications and technical design aren't described publically. Employees can connect to this server using remote connection.

After the internet voting is finished (4 days before the elections in the traditional voting poles), the list of internet voters is sent to the elections committee, which marks persons who has already voted in the voter lists. Traditional voting in the constituency is still a priority. A voter who has already voted on the internet may come to vote on the day of elections in voting pole. In this case the internet voting ballot will be erased (Estonia.eu, 2015).

According to the findings of the independent security expert teams from the United States (2014), United Kingdom and Finland have studied the security of the internet voting system in Estonia and publically announced the results of the researches, which have been a source of great clout. These results state that *it is possible to counterfeit the voting results on the election committee servers, by breaking into the computers used to prepare the system code, before installing it into vote counting servers.* Scientists have demonstrated exploitation of systems vulnerabilities in their lab. Experts from the Estonian National Election Committee replied that the researchers did not find any new attack vectors that has not be foreseen in the internet voting system design, and that expert-submitted attack techniques can not be effectively managed to change the results of the elections. It was also noted that the election committee has strong protection and automatic mechanisms that are able to detect attacks against the internet voting systems or attempts to falsify election results, while the errors in the online web site estoniaevoting.org do not reveal any technical details about the alleged vulnerabilities of the internet voting system (University of Tartu 2015).

Geneva solution internet voting model. The Swiss government launched internet voting project in 2000. There was a very high number of referendums in the country, so the Internet voting had to increase voter turnout and possibility to participate in the elections. The implementation of the system was also encouraged by the high level of internet penetration. Present, Swiss citizens are allowed to vote using internet voting system only in the European Union and in the Wassenaar countries.

In order to be included as a voter living abroad, it is necessary for the citizen to register their place of residence in the Swiss consular offices and renew the registration every four years (Barrat, Gildsmith, Turner, 2012).

Before every election, the Geneva canton residents receive a letter with a one-time voter card containing a voter identification number valid for a certain period of time. This card stores the citizen's (voters) number and PIN code (Geneva State Chancellery, 2010). The voters in the internet voting system confirm their identity by using this card and entering their birth date and place of birth (Parliamentary Research Department of the Parliament of the Republic of Lithuania, 2015). To secure voters connection (access) to the internet voting server an HTTPS communication session using SSL connection is created.

The internet voting website becomes publicly accessible after the electronic ballot box stamping-up procedure. To vote online, the voter connects to the https://www.evote-ch.ch/ge website and enters the voter card number received by mail. By pressing *acquaint* button, the voter confirms that he has acquainted with the actual legal information appearing on the screen (causing liability for election law violations) (Barrat, Gildsmith, Turner, 2012). Vote recording begins on the voter's computer after the voter marks his decision. Later, a secure communication channel is used to send the ballot to the electronic ballot box, decode the ballot and verify the voter's eligibility and the integrity of data of the voting ballot. The system sends a confirmation to the voter with a unique code known only to the internet voting system and the voter himself. Then the voter must confirm identity by entering birth date, password from the voter card and the place of birth. This data is not available in publicly accessible registers. The place of birth is also indicated on the Swiss citizen's identity cards and citizens passports. The voting server verifies the voter's data, whether the voter has not yet voted and after that record the voice. Finally, the internet voting server sends a confirmation to the voter that his voice has been counted.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Geneva solution internet voting model use asymmetric encryption method to encrypt votes. Public and private election committee keys used for this encryption are generated before the election. Before sending a ballot to the voting server it is additionally encrypted with a symmetric key (the secret code which is taken from the voter's card). This dual ballot encryption increases the security of the ballot. In addition, the internet voting system server uses the hash function to check whether the ballot has not been changed during transition or after it was received.

The *Geneva solution* internet voting system has one voter list for all three voting methods: voting via the Internet, postal voting and traditional voting polls voting. This option prevents the possibility to participate in elections more than once. The internet voting allows to vote only one time, without the ability to change your ballot later. The citizens who voted on the internet could not to vote in other ways (by post or in traditional voting polls (Parliamentary Research Department of the Parliament of the Republic of Lithuania, 2015). This solution creates situation in which it is difficult to ensure that citizen voted on a voluntary basis, also the possibility that one family member can vote for others exists. According to the election committee during the internet voting process this problem is solved by asking a private question that only the voter can answer. Election committee also calls 2% of internet voters to make sure they voted for themselves without any pressure from anyone (Geneva State Chancellery, 2010).

Internet voting ballots are counted during a formal meeting of the competent authority, it contains representatives of different political parties. Election committee's computer with special application is used to collect all election committee employees' passwords which are needed to generate private election key that will be used to decrypt and count voting ballots. (Geneva State Chancellery, 2010).

The *Geneva solution* internet voting model process is shown in Figure 3. The voter connects to the online voting system by downloading and installing voting application on his device. This application automatically adds a Java script to the web browser that ensures secure communication between the voter and the internet voting system. This creates a controlled environment. A connection to an internet voting system using the SSL protocol is initiated. Data flow is checked by the firewall. The internet voting system has a web server that manages queries in voter database, which is monitored by the elections committee. There is also a unique code generator that generates voter ID numbers and a cryptographic generator that generates cryptographic keys. The *Geneva solution* voting model does not cover the whole voting process - only the first part: voter registration, identification and formation of a voter's ballot.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

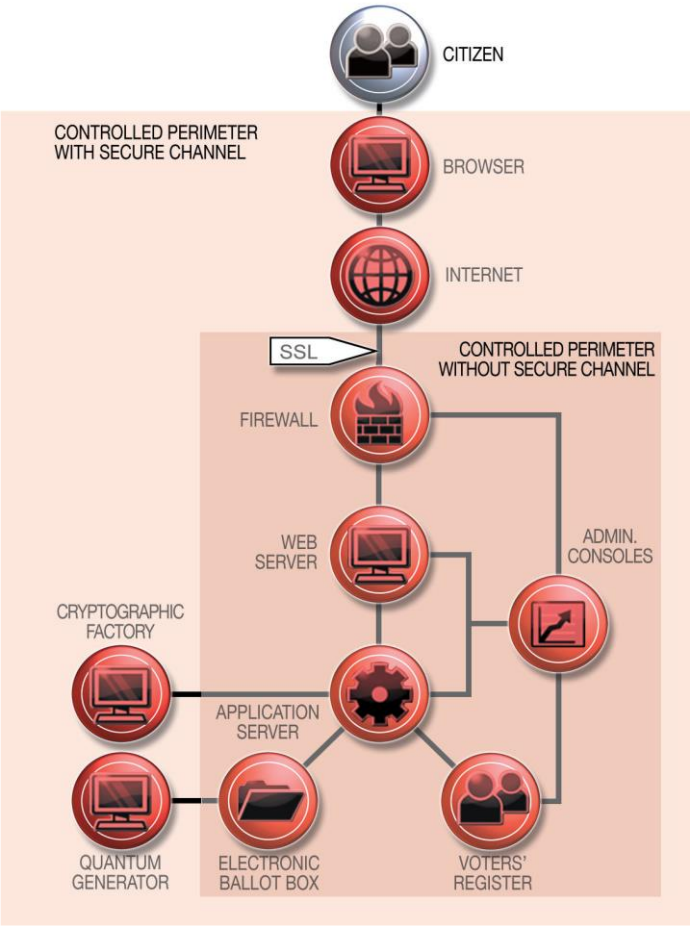

Fig. 3. The Geneva solution internet voting process
Source: Geneva State Chancellery, 2010

Comparative analysis of internet voting models. In this comparative analysis aspects of internet voting process of the different internet voting models are compared.

The voter registration methodology differs in the analyzed models. In the *Scytl* and *Cybernetica* models, voters registers on the internet voting day by joining the election website. Meanwhile, the *Geneva solution* internet voting model requires voter to register their place of residence in Swiss consular offices and are asked to renew registration every four years. The *Scytl* voting model enables voters to register and vote on devices with Google, Android, Blackberry and Apple IOS, while others allow voting only by usage of the personal computer.

The most sophisticated *voter recognition technique* is applied by *Scytl*, which declares that any method of voter identification could be adopted to the *Scytl* voting system. In the *Cybernetica* model, the identity of the voter is determined using a personal identity card and the government of Estonia encourages the use of a mobile signature. The *Geneve solution* voting model uses data from the card received by a voter for a special election and entering confidential data known only by voters: date and place of birth.

Voting and voice counting mechanisms and methodology. All analyzed internet voting models use public key

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

infrastructure to ensure voice secrecy by creating a double-envelope analogue that is used for postal voting. Only *Scytl* offers the ability to vote on devices with Google, Android, Blackberry and Apple IOS, while other voting models allow only the use of personal computer.

Scytl and *Cybernetica* models allow the voter to vote online as many times as needed counting only the last vote. This possibility reduces the probability of a bribe. *Geneva solution* model allows a voter to vote only once. In addition, the *Geneva solution* model users, after having voted online, lose the right to participate in postal voting or in traditional voting at the voting pole.

The *Scytl* model gives the voter possibility to check his voice and ensure that it was counted as expected. In this way, without submitting the content of the ballot, it's possible to make sure that the voice is recorded correctly. *Cybernetica model* sends a unique QR code to the voter. Citizens using smartphones can check that voice has been correctly recorded. The *Geneva solution* model does not provide voice verification feature.

The methodology for counting votes in the analyzed online voting models is very similar. After the election, electronic votes are firstly de-personalized and then recorded on a DVD or other media and transferred to a safe environment where they are decrypted using the election committees private key and counted.

Specifics of internet voting models audit. The *Scytl* internet voting system can be checked before, during and after the election. Election audit system is integrated with the management of security information and infringement reports. In the ongoing scan of vulnerabilities, the system has a real opportunity to block security breaches even before they cause damage to the system. The *Cybernetica* model uses an authentication server to monitor the internet voting process, which is an internal platform for tracking events and collecting statistics from the voice forwarding server and voice counting server.

In summary it can be stated that all the internet voting models are very different. All of them are united by the use of the *double envelope* technology to ensure the secrecy of votes. According to the authors *Geneva solution* model is unacceptable for the implementation in Lithuania internet voting due to insufficient security in determining the identity of the voter. The voter's card sent by mail may be stolen, and the date and place of birth of the voter is not classified as confident information in Lithuania. *Scytl* and *Cybernetica* models are much safer in this perspective. It is hard to decide which of the two models is better for Lithuania: *Scytl* which provides wider options for the voter when choosing a voting device or *Cybernetica*, whose vote checking method is criticized for potentially disclosing the content of the vote.

4. Evaluation of the characteristics of cybersecurity management during the implementation of Internet voting in Lithuania

Research methodology: Semi-structured expert interview method was chosen for the qualitative research. The survey was conducted by interviewing experts from two fields as currently there are no experts on cybersecurity management in Lithuania. Experts on Internet voting and cybersecurity were interviewed by the authors using two different questionnaires. Experts on Internet voting were asked about the security issues during connected with internet voting, while cybersecurity experts were questioned how to deal with cyber security issues that can occur during the usage or implementation of the internet voting systems. Six internet voting and six cybersecurity experts were interviewed during the survey.

Number of experts was based on the methodological assumptions presented in the classic testing theory, which states that the reliability of aggregated solutions and the number of decision-makers (in this case - experts) are associated through a rapidly decreasing nonlinear relationship. According to Baležentis and Žalimaitė, the group

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

of 7 experts is sufficient for a qualitative research, and the accuracy of the assessment is sufficiently precise. As the number of informants continues to increase, the accuracy of the assessment is increasing very slightly; therefore, it can be assumed that the reliability of the survey is sufficient (Baležentis, Žalimaitė, 2011).

The purpose of this survey: to clarify the issues of cybersecurity in connection with the internet voting and to provide with the possible solutions in accordance with the problems identified. *Survey tasks*: identify problems regarding the internet voting in Lithuania; discuss separate stages of the Internet-based voting system while keeping in mind the cyber security issues; find out what is the expert opinion on the possible security issues and security solutions to solve them; find out the point of view of cyber security experts on the most problematic aspects of the cybersecurity management in internet voting.

Issues of Internet voting. Three of the four internet voting experts participating in the survey indicated that the internet voting system is not legitimized in Lithuania largely due to the "*lack of political will*". A number of legislative amendments were prepared to validate the voting during the elections of the President and the Parliament of the Republic of Lithuania, municipal council or European Parliament, but all of them were rejected by the Parliament of the Republic of Lithuania. Other experts argued that the biggest problem with online elections is the lack of clarity: the amendments proposed to the Parliament on the possibility of voting online in the elections and referendums essentially will not restrict the voters from doing that through traditional means and will meet all the voting principles and requirements of the law; the electorate will be able to vote online several times, but only the last vote received from the voter will be counted. However, the whole internet voting process is not clearly defined to this day. Experts argued that before setting up the online voting (internet voting), it should be completely clear what type of system will be implemented and used during the internet voting process in Lithuania. Experts also recommended that the law should be clearer to identify and detail the principle features of the system, ensure a clear division of responsibilities between the institutions involved in the voting process and provide external control mechanisms to ensure competent and independent quality inspections during the process. According to a few experts, it seems that the internet voting is used by politicians in the advertising campaign, but it is not enough to initiate changes of laws to implement internet voting in Lithuania – it is necessary to carry out a lot of "*technical*" work too. It was noted, that risk analysis of the internet voting system in Lithuania is not carried out until now, but it is strictly mandatory to coordinate the tolerance of risks with the electorate of Lithuania.

While summarizing the answers of the experts to the first part of the questioner, it can be assumed that Internet elections in Lithuania are not legitimized due to four main reasons: lack of political will by the members of the Parliament; there is no consensus on how the Internet voting system should look like; no risk assessment carried out and tolerable risk levels are not defined; insufficient involvement of the society in the implementation of Internet voting processes. There is a lack of public information on the Internet voting topic (discussions, conferences).

The possibilities of using existing internet voting models in Lithuania. Experts emphasized that it is undoubtedly important that the internet voting should be integrated into the entire voting system of Lithuania as an integral part. This is a prerequisite for the creation of a well-functioning, uninterruptable election process. The opinions of experts on internet voting also differed due to the possible models of the internet voting in Lithuania. Only one expert confidently suggested using *Scytl* model in Lithuania. The expert highlighted the benefits of the *Scytl* internet voting model: it is possible to install different voter identification tools and it can be easily integrated into devices using Google, Android, Blackberry and Apple operating systems providing the same level of security as a personal computer. Other experts, however, spoke more cautiously about the *Scytl* model. One of the experts distinguished *Cybernetica* voting model as the most suitable for Lithuania. In Estonia *Cybernetica* model was suitable due to the well-developed electronic signature infrastructure. Meanwhile in Lithuania, while the majority of citizens have the electronic signature on a personal identity card, but rarely use this option. The remaining

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

experts were unable to tell which model of the internet voting would be best to use for the elections in Lithuania. Experts emphasized that in development of the model of the Lithuanian internet voting system it is necessary to clearly identify requirements that are compatible with the laws of the Republic of Lithuania and the specifics of the public administration system.

To summarize, it can be stated that internet voting experts do not agree on the particular internet voting model that should be selected and used in the context of internet voting in Lithuania. Experts suggested using either *Scytl* or *Cybernetica* model. It was also believed that Lithuania, using global practice, could develop its own model of internet voting which could be adapted to the specifics of the Lithuanian legal framework and public administration specifics.

Security problems of Internet voting. One of the most important conditions for conducting internet voting is to ensure that only eligible Lithuanian citizens can vote using the internet voting system and that the person could be clearly identified. One of the experts said that the internet voting is very similar to the pre-voting (postal voting using two envelops principle): the voting pole opens the external envelope, finds the identity of voter and verifies that the voter has voted. It is also checked whether the voters belongs to the voting area and that voter did it only once. When everything is checked, the election committee marks voters list and indicates that the voter has voted. The inner envelope with the voting ballot is put into the ballot box with the other envelopes. All of these principles must remain during the internet voting and it can be achieved through cryptographic measures. All interviewed internet voting experts have unanimously opposed the use of the online banking system for the voter identification for the internet voting system in Lithuania. One expert stressed that confidentiality in the bank is understood as the protection of information from third parties. Meanwhile, the bank knows and sees all the steps of its customers. The secrecy principle of the voting is based on the fact that the system does not know how the voters voted. Voting system just could identify the fact that voter has voted, but it cannot identify for which candidate or party. According to the expert, this is a *significantly higher level of system secrecy*. Experts also mentioned that the identity of the voter in the Lithuanian internet voting could be determined using an electronic signature or a mobile signature. The opinion of experts on the possibility of using a personal ID card for identification was split: three experts said that this project failed in Lithuania, but did not deny that it was a safe way to both identify and vote; meanwhile, other experts said that it is essential to provide the wider variety of choice of identification measures for internet voters and it is most important that it has to be safe and reliable.

As a problematic issue, experts identified the voters' ability to test their choice (the possibility to receive voting confirmation). This option is mentioned in the amendments. One expert noted that the *Scytl* internet voting model is currently using the best voice verification method. The voter can take a few steps to verify if his voice has been counted and counted as intended. Other experts mentioned the checking method used in the Estonian internet voting model, but this model has been criticized for the release of vote content, which creates the possibility to buy voices. One expert feared that internet voting would create additional opportunities to buy/sell votes. Meanwhile other experts have stated that the criminal purchase of votes in Lithuania has been noticed a few times, while the possibility of voter to vote many times through the internet and later traditionally at the voting pole would cause the decrease in the bribing the voters.

In summary it can be concluded that there are five main problematic points of the internet voting: the registration of the voter; identification of the person in cyber space; possibility for the voter to check his voice; additional opportunity to bribe voters and issues of internet voting audit.

Internet voting cybersecurity management issues: cybersecurity experts (participating in the survey), after being asked about the cybersecurity management issues in the internet voting organization and implementation process, unanimously emphasized that currently it is not possible to ensure the security of voters device used for internet voting without compromising voters privacy. Experts noted that frequently citizens may use some *pirated*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

software on a personal computer or not have a supported antivirus program which can update its virus databases from the official source. Some expert, working with cyber security issues, mentioned the naivety of users when the use of pirated antivirus programs is providing them with a false sense of security (outdated software, not up to date definitions, possibly malicious cracks used). In solving the problem of an unsecure voter device (personal computer), several experts suggested together with internet voting program to install a Java script that would block other applications during the internet voting process. However, experts warned that this could violate voters' privacy. Experts have published recommendations for the voter that should be followed during the voting over Internet: web page address should be typed manually (clicking on link could lead to phishing websites using *social engineering*); ensure that encrypted HTTPS connection is used during the communication with a server; verify that the site security certificate exists and is still valid. Experts mentioned that a cyber attack could also be expected while the voter is communicating with the internet voting system. All experts recommended the use of a secure encrypted communication channel to guarantee the confidentiality and integrity of the data transferred between voters computer and internet voting system.

According to cybersecurity experts, absolute security exists only theoretically - even in the most protected systems, there is always a possibility of an error and intrusion - this possibility cannot be eliminated. Therefore, before the internet voting system is implemented and used, a comprehensive risk analysis (risk assessment, probability of occurrence, damage, possible resources, risk reduction, etc.) and a tolerable risk assessment are required.

In conclusion, it can be stated that at present, without violation of personal privacy, there are no technical possibilities to ensure the safety of a voter's device - only recommendations to secure the device can be made (but the voter has to follow them). Secure communication between the voter and the internet voting system can be ensured using a secure encrypted connection (TLS). Cybersecurity experts also recommend the use of all possible technical, organizational and legal measures to protect internet voting system.

5. Dynamic analysis of public opinion on the possibility to implement Internet voting in Lithuania.

Two identic studies were carried out to evaluate the public opinion, as well as the support or disapproval towards the implementation of electronic voting systems in Lithuania (the first research was conducted in 2007, second in 2017).

Research methodology: research was carried out using a questionnaire consisting of twenty questions. The target sample size must be at least 384 respondents. As the population continues to grow, the number of respondents varies considerably, so it can be assumed that the reliability of the study is satisfactory. In 2007, 419 respondents were interviewed, and in 2017 researchers addressed 436 respondents, while the reciprocity of the questionnaire was 63 and 54 percent respectively.

Results of the study: As it was mentioned, 419 and 436 respondents were interviewed during the study. The distribution of respondents (by age) is presented in Chart 1.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

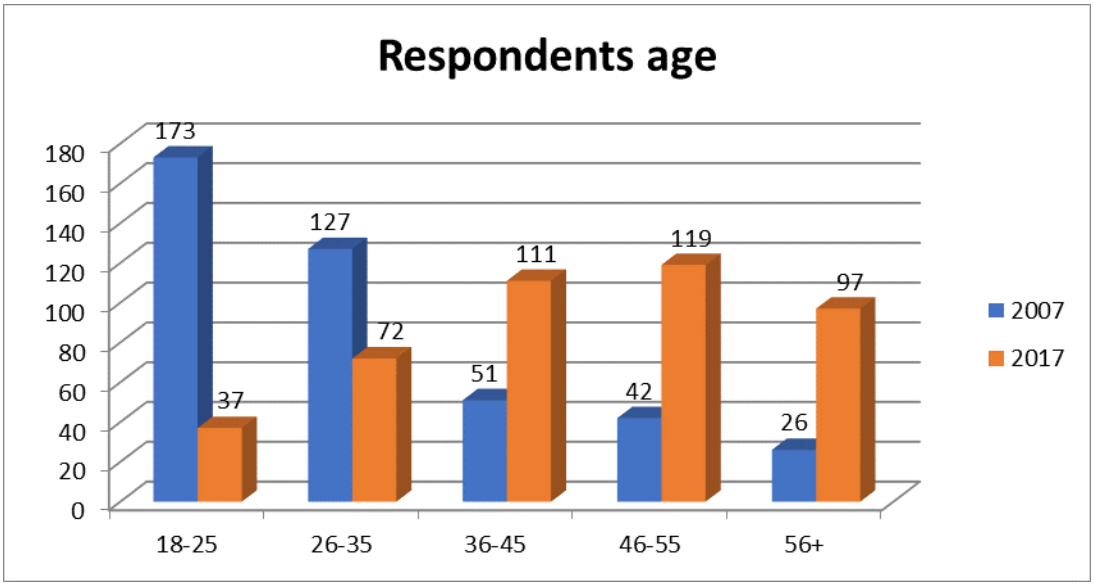

Chart 1. Distribution of respondents by age.
Source: Compiled by authors.

The distribution of respondents by gender is presented in Chart 2.

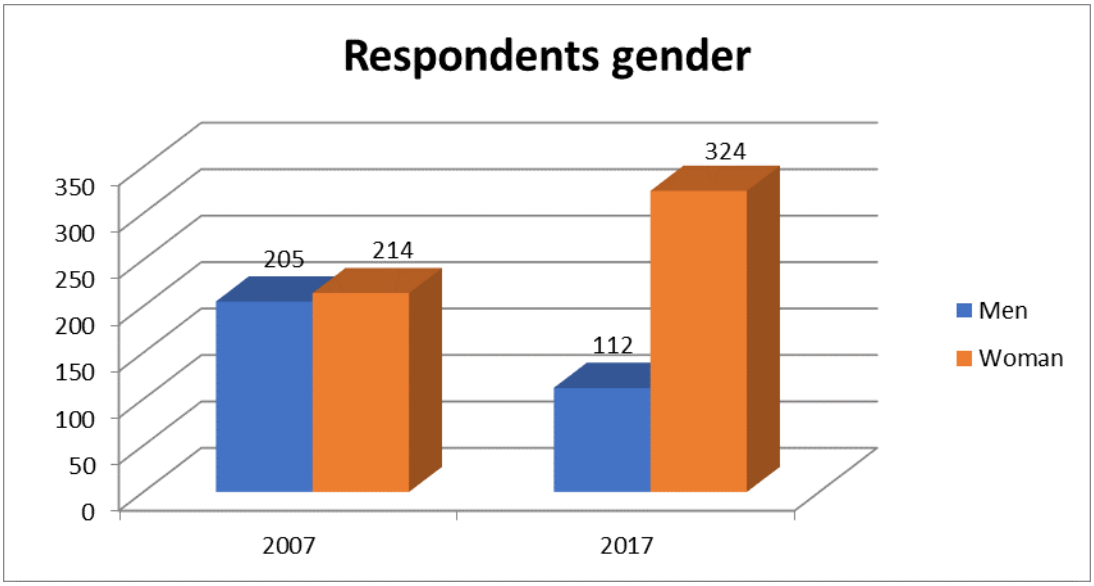

Chart 2. Distribution of respondents by gender.
Source: Compiled by authors.

The distribution of respondents according to their place of residence is presented in Chart 3.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

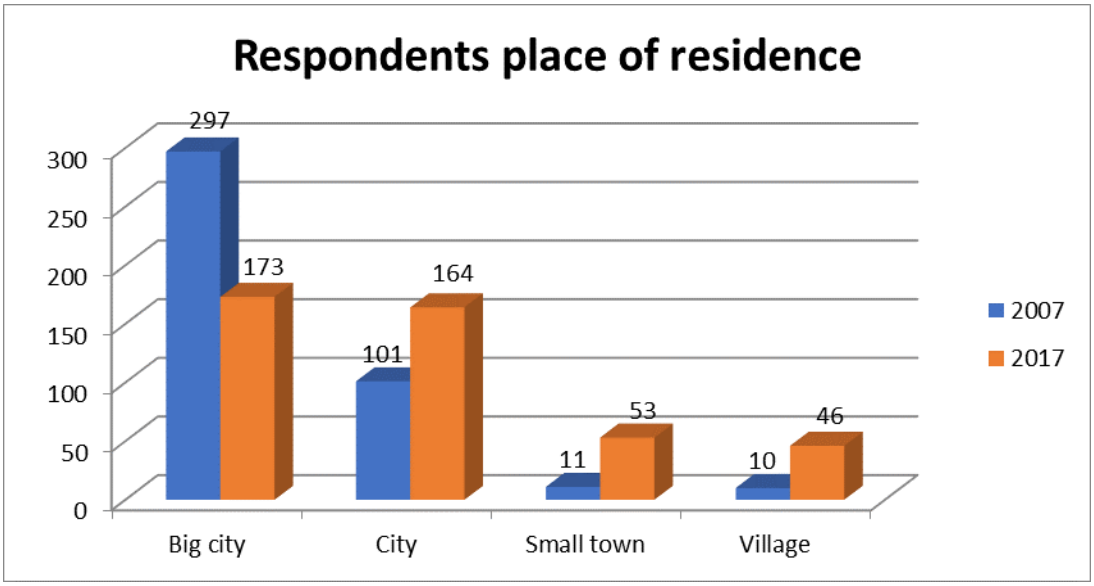

Chart 3. Distribution of respondents according to their place of residence.
Source: Compiled by authors.

Distribution of respondents by education is presented in Chart 4.

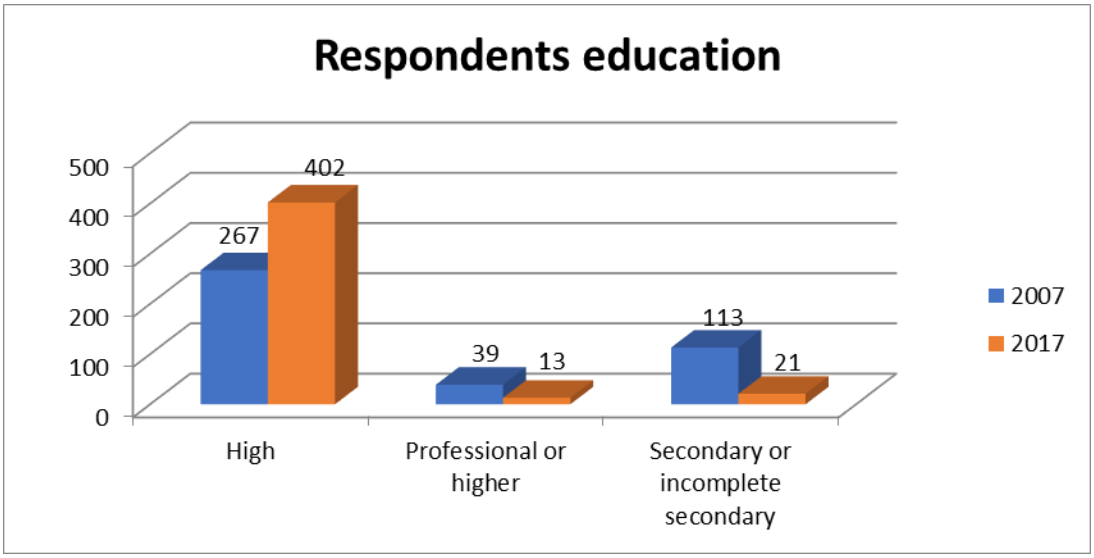

Chart 4. Distribution of respondents by education.
Source: Compiled by authors.

The distribution of respondents according to their occupation is presented in Chart 5.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

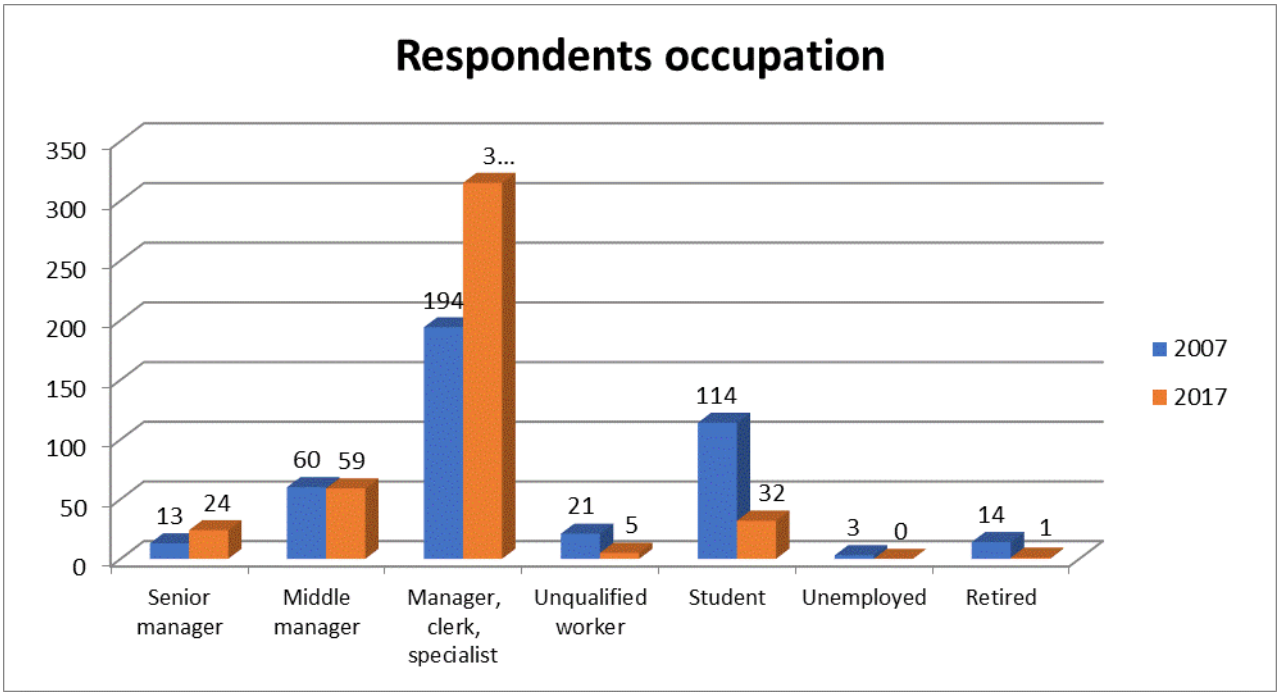

Chart 5. Distribution of respondents according to their occupation.
Source: Compiled by authors.

The distribution of respondents by income is presented in Chart 6.

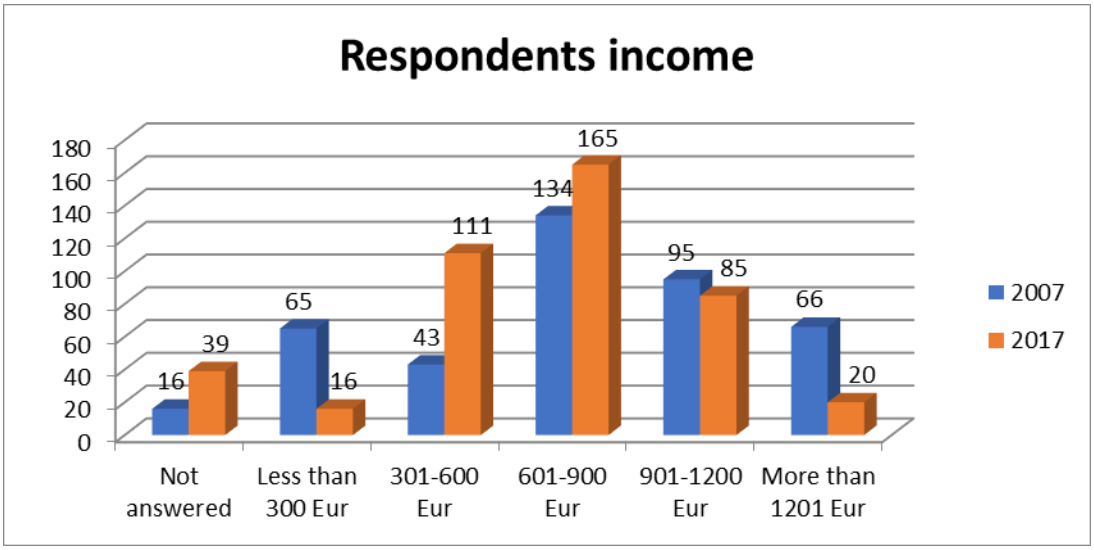

Chart 6. Distribution of respondents by income.
Source: Compiled by authors.

The distribution of answers of respondents according to the distance from their home to voting pole is presented in Chart 7.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

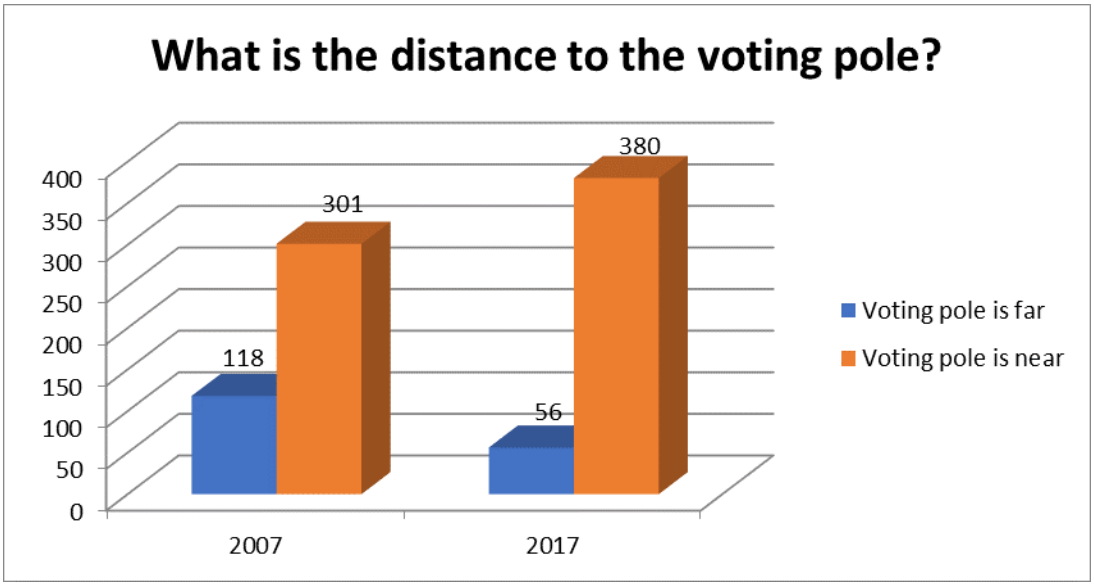

Chart 7. Distribution of respondents answers about distance from their home to voting pole.
Source: Compiled by authors

The distribution of answers of respondents based on their participation in elections is presented in Chart 8. It can be argued that respondents are participating in the elections more actively.

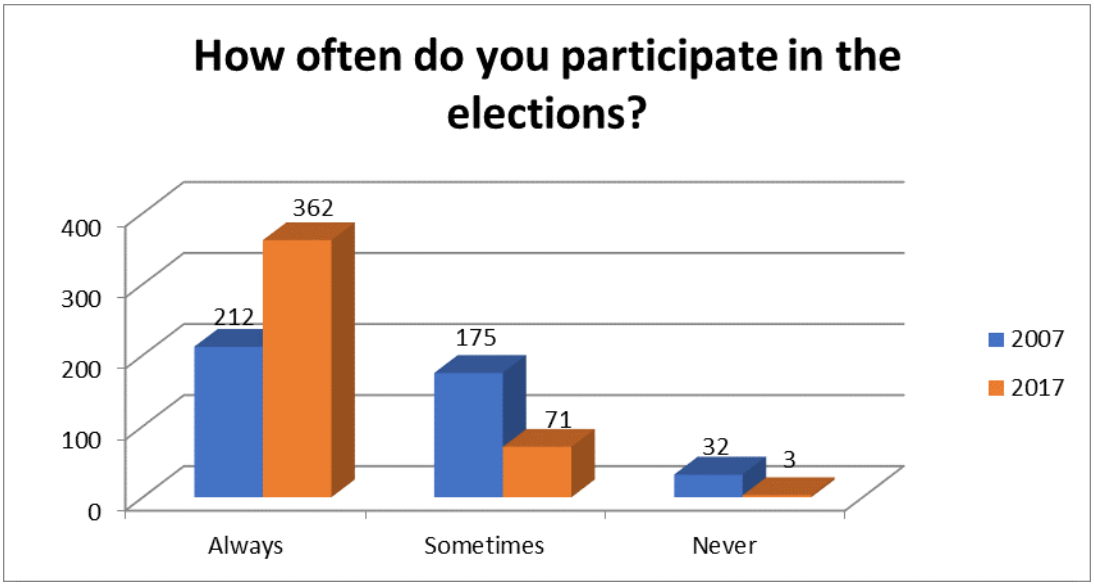

Chart 8. Distribution of respondents answers about their participation in elections.
Source: Compiled by authors

The distribution of answers of respondents based on non-participation in elections is presented in Chart 9. It can be stated that respondents began to favor candidates in the elections more favorably, but the inadequacy of candidates is still the main reason that encourages residents to refuse to participate in the elections. Only the respondents who answered the previous question "sometimes" or "never" were evaluated.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

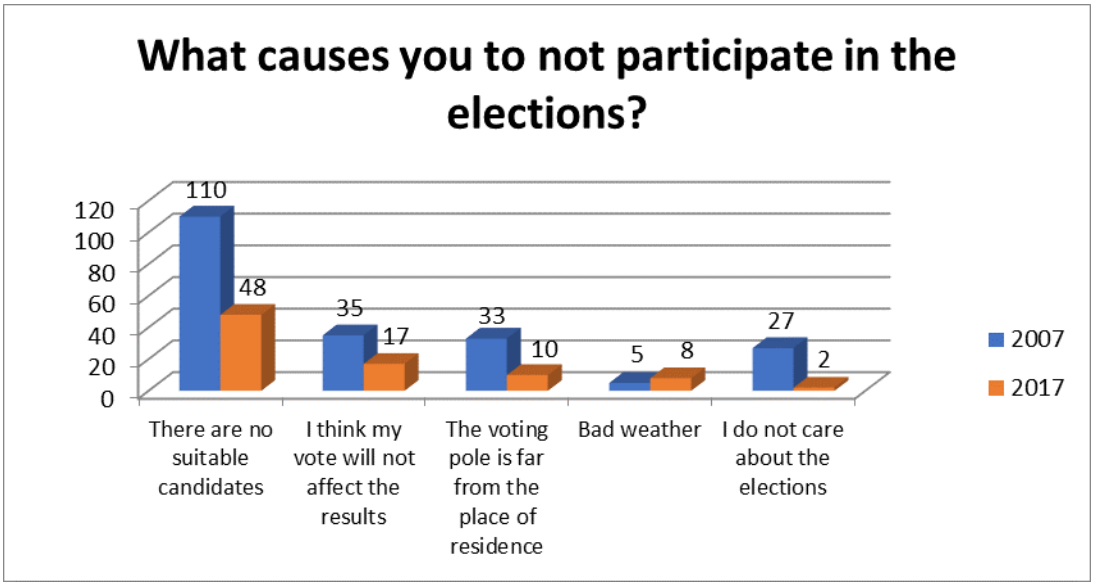

Chart 9. Distribution of respondents answers about non-participation in elections.
Source: Compiled by authors

The opinion of respondents on internet and traditional elections is presented in Chart 10. It can be noted that in the surveys conducted in 2007 and 2017, respondents considered internet voting more attractive than the traditional method of voting.

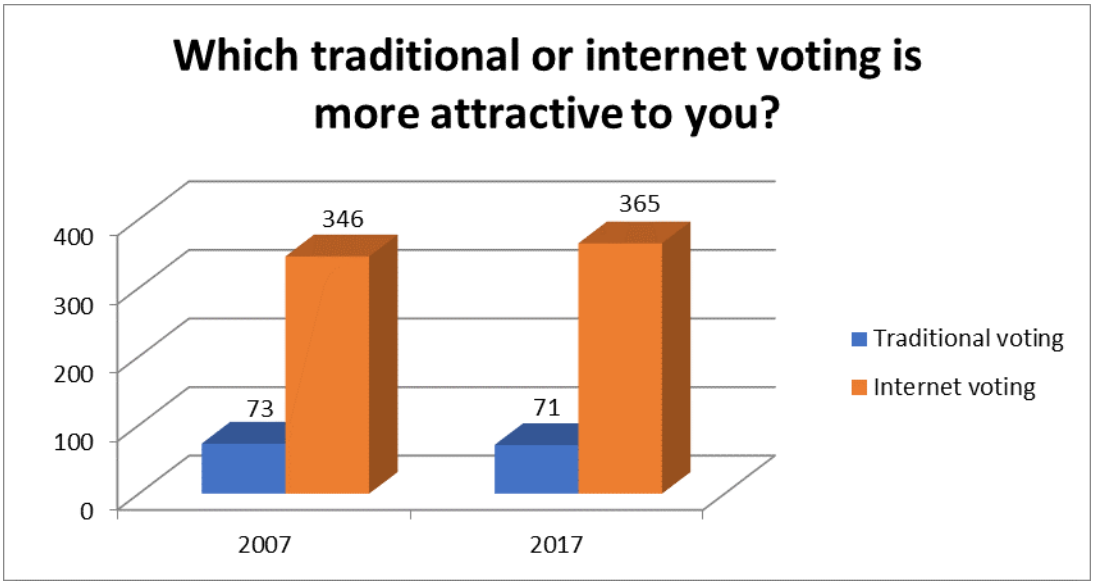

Chart 10. The respondents' opinion about internet and traditional voting.
Source: Compiled by authors

The distribution of answers of respondents based on the use of identification tools in the electoral process is presented in Chart 11. It can be noted that most respondents considered the identification by using electronic banking as the priority. It can also be noted that there was a drop in respondents consent to the use of personal identification cards with electronic signature, as well as the desire to use an additional identifier. There is a slight increase in the possibility to use mobile signatures, but it is not as obvious as the increase in the number of supporters of the use of the banking system's as the identification tool.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

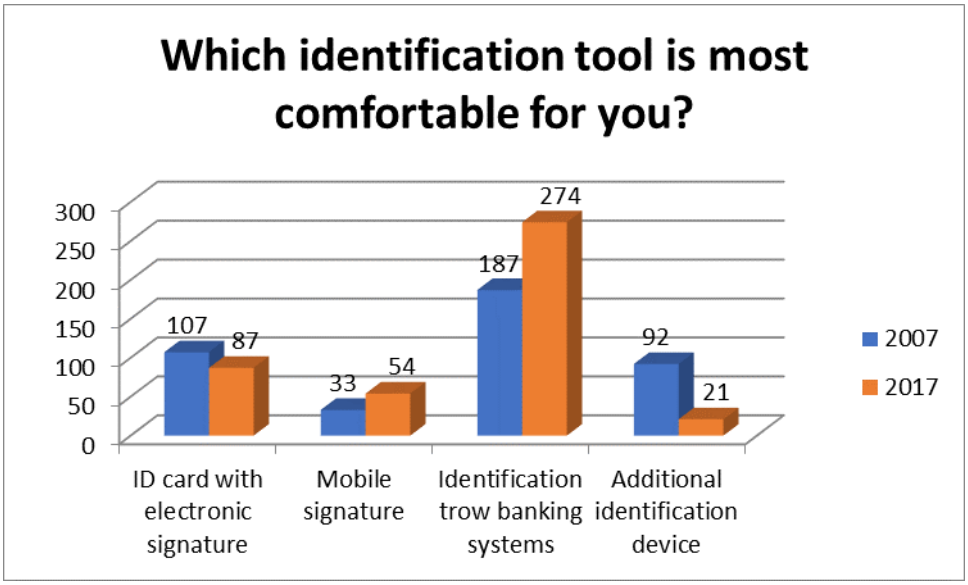

Chart 11. Distribution of respondents' responses about the use of identification tools in the electoral process.
Source: Compiled by authors

The respondents opinion on the impact of internet voting on voter turnout is presented in Chart 12. Most respondents believe that the implementation of internet voting would fundamentally change voter turnout during the elections and encourage them to take part in them.

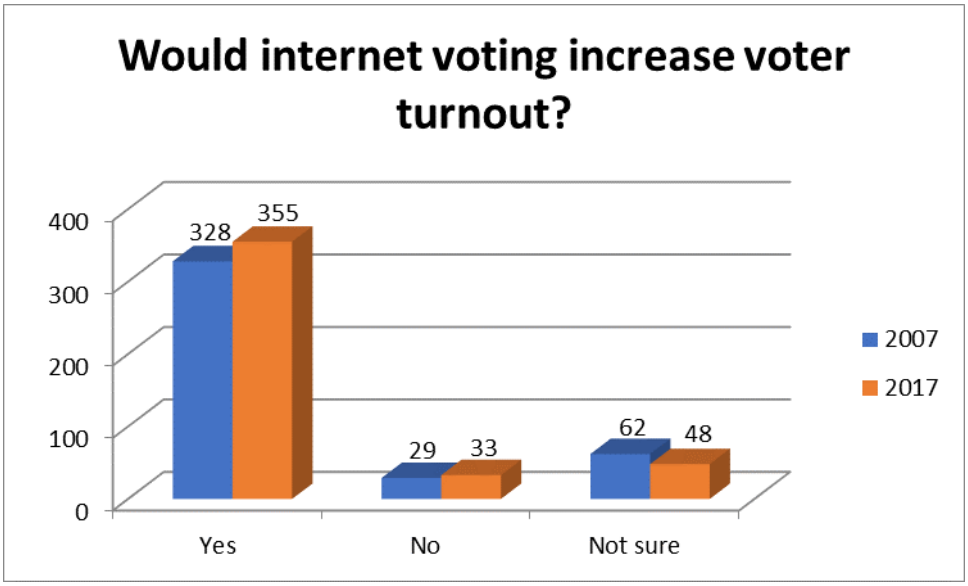

Chart 12. Respondents' opinion on the impact of internet voting on voter turnout.
Source: Compiled by authors

The distribution of answers based on the use of internet voting systems when living or working abroad are presented in Chart 13. During the surveys, respondents positively assessed the possibilities to use the internet voting system if they lived or worked abroad. It can be argued that the number of respondents, evaluating more positively has grown in 2017 and the number of people who have not known or disliked the idea of using such system has decreased.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

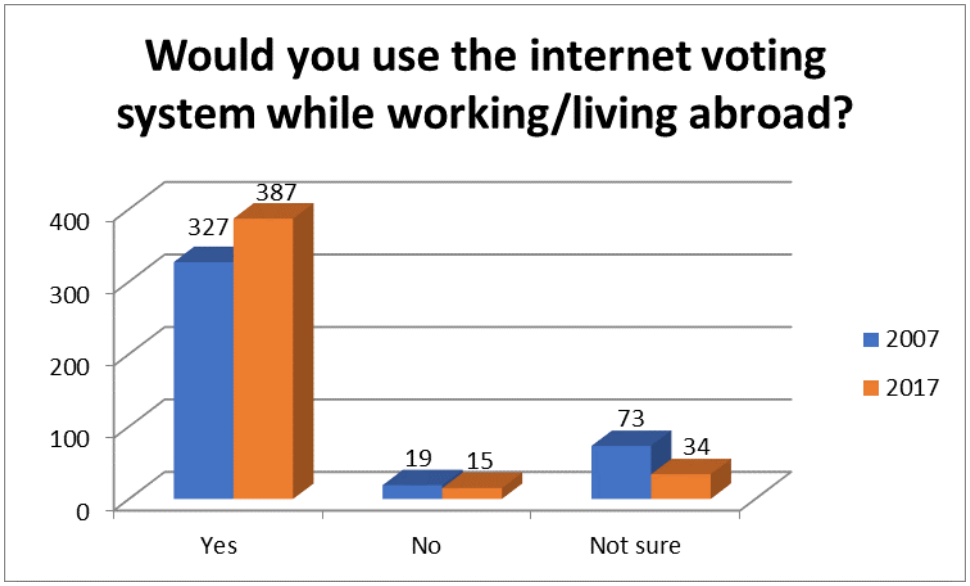

Chart 13. Respondents' answers on the use of internet voting systems when living or working abroad.
Source: Compiled by authors

In the course of the survey, respondents were also asked questions about traditional and internet voting systems:

- Question 1: Are you satisfied with the current voting system?
- Question 2: How do you rate the internet voting system?
- Question 3: Would internet voting boost your electoral performance?
- Question 4: Would you support capability to vote in any voting pole?
- Question 5: Would you support the roll-out of the internet voting end before traditional voting begins?
- Question 6: Would you support the fact that once person have voted online, there would be a possibility to change his or her choice during the voting in a voting pole?
- Question 7: Do you agree with the statement that electronic voting may positively affect voting transparency?

The summary of answers is presented in Chart 14. As it can be seen, respondents began to favor existing traditional voting system, but the internet voting system also received a more favorable assessment from respondents. Respondents also noted that they favored the emergence of an internet election system and believes that this system would encourage them to participate in the elections more actively. It was also noticed that respondents welcome the possibility of casting their vote in any voting pole, and also agree that electronic election service would begin and end before the election process in the voting poles. Answering the question about the possibility of changing the will expressed during the internet voting, respondents, as in 2007, evaluated this possibility negatively.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

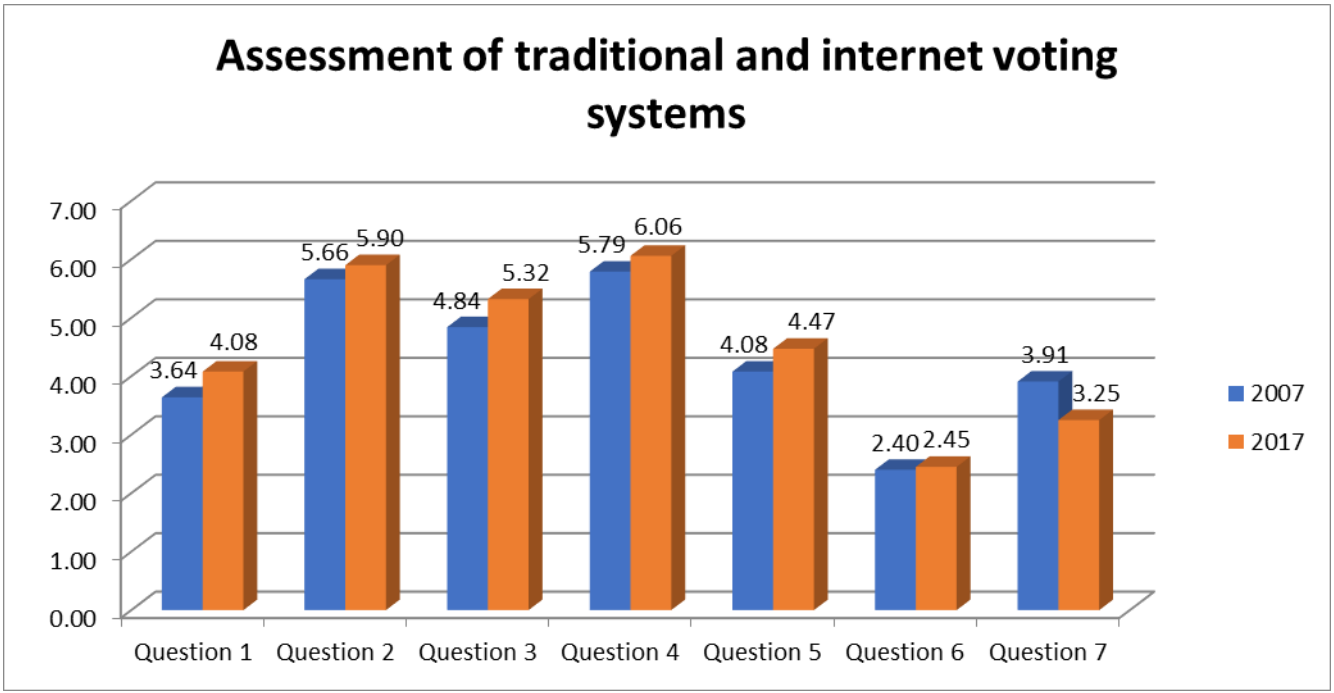

Chart 14. Assessment of traditional and internet voting systems.
Source: Compiled by authors

To sum up, it can be said that the public is beginning to see the internet voting as a more favorable choice than in 2007, although this favor is not yet very clear. It should be noted that the residents of Lithuania do not consider that it would negatively influence the transparency of the voting (internet vote security), and the statements of politicians and political parties, that citizens do not understand the security mechanisms used in the internet voting process and therefore are not prepared for the introduction of this technology, are not well motivated. Respondents also believe that the emergence of internet voting will help solve the problems of active participation in the country's political processes. Most respondents believe that the implementation of internet voting would fundamentally change turnout of voters during the elections and encourage them to take part in them.

6. Proposed cyber security model for the Lithuanian internet voting

The process modeling methodology was chosen for the development of the internet voting cyber security management model. Activity-oriented approach is chosen for the development of the model, focusing on the activities of the process and the relationships between them. Other elements of the process are not defined or analyzed in the context of process activities.

The purpose of the simulation is to create a cyber security model for managing of internet voting system. Modeling tasks:

- Create internet voting system infrastructure;
- Draw a logical internet voting scheme;
- Integrate cyber security management tools into the final model.

Before the analysis of the internet voting cyber security management model it is assumed that the devices of users, participating in the voting system, has a legitimate, regularly updated operating system with legal and

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

proprietary software supported by the manufacturer. The device is securely configured, with an updated antivirus program installed and etc.

According to the proposed internet voting cyber security management model (see Fig. 4), voters connect to the internet voting systems webpage using secure (TLS) connection using its own equipment and own internet connection or connection which could be provided by public libraries or other trustworthy places where an internet-capable device can be used. The voter downloads the application used for internet voting and installs it onto the device that will be used for voting (computes, phone or etc.). By using a mobile signature or other secure electronic signature voter confirms his identity and registers to the internet voting system.

Internet voting system, for security reasons, communicates with an external (unsafe) environment only through the demilitarized zone (DMZ). All communications initialized only from the inside of the network. In other words, it's not possible to directly connect to the internet voting system from the outside. The DMZ has a firewall software that allows only the default size and type queries and monitors the whole traffic. During the DDoS attack, the firewall application blocks and filters attacker's connections allowing legitimate user to connect to the system. The communication server periodically sends queries to the DMZ zone. When the voter sends a registration request, the communication server receives it and verifies the voter's eligibility (according to the voter's public key). According to the voting district to which voter belongs (place of residence), an electronic ballot is sent to the voter. If the voter is voting using the internet voting system for the second time, the internet voting system shall remove the previous vote from the ballots storage server and send him a new electronic ballot.

After the voter fills electronic voting ballot internet voting application encrypt it with an election committee public key (inner envelope) and voter signs encrypted ballot with his private key (external envelope), ensuring that the ballot belongs to that exact voter. Then voting ballot is transferred to internet voting system using encrypted communication channel.

Ballot travels into the DMZ zone. Electronic ballots storage server periodically sends queries to the DMZ zone server and transfers encrypted and signed ballots to the ballot storage also sends information to the voter database, marking the voter as one who has already participated in the internet voting. A voucher with a unique QR code (valid for 30 minutes) is sent to the voter to create the possibility for a voter to check if his choice has been correctly transferred and recorded on the ballot storage server.

Encrypted ballot is saved on a ballot storage server until the end of the traditional voting in voting polls. After closing the voting polls, voter identities are removed from the encrypted ballots (the inner envelope is removed from the outer envelope). Election committee audit team is monitoring the process of ballots depersonalization. After that, encrypted ballots are recorded on a DVD and transferred to a secure environment where the ballots will be decrypted and counted. Election audit follows the process of decoding and counting votes and after the end of counting the results are published.

All communications between the voter and the internet voting system during the voting processes is organized using a secure encrypted TLS connection. Internet voting system must be tested and certified before it is going to be used in elections. In order to ensure the security of the voting system from external and internal threats, a security policy that includes technical, organizational and legal security measures must be developed. While implementing the Resolution of the Government of the Republic of Lithuania (No. 716 of 24 July 2013) on general requirements for the security of electronic information, safety regulations, rules for the safe management of electronic information, information system continuity management plan and the rules for the administration of the information system must be prepared and approved.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

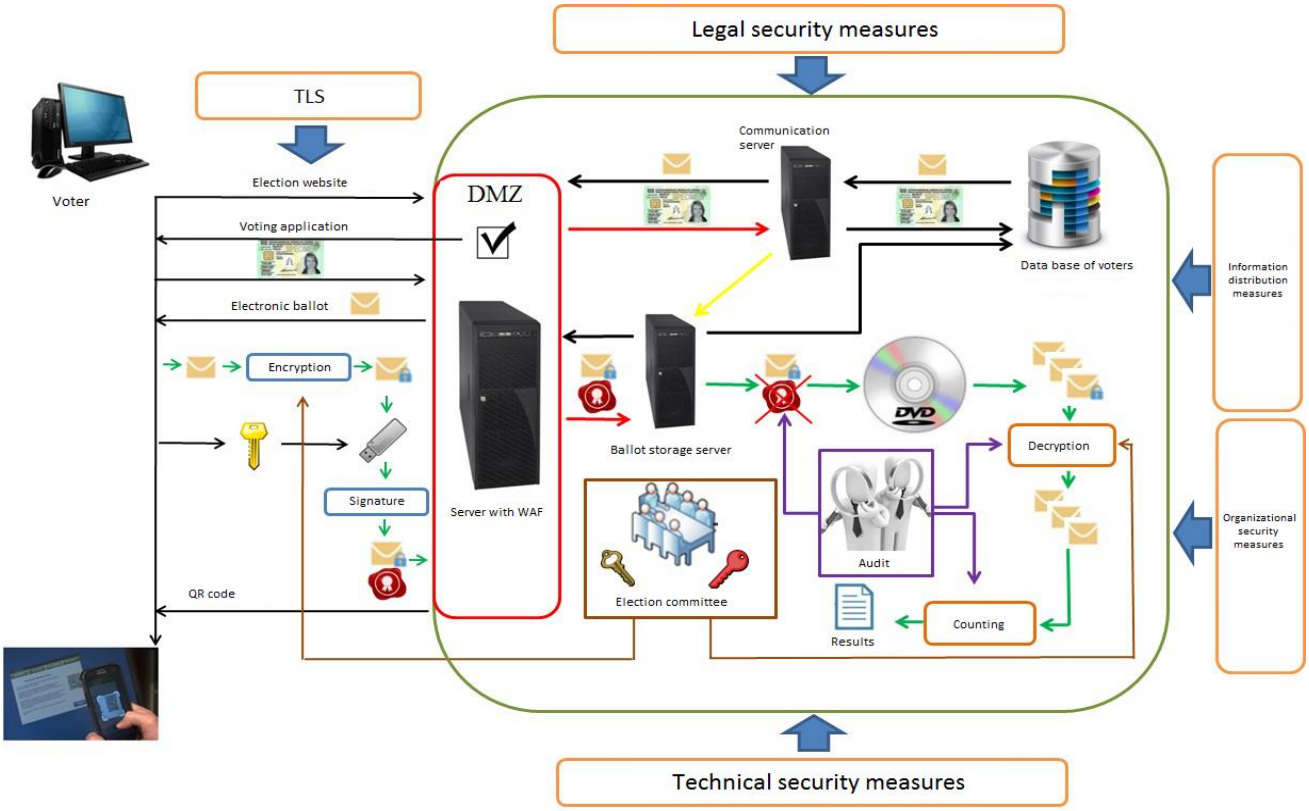

Fig. 4. Internet voting cybersecurity management model
Source: Compiled by authors

Possibilities and development perspectives of the Internet voting model. Created internet voting cyber security management model is based on good theoretical and practical examples: *Scytl* that is used in France, United Kingdom, Norway, Austria etc. and *Cybernetica* which is successfully operating in Estonia and "*Geneva solution"* internet voting models. The issues of Internet voting model have been discussed with internet voting experts and cybersecurity experts who have made recommendations on the cyber security management model. During the development of the model authors took into consideration specifics of public administration and the legal regulation in Lithuania: legal acts regulating the security of electronic information and cyber security in Lithuania, laws of the Parliament and Presidential elections, municipal councils and elections to the European Parliament, referendum law and five amendments to these laws, allowing the possibility to use the internet voting systems during the elections were analyzed. Therefore, it can be argued that represented internet voting cyber security management model could be used to conduct internet voting not only in Lithuania, but also, considering the similar legal regulation on cyber security and internet voting, in other Member States of the European Union.

Concept of Internet voting during the Elections and Referendums was agreed upon in Lithuania in 2006. Government of the Republic of Lithuania approved Internet Voting Implementation Program in 2007; it was designed to create and implement an internet voting system. Nowadays this Concept is morally obsolete and the Program has not yet been implemented. The perspective of the Internet cyber security management model represented by the authors in Lithuania is limited by the fact that currently internet elections are not legitimated, i.e. there are no laws regulating the possibility to use internet voting systems during the elections of the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Parliament, President, European Parliament, municipal councils and voting in referendums. However, if the amendments to the aforementioned electoral laws were to be adopted, the model could be applied in the internet voting in Lithuania.

The internet voting cyber security management model is very similar to the *Scytl* and *Cybernetinca* models: models are united by the same phases of the internet voting process (registration, identity verification, ballot encryption, vote confirmation, voice counting and storage, deletion, decryption and counting procedures). Author's proposed model, like *Scytl*, uses the same identification methodology. Ballot encryption takes place using the public key infrastructure methodology by creating a double-envelope analogue (used by *Scytl* and *Cybernetica*); voice counting technology is the same as for the *Cybernetica* internet voting model (usage of QR code).

The analysis of *Scytl* and *Cybernetica* voting models involved only the internet voting process, providing the secure communication between the voter and the voting system. Publicly available sources do not provide any information about the technological aspects of cyber security management in these internet voting systems. Internet voting cyber security management model includes the entire range of legal, technical and organizational security measures. These measures and instructions should help preventing, detecting, analyzing and responding to incidents while also providing the system recovery after the incident or attack.

The strength of the proposed internet voting cyber security management model is that it has benefited from global good practices and takes into account the views and recommendations of internet voting and cyber security experts. The model does not specify the methods and methodologies used during the internet voting process stages, which would make the perception of the model more difficult. However, it can be broken down into scenarios according to the stages of the internet voting process, which could indicate the methods proposed for certain stages. Depending on the aspects of public administration internet voting cyber security management model can be adopted by other EU Member States with similar legislations.

Conclusions

After reviewing the opinions described in the scientific literature, it can be stated that internet voting should be subjected to the requirements of traditional voting and all principles of democratic elections and referendums, also cyber security management, information dissemination, organizational and technical measures must be retained. The whole range of these tools should help protect against the internal (administrators, other system users and civil servants) and external (foreign intelligence services, software, typical criminals, and hacktivists) intruders during all stages of the internet voting process.

Currently period authorities of Lithuanian government institutions are only declaring their intention to legitimize internet voting. However, the peculiarities of the legal regulation of the Republic of Lithuania, the amendments to electoral laws and the global opinion on cyber security allows us to expect that the situation is going to change shortly and legal acts will be adopted to allow the possibility to use the internet voting in election processes, as well as development of the internet voting system.

The survey on the possibility of implementing internet voting in Lithuania has shown the attitude of the population towards this *problem*. It is noticeable that in the last decade the opinion of the Lithuanian population on the possibility of internet voting has changed slightly and this opportunity is viewed by Lithuanians as a positive thing. Further changes in the opinion of the population can be encouraged through the implementation of programs (campaigns) for the promotion of internet voting as well as through the explanation of the peculiarities of the structure and functioning of the newly introduced voting system for the population. It should be noted that the residents of Lithuania do not consider that it would negatively influence the transparency of the voting

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

(internet vote security), and the statements of politicians and political parties, that citizens do not understand the security mechanisms used in the internet voting process and therefore are not prepared for the introduction of this technology, are not well motivated. Survey respondents also believe that the implementation of internet voting will help solve the problems of participation in the country's political processes. Most respondents believe that the implementation of internet voting would fundamentally change voter turnout during elections and encourage them to take part in the elections.

Despite the absence of technical barriers (without violating personal privacy, there is currently no way to secure the voter during the internet voting process), legitimization of internet voting could not be done because of the lack of political will. There is currently no consensus on what the model for internet voting should look like. So far risk assessment has not been carried out and tolerated risk has not been identified. The lack of trust of citizens towards the online voting system is based on the insufficient society involvement in the implementation processes of internet voting.

The internet voting model, which should be implemented in Lithuania, should unite methods and technologies that are used in *Scytl* and *Cybernetica* internet voting models. Proposed internet voting cyber security management model was developed using the best features of *Scytl* and *Cybernetica* models, taking into account the views and recommendations of internet voting and cybersecurity experts. The model was developed in accordance with the existing specifics of public administration and the legal regulation in Lithuania. The internet voting cyber security management model could be used to implement internet voting not only in Lithuania but also in other EU Member States with similar legislation base.

References

Antonucci D. 2017. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.

Association for Computing Machinery, (2006). Statewide Databases of Registered Voter: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery. Available on the Internet: https://people.eecs.berkeley.edu/~daw/papers/vrd-acm06.pdf

Baležentis A.; Žalimaitė M. 2011. Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. Available on the Internet: http://mts.asu.lt/mtsrbid/article/viewFile/269/298

Barrat J.; Goldsmith B.; Turner J. 2012. International Experience with E-Voting. Norwegian E-Vote Project. Available on the Internet: https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf

Clarke D., Martens T. 2017. E-Voting in Estonia. Real-World Electronic Voting: Design, Analysis and Deployment, p. 129-141, CRC press.

Cyber security law of Lithuania Republic, 2014.

Cybernetica, 2015. For greater safety and security in the world. Available on the Internet: http://cyber.ee/en/about-us

Dykstra J., 2017. Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.

Elections BC. A non-partisan Office of the Legislature, (2011). Discussion Paper: Internet Voting. Available on the Internet: http://www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf

Erbschloe M., 2017. Threat Level Red: Cybersecurity Research Programs of the U.S. Government, CRC press.

Estonia.eu. 2015. Estonian Internet voting system.

Fuschi D.L.; Tvaronavičienė M. 2013. Big Data and supervisory control: service quality in the banking sector, Journal of Security and Sustainability Issues 3(3): 5-14. http://dx.doi.org/10.9770/jssi.2013.3.3(1)

General Lithuanian Police Commissioner Order No. 5-V-101 "On Approval of the Description of the Information Required for Cybercrime Investigations, Possessing, Police Instructions and Cybersecurity Investigation Procedures" (2015).

Geneva State Chancellery, 2010. The Geneva internet voting system. Available on the Internet: https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/EVoting_Documentation/passport_evoting2010.pdf

Goldsmith B., 2017. Guidelines for Trialling E-Voting in National Elections. Real-World Electronic Voting: Design, Analysis and Deployment, p. 19-47, CRC press.

Halderman J. A., 2017. Practical Attacks on Real-World E-Voting. Real-World Electronic Voting: Design, Analysis and Deployment, p.143-170, CRC press.

Hampson C. N., 2012. Hacktivism: A New Breed of Protest in a Networked World. Boston College Internwtional and comparitive Law Review, p. 511-542.

Hao F., Ryan P. Y. A., 2017. Real-World Electronic Voting: Design, Analysis and Deployment, CRC press.

Independent Panel on internet Voting, (2014). Recommendations Report the Legislative Assembly of British Columbia. Available on the Internet: https://www.verifiedvoting.org/wp-content/uploads/2014/10/CA-BC-2014-recommendations-final-report.pdf

Jastiuginas S., 2011. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje [Management of information security in public sector], Informacijos mokslai 57: p. 7-25.

Jefferson D., Rubin A. D., Simons B., Wagner D., (2004). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).

Kiškis M. et al., 2006. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universitetas.

Kohnke A., Shoemaker D., Sigler K., 2016. The complete guide to cybersecurity risks and controls, CRC press.

Law on State and Service of Securities of the Republic of Lithuania, 1999.

Limba T.; Agafonov K., 2012. Elektroninių rinkimų sistemų konstravimo principai, modeliai ir jų apsaugos užtikrinimas [Construction principles of electronic voting systems], Socialinės technologijos, 2(2): 376-389.

Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4): 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Lithuania state security department (2014). Kas, kaip ir kodėl šnipinėja Lietuvoje. Available on the Internet: https://www.vsd.lt/wp-content/uploads/2017/03/kaip-snipinejama-Lietuvoje.pdf

Middleton B., 2017. A History of Cyber Security Attacks: 1980 to Present, CRC press.

Ministry of the Interior of the Republic of Lithuania, (2005). Information security for employees of state institutions.

Owen T.; Noble W.; Speed F. C., 2017. New Perspectives on Cybercrime.

Parliamentary Research Department of the Parliament of the Republic of Lithuania, 2015. Online voting: foreign experience and perspectives in Lithuania. Available on the Internet: http://www.vrk.lt/documents/10180/556540/Balsification+internet.pdf/a5247fe6-d96e-437d-8135-5db76da1f66f

Puiggalí J.; Cucurull J.; Guasch S.; Krimmer R., 2014. Verifiability Experiences in Government Online Voting Systems.

Repečka G., 2007. Elektroninis parašas [Electronic signature], Naujoji komunikacija 16 (212): 22-24.

Repečka G., 2007. Saugus duomenų perdavimas internetu: SSL/TLS. Naujoji komunikacija, 12 (208), p. 15-16.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Resolution of Government of the Republic of Lithuania No. 796 "On the Approval of the Program of Electronic Information Security (Cybersecurity) Development in 2011-2019" .2011.

SANS Institute InfoSec Reading Room, 2001. Understanding Intrusion Detection Systems. Available on the Internet: https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337

Scytl Innovating Democracy, 2015. Scytl Voter Registration. Available on the Internet: http://www.scytl.com/en/products/pre-election/scytl-voter-registration

Scytl.com, 2017. Online voting technology. Available on the Internet: https://www.scytl.com/wp-content/uploads/2015/09/DIGITAL_online-voting.pdf

Shah N., 2013. On The Radar: Scytl. An end-to-end election modernization platform.

Shahandasht S. F., 2017. Electoral Systems Used around the World. Real-World Electronic Voting: Design, Analysis and Deployment, p. 77-102, CRC press.

Springall D. et. al., 2014. Security Analysis of the Estonian Internet Voting System. University of Michigan. Available on the Internet: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

Štitilis D., 2011. Elektroniniai nusikaltimai [Electronic crime] (mokomasis leidinys). Vilnius: Mykolo Romerio universitetas.

Štitilis D., 2013. Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos [Legal regulation of cyber security: strategies of cyber security], Socialinės technologijos 3(1): 189-207.

The Center for Internet Security, 2015. Critical Security Controls for Effective Cyber Defense.Available on the Internet: https://cybersecurity.idaho.gov/wp-content/uploads/sites/23/2016/10/CSCmaster.pdf

The Government of the Republic of Lithuania resolution No. 716 "On the approval of the description of the guidelines for the determination of the general electronic information security requirements, the description of the guidelines for content of documental content documents and of the state information systems, registers and other information systems classification and electronic information". 2013.

University of Tartu, 2015. E-voting. Available on the Internet: https://courses.cs.ut.ee/2015/infsec/fall/Main/E-voting

Vegas C., Barrat J., 2017. Overview of Current State of E-Voting Worldwide. Real-World Electronic Voting: Design, Analysis and Deployment, p. 51-76, CRC press.

Virbalienė A., 2011. Vidinė organizacijos komunikacija [Inner communication in organization]. Klaipėda: Socialinių mokslų kolegija. Available on the Internet: http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2011_Vidine_organizacijos_komunikacija.pdf

Wohlin C. et al., 2012. Experimentation in Software Engineering, Springer.

Tadas LIMBA is a professor at the Mykolas Romeris University (e-mail: tlimba@mruni.eu). He obtained PhD degree in management from Mykolas Romeris University in 2009. He is the head of Joint Study Programs "Informatics and Digital Contents" with Dongseo University in South Korea taught en English at Mykolas Romeris University. His research interests include over than 15 Years of experience in a field of E-Government, E-Business, IT application for the organizational change and Digital Contents. He is actively developing and expanding the relations for the future prospectives of the common activities with Dongseo University. Tadas Limba has over 30 scientific publications on different topics related with New Public Management, E-Government, E-Signature, E-Time Stamping, E-Business, E-Marketing, IT and Patent Law, Biotechnology Strategies. He is also the international expert in a field of E-Government and has trained the Faculty Members of Public Administration Academy of Republic of Armenia and Eurasian International University in Armenia in 2014. Tadas Limba visited Communication University of China in 2014 and had the research internships at Arizona State University, USA and at Dongseo University, South Korea in 2015.
ORCID ID: orcid.org/0000-0003-2330-8684

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 5 Number 2 (December)
http://doi.org/10.9770/jesi.2017.5.2(15)

Konstantin AGAFONOV is a PhD student at the Mykolas Romeris University (e-mail: ka1979@gmail.com). His PhD topic is related to cyber security management for electronical voting systems. His research interests also include information and data security, data protection and cyber security issues.
ORCID ID: orcid.org/0000-0002-8962-0083

Linas PAUKŠTĖ is an IT Security Consultant at Cognit Consult (e-mail: linas.paukste@gmail.com). His research interests are Offensive Security, Digital Forensics, Cybersecurity Management, Information Security, Network Security, Application Security, Cryptography and Cryptanalysis.
ORCID ID: orcid.org/0000-0003-0807-6125

Martynas DAMKUS is a lecturer at Mykolas Romeris University (e-mail: martynas.damkus@gmail.com). He is the member of Electronic information security (cyber security) Advisory Board of Lithuania. His research interests are related to cyber security and data protection on critical state IT systems, intellectual property, cyber security, online security issues.
ORCID ID: orcid.org/0000-0002-3771-6323

Tomas PLĖTA is a CIS officer at the NATO Energy Security Center of Excellence (e-mail: tomas.pleta@enseccoe.org). His main research interests related to Cybersecurity management of states critical energy infrastructure, also data protection on critical energy IT systems, intellectual property, cyber security, online security issues.
ORCID ID: orcid.org/0000-0002-5376-6873