Review article

Electronic Voting System. History, Problems, and Perspectives

Vytautas Šulus*
Department of IT, Vilnius Business College, Kalvarijų g. 129-401, LT-08221 Vilnius, Lithuania
* Corresponding author, e-mail: *vytautas.sulus@gmail.com*

Received: 15 October 2023
Accepted: 15 December 2023
Online: 30 December 2023

JEL: D72.

Abstract. This paper presents a theoretical analysis of the development and application of electronic elections (e-elections) in the context of cyber security management. Components and tools of e-elections were presented and discussed in the organizational framework. The implementation of e-elections was analysed on the example of Estonia and Switzerland.

Keywords: e-elections; e-voting.
Citation: Vytautas Šulus (2023) Electronic Voting System. History, Problems, and Perspectives. – *Applied Business: Issues & Solutions* 2(2023)10–21 – ISSN 2783-6967.
https://doi.org/10.57005/ab.2023.2.2

Introduction

During regular elections in Lithuania, voting activity has been decreasing every decade. The highest voter turnout in Lithuania was recorded in 1992 (about 75%, the first elections to the Seimas after the Restoration of Independence). After 24 years, in 2016, voter's activity was significantly lower (about 50 %, elections to the LR Seimas) [1]. The main reasons for the decline in voter turnout are the aging of the population, Lithuanian emigration, and changing consumer behaviour. About 2.8 million people live in Lithuania. Future forecasts show that by the 2030s, the working-age population of Lithuania will decrease by a quarter [2]. That is, out of 400 thousand emigrating Lithuanians who have the right to vote in 2016, only 17 thousand registered to vote at elections of LR Seimas. Most immigrants and young people do not vote because there is no way to do it electronically [3].

The main reason for the decline in voter turnout is emigration, so electronic voting would encourage Lithuanian citizens living abroad to participate in the elections as well [4]. The change in consumer behaviour due to competition in the electronic space also has a significant impact on voting activity. Society is increasingly inclined to use modern technologies (online elections, ordering services, paying taxes, electronic banking, etc.), which encourages some competitors and state structures to create a convenient and reliable electronic system that would benefit every user.

Establishment of electronic voting in the country could help solve these problems. In 2006, the Seimas supported the e-voting conception, which formulated the goals and requirements for the imposition of online voting, the electronic voting scheme, and requirements to the legal framework. Electronic voting (e-voting) is based on traditional voting systems that use certain online devices that collect, process and store voting results [5]. The Government of the Lithuania Republic initially planned that the online voting system should be created in the second quarter of 2018, and online voting will be possible for the first time in 2019 municipal elections.

However, due to inadequate system security, several illegal hacking of the system could be possible. Such events may aim to falsify election results. This can lead to public uproar and lead to the questioning of the election results" [6]. Lithuania is the leader in the implementation of FTTH and FTTB in the European Union - more than 21% of households here use fibre-optic Internet [7]. Due to well-developed computer communications, the probability of cyber-attacks is quite high. When implementing electronic voting, it is necessary to be ready to defend against cyber-attacks. For that, it would be necessary to examine the current cyber security systems of Lithuania.

This work is intended to analyse successfully operating Internet election systems in the world, for which there are known sources of threats, possible attack vectors, methods, and methodologies. According to this, it is possible to assess the lack of cyber security in Lithuania, when implementing the electronic election system:
1) to assess the methods of ensuring cyber security, management systems and technologies,
2) to determine the extent to which the legal regulation is undefined, which can lead to cyber incidents,
3) to predict the improvement of management systems and e-voting technologies related to the cyber security.

1. E-voting: Aspects of Cyber Security

1.1 Conception of Cyber Security Management

The internal management processes of modern organizations are not possible without information technologies and information systems and the Internet. The Internet has more and more influence on everyday life, including the global economy [8]. Today, everyday education, basic rights, social interaction, and economy require the smooth operation of information and various technologies. The phenomenal development of cyberspace has brought unprecedented economic growth and new opportunities. Modern research and information security took shape after the emergence of computers and the need to manage information and knowledge in the second half of the 20th century.

However, this is the situation and the emergence of new threats. These trends force countries' governments to take measures and create infrastructure that would ensure further economic development, efficiency, and security [9]. The Cyber Security Strategy of the European Union [10] notes that "deliberate and accidental cyber security incidents are increasing at an alarming rate". These incidents can disrupt the provision of basic services (water, electricity, health care and mobility services). Štitilis [11] observes that "the globalization of electronic space has created unprecedented opportunities to commit crimes from any point in the world, where there is Internet and threats in electronic space are not only for individuals for consumers, but also for remote countries".

The concept of cyber security. In the Cyber Security Law of the Republic of Lithuania [12] cyber security is defined as "a set of legal, information dissemination, organizational and technical measures intended to prevent cyber incidents, to detect, analyse, and react to them, i.e. to manage the information systems in networks ... and restore system after some incidents". In society, the concept of cyber security is often associated with such concepts as electronic information security, information security, network and information security, and information system security.

Network and information security is the ability of networks and information systems to remain with a certain degree of probability free from accidental intrusions or illegal or deliberate actions that would cause damage to stored or transmitted data and related threads. of those networks or systems for the availability, authenticity of the services received, integrity and confidentiality (stored or transmitted data and associated networks). Network and information security ensures a certain level of security, which is used to avoid certain harm. The term does not mean interpretation, analysis, possible response and recovery of activity.

Information security represents the protection of information and system infrastructure from accidental or intentional, natural, or artificial hacking, which can cause damage to the owners of information and system infrastructure. and for users [13]. This concept is only a narrow part of the definition of cyber security, which refers to the protection of information and system infrastructure from possible harm.

The law on cyber security states that cyber security is depending on legal, informational, organizational, and technical tools and services. Jastiuginas [14] defined the conception of information security management in three dimensions.
1. Strategic dimension covers administrative, organizational, government, economic, legal, good tactics aspects.
2. Human factor dimension covers the cultural, ethical, intellectual, educational, psychological, etc. factors affecting safety.
3. Technological dimension includes the aspects of information technologies, technical and software tools, mathematical, cryptographic etc.

Cyber security in the workplace. One of the most important issues when it comes to ensuring cyber security is the question about organization needs: which field must be protected. Countries in European Union (EU) have critical infrastructure that must be protected if events of a cyber incident occur. According to Council Directive [15], two main sectors (energy; transport) and eight subsectors (electricity; oil and gas industry; road, railway, and air transport; inland water transport; sea shipping and seaports) belong to critical infrastructure.

1.2. Essence of Electronic Elections

The penetration of information technologies into various areas of state government is encouraged by the need for transparency, efficiency increase and cost reduction of existing political and administrative processes. "The political and scientific initiatives that have appeared in Europe are examining the implementation of information technologies in electoral processes, health care, tax collection and administration, self-governance, education" [16]. These areas of public education are traditionally criticized for the poor quality of public services, high costs, lack of efficiency, etc.

Current technologies allow automating the execution of tasks in various branches of the industry, where people traditionally play an important role. Electronic voting can be named as one of the representative areas of application of new technologies. The installation of voting systems allowed people to shorten the time of the results announcement, that is, to maximally eliminate the influence of the human factor on the results announcement. Implementation of e-voting and use in various countries showed the high level of requirements which must be placed on the systems to ensure safe, fair, and open elections.

Electronic voting (e-voting) means voting when electronic devices are used in at least one of the polls [17]. Assigned e-voting could be realized in the polling station using devices with touch sensitive screens, standard computers. The results are announced (compressed) after the end of the voting, they can be automatically transferred by network in compressed/encoded form. Each voting data can be recalculated, and the correctness of the voting procedures could be renewed.

Remote e-voting could be realized when voting is done on the Internet, by mobile phone (trial voting only) and at an office, to which a person can go after establishing the agreement of an authorized election commission official or consular office to her. Basic methods of electronic voting [18] are presented below.
1. Voting in the polling station using electronic devices (for example, a computer or a serial voting machine).
2. Unsupervised voting, especially in booths located in public places (trade centres, post offices etc).
3. Internet voting (I-voting) – voting from anywhere using the Internet (computer or phone). I-voting uses information and communication technologies, casting a vote on the Internet.

There is no common definition of the concept of electronic elections in the literature. According to definition of Kiškis et al [16], "Electronic elections are any type of voting that is carried out using electronic devices". Electronic voting can be understood in two ways: elections include the following services: electronic election information, electronic election campaign, electronic election of representatives and electronic referenda [19]. Voting in electronic referenda and electronic elections is the assignment of one's own decision using information technologies.

Electronic elections are defined as any type of voting in which electronic devices are involved in the process. In the context of e-voting, it is important to distinguish the voting using electronic machine and electronic distance voting:
a) for Internet voting, an auxiliary device is necessary which does not determines how voting will be done and allows the voter to vote in a convenient place with an Internet connection;
b) for online voting, an complex system is necessary that includes both Internet voting, voting in the polling station with the help of online voting machines, and online voting in the terminals.

Vaigauskas [20] conducted the voting in an online auxiliary voting system, which can conduct preliminary voting, preserving the traditional voting in the polling station: "everyone can vote in this way who has completed a certain procedure at current time, convinced that he is the voter who has the right to vote. As in case of remote usage of bank service, we sign in using previously declared and documented name and surname, and only after that the system established verified identity" [20].

Paršonis defines this concept differently. In his opinion, electronic voting refers to an ATM, and Internet voting refers to an e-banking. Paršonis claims that electronic voting is a more recent concept that defines the voting model when electronic voting devices are used. This term could be applied on the election day when voting is organized in the polling station using the central voting machines [20].

1.3. Development of Electronic Elections

In 1869 Thomas Edison invented the first electronic voting system and demonstrated this system to the United States Congress. The first proposal for automated voting in Congress was introduced in

1886. Over the next 84 years, more than thirty laws and resolutions were passed to create an automatic, mechanical, and electronic voting systems in Congress. In 1970 a law allowing electronic voting was passed in the USA, and electronic voting was used for the first time in New York in January 23, 1973.

In 1970s, the first system, leading to a computerized electronic voting system, was created by Prof. Murrow Turoffin in New Jersey Institute of Technology (NJIT)[21]. This system named EMISARI (Emergency Management Information System and Reference Index) was developed to organize computer conferences, to discuss topical issues for users and to vote. In 1971 Ohlin [22] described a different system using the terminal connection to the public network. This was supposed to increase people's activism in solving problems related to state governance.

In the middle of the 9th decade of 20th century, many political structures and the public sector more and more often started to organize various projects using Internet network facilities. This was caused by the spread of the global Internet network and improvement of information exchange. Based on these projects, proposals for online elections were presented.

In 1996 Internet voting for the US presidential election was provided [22], where about 2,000 voters voted. In 2000 during the US presidential election, many polling stations refused to use registered ballots. Voting was done in different ways:
a) by manual voting arrows when the respective hand of the selected candidate was turned,
b) by the help of reference cards or electronically, using voting machines.
The first attempt at electronic voting was considered unsuccessful due to the use of different technical equipment. Voting results changed very often, the counting of votes was interrupted. However, experts claimed it happened due to usage of old devices. All recommendations for future (how to improve the processes of voting) were related to replacing the electronic voting with new modern contemporary devices.

In 2002, USA passed the HAVA (Help America Vote Act) [23], which authorized the Election Commission to develop a centralized electronic voter database. The government has decided to allocate budget funds for the purchase of old voting cards and swing voting machines. That is why a commission was created to control the implementation of the election modernization process. in 2006 66 million US voters (38%) had the opportunity to use electronic voting devices. However, 10% of American voters used this option during the elections to the US Congress.

Establishment of electronic voting is actively discussed in other countries as well. In 2002 an initiative group of representatives of the European Parliament submitted a proposal to adopt a resolution on Democracies. The representatives suggested to introduce an online voting system during the elections to the European Parliament in 2004. In their opinion, it could be a promotion of passive voters to express their needs. However, it was decided that such a large-scale project could not be completed in two years. The member states have started to install experimental electronic voting projects in their countries. The United Kingdom had even 150 pilot projects, Switzerland - 8 pilot projects. In 2007 electronic elections were introduced in France, and the introduction of this innovation coincided with a very large number of voters. Several projects related to electronic voting were also implemented in other countries: the Netherlands, Germany, France, UK, Brazil - see Table 1. The pioneer of online elections in the Baltic countries is Estonia, where electronic elections have been in use since 2006.

1.4. Components of Electronic Elections

Stages of voting systems. The Constitution of the Republic of Lithuania and the principles of democracy require ensuring the anonymity and security of voting. The European Security and Cooperation Organization makes such clear demands for democratic elections. The voting equipment used in the election process must ensure a very high level of security due to use the complex set of security protocols.

Basically, any electronic voting system consists of six main elements, which are known as the traditional voting system [24].
1. Voter registration system. The e-voting system provided the voter with authentication data and the possibility to connect to different voting systems. The main task must be the ensuring cyber security: a) for ensuring the transparency of the registration system and b) for protection the system from the unauthorized disclosure of individual information.
2. Authentication. A test intended to verify whether the voter has the right to register and vote. According to the Constitution of the Republic of Lithuania, only persons who have reached the age of majority have the right to vote. Therefore, the register of electronic voter should ensure the legal voting.
3. Voting is the stage when verified voters vote and votes are saved.
4. Management of voting is the stage during which the votes are managed, sorted and prepared for counting.
5. Counting of votes is the stage for decrypting data, counting of votes, and outputting the results.

Table 1. Development of Internet voting: historical facts. Constructed using data of Refs. [22, 23, 24, 25]

Date	Country	Events
1990 - 1999	Belgium	For E-voting, electronic voting machines were used.
1990	Canada	Since then, municipal elections in different cities have been held online using e-voting.
2001	Danmark	Residents of Leeds and Voorburg (Danmark cities) voted online for the new name of the joint city.
2003	UK	An online voting experiment was conducted in the local elections.
2003	Switzerland	In the three cantons, experiment of e-voting was provided.
2004	US	Department of Defence has commissioned a research and development to allow the quality of online voting.
2004 - 2005	Switzerland	Five probing e-voting was held in the cantons of Geneva, Neuchâtel and Zürich (national referenda).
2004 - 2006	Norway	A special commission was instructed to evaluate e-voting opportunities. The two-year commission concluded that e-voting in an uncontrolled region would be possible, but generally it is important to ensure the security aspects.
2005	Estonia	Internet voting was tested and used in local government elections.
2007	Estonia	Internet voting is allowed in the parliamentary elections.
2008	Finland	E-voting was tested in municipal elections.

Table 2. Comparison of the principles of electronic voting

RolNo	Cabello et al [26]	Bogdan et al [27]
1.	Anonymity: it should not be possible to link the ballot to voters	To ensure the anonymity of voting.
2.	Completeness: only those who have a tee can vote to vote.	To eliminate the possibility of vote falsification.
3.	Uniqueness: every legal voter can vote only once.	To ensure the reliability of the software and the save traffic of Internet.
4.	Fairness: every voter should be able to check if your vote has been included	Unique routine of the person identification must be ensured and applied to all voters.
5.	-	To ensure the safety against unauthorized access.
6.	-	To ensure the accuracy of vote counting.
7.	-	The e-voting program must have an intuitive user-friendly interface and must be accessible to people with disabilities.

6. An audit is a test intended to check whether the votes of the voters who voted were included in the final evaluation.

All electronic voting systems have basic minimum requirements that all electronic voting systems must meet. Table 2 represents the main principles formulated by Cabello et al [26] and Bogdan et al [27]. Minimum requirements for e-voting systems were formulated as follows: anonymity, elimination of vote falsification, ensuring the accuracy of vote counting. In e-voting, the provision of personal consent and ensuring the security and reliability of this procedure are of great importance.

Remote authorization available in the following ways:
1) when personal data are confirmed by a qualified electronic signature that meets the established requirements;
2) when personal data are verified by electronic identification devices issued in the European Union, operating under high or low level security electronic identification schemes, which correspond to requirements of Regulation (EU) No. 310/2014 [28];
3) when used electronic devices allow the live video playback in one of the following ways:
3a) during live video translation, the original document confirming the identity or the corresponding permission to obtain in the Republic of Lithuania is recorded and the person identity is confirmed using electronic signature;
3b) during live video translation, capturing the image of the person's face and obtaining the original document confirming the identity or its corresponding permit in the Republic of Lithuania.

1.5. Tools

Use of digital certificate. Identity confirmation or authentication is a method used to verify the source of the transmission or to identify the system participant and to make sure that the transmission has not been modified or hacked during transmission. Personal authentication is a method that allows you to check the authenticity of the subject. In electronic voting, authentication is performed [29] in one of the following routine:
1. Knowledges of subject. The user's account is determined by the password or identification number provided to him.
2. Equipment of subject. Various devices for confirming transactions (magnetic cards, chip cards, generators with a one-time password, etc).
3. Features of subject. Biometric information of a person is available (fingerprints, personal handwriting, retina, etc).

One of the safest ways to do this is to authenticate using a digital certificate. Personal authentication is performed by means of a certification service provider. It is the responsibility of the provider to link the agreement of the person signature with the previous data of signature and verification. Personal digital certificates as the electronic equivalent of a personal contract document are used for this operation. Digital certificate is an electronic equivalent of a driver's license or membership card, which you can use for proving your identity or the right to access the requested information from the Internet [30].

The functionality of digital certificates is based on the coding technology using generated private key and public key. The private key is kept by the owner of the certificate, but public key is distributed to the persons with whom the relations are maintained. The message is encrypted using a private key, decrypted using only the public key which is related to the private key. If the message being sent is encrypted with a public key, it can only be decrypted with the private key. The institution providing the certification service creates and issues a digital certificate by signing with its own private key [30]. The use of the digital certificate provided an opportunity to verify the authenticity of the user's rights to a specific key and in this way to prevent the unauthorized use of the private key.

Use of electronic signature. To connect to various electronic banking systems or use electronic government services, one of the most common authentication methods are the use of an electronic signature:
i) any data that is linked with other data can be annotated to identify the person signature and confirm the data authenticity;
; ii) set of tools (lar related, mathematical, etc.), which together are necessary for electronic signature. It should be noted that a digital record is just a mathematically based sequence of data coding, which, due to its unique characteristics, is used to perform basic functions - authentication and establishing originality.

The requirements for secure electronic signature are related to the requirements of the Civil Code for the security of the authorized text and the identification of the person signature. The following requirements are necessary for secure electronic signature:
a) is clearly related to the signaturing person;
b) allows to identify the signaturing person;
c) it is created by tools/apps that the signaturing person can handle according his own needs only;
d) it is strongly related to signatured data, so any alteration of this data is surveillance.

The use of electronic documents has the same legal force as written documents. The use of such an electronic instrument is carried out by means of the dedicated special tools.
1. USB storage device. When choosing this electronic method of signing, the user must install the software for the USB storage device on his computer, and the use of the cryptographic USB storage device requires a USB connection on the computer.
2. Use of the mobile app. After signing an agreement with the certain company, the mobile service provided by this company allows to use a local SIM card with a secure cryptographic module installed. Therefore, it is possible to obtain a PIN code for the digital use of the certificate, which allows connecting to various online systems and electronically determining the identity of the person signing it.

3. Use of a personal identity card. Since 2009, citizens of Lithuania have been able to use chip-based personal identification cards. Identity cards can be used as a tool for creating electronic signature. The person registry services have created digital certificates that confirm electronic documents created using personal identification cards.

Use of electronic timestamp. A timestamp is a sequence of characters identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second [31]. Timestamp can be defined as the data that are logically related with other data and confirms the existence of those other data until the time specified in the timestamp. The time management service provides the regulations and public availability of the time management service by publishing the regulations on its website. Without having its own website service provider, organiser must ensure the free and public usage of the service. The regulations must specify the entire procedure for the creation and management of the timestamp, the identifier of the timestamp rules, all the necessary information related to the provision of the timestamp formation services.

Timestamp can be used to sign [32]:
a) contract in electronic form, for banks, insurance companies or others;
b) electronic documents to preserve their value as evidence;
c) statements and letters sent electronically to public administration institutions;
d) internal electronic documents to protect them from forgery and backdating;
e) system logs, in order to protect them from forgery;
f) electronic invoice sent to recipients in electronic form;
g) electronic documents stored on a personal computer in order to protect them from forgery and backdating;
h) computer programs to protect them from counterfeiting and viruses.

2. Organization of Electronic Elections

2.1. Principles of Organization

The right to vote belongs to the basic principles of democracy. All principles of democratic elections and referenda must be maintained even after the establishment of the electronic election system. Electronic elections must be so safe and reliable that they are traditional without usage of modern electronic equipment. For the electronic voting system to be attractive to the public and the traditional voting system to be implemented in the future, following essential and undoubtedly important skills must be realized [33].

Publicity and global development. It is possible to ensure that all voters with the right to vote can participate in the elections, and voter identification and registration can be carried out by legal tools. For realization, the most important rules must be implemented as presented in Ref. [34]:
a) every person who has the right to express his opinion can do so;
b) the possibility to participate in elections must be guaranteed by law;
c) voting technologies and equipment must be clearly explained to voters and there must not be any restrictions on dealing with the technologies used in the election process;
d) electronic voting is only a secondary tool in the context of basic voting;
e) the infrastructure used for voting must be accessible to all voters.

The guarantee of freedom of choice. This principle ensures that the voter was not forced to use the electronic voting system, that is, he was not technologically challenged to express his opinion. Essentially, several other aspects must be considered when ensuring this freedom: the voting system must provide the voter with the opportunity to vote with a "blank ballot".

Principles of equality. The equality of the candidates and candidates participating in the elections must be ensured, that is, the equality of the rights of the voters who have the right to vote. The main e-voting requirement could be formulated as follows: paper and electronic ballots must be equivalent. For implementing this principle, it is necessary to ensure the same possibility for political parties to monitor the e-voting system and the e-voting process. According to the advice of some experts, e-voting must be realized earlier than "ballot-elections" (voting using bulletins).

Privacy Policy. Due to this principle: a) e-votes will be hidden all the time until the final counting;
b) no possibility to relate any person who voted and his vote;
c) the phases of registration for voting and voting will be clearly separated;
d) any user will not be able to provide information about his choice by any means related to the voting system.

In the voting system, the possibility of accurate counting and recounting of votes must be ensured, without identifying the person who voted [34].

The principle of directness. This principle determines the behaviour of elections: each vote must be directly recorded and counted. In order to simplify the e-voting systems and to track their operation, most often all votes received during the election period must be stored in encoded form and must be decoded only after the election.

Democracy principle. According to this principle the compliance of the voting systems with the usual traditional voting systems must ensure. There are certain essential requirements that must be met in the e-voting system. These requirements refer to the legality, transparency, security, and accuracy of e-voting systems being developed or created. Users of the e-voting system must understand how the system works, but sometimes it is impossible. Some persons do not have the basic knowledge required to use information technology. In other words, trust in e-voting systems is based on trust in technology and the willingness of the voting person to acquire and use technology.

2.2. Models of Electronic Elections

Two models of electronic elections could be realized: single-phase model, and n-phase model.

Single-phase model. Certain voter who wants to express his choice in the election can do in one simple action. Voting takes place in one cycle. In such model, voter does not need to identify himself when voting. This model is difficult to apply to electronic elections provided remotely, as there is no way to ensure that the user will not vote twice. The model of such e-voting system can only be used for e-voting provided in polling stations, since there it is possible to control who is preparing to vote.

The availability of this system for regular voting is only such that the voter, coming to the polling station, cannot damage the ballot paper and in any case must express his choice. This model can be applied together with the two-phase model, and in the future, it could replace regular voting in polling stations, as it would be better to use electronic ballot boxes than paper ballots [36]. Under the conditions of modern democracy, the one-phase model would simplify and speed up the process of calculating election results, reduce costs. Otherwise, one-phase model would not give voters the oppor-

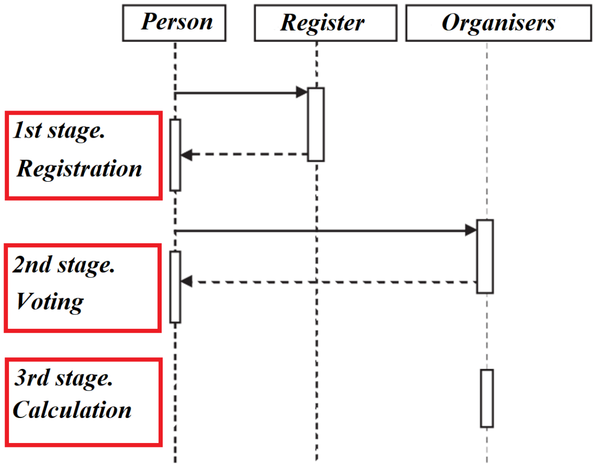

Fig. 1. N-phase model of electronic elections.
Adapted according to Ref. [36].

tunity to vote in requested geographical area, only in the place where they were at that time.

Two-phase and n-phase model. Most electronic voting systems are based on a two-phase model as presented in Fig. 1. In the first phase of e-voting, the voter must identify himself in the e-voting system, which gives him a certain permission to vote. In this way, the voter gets access to the second and main phase of the model - voting.

Sometimes the electronic election system may require additional actions from the voter during the initial (registration) and secondary (primary voting) phases. Using so-called n-phase model, e-voting person receives the messages that require the person to identify himself in separate steps in several identification systems of responsible institutions. In such a situation, the registration phase is divided into several phases and such an electronic voting system is based on the n-phase model.

2.3. Implementation of Electronic Elections

Initially it is important to consider the risk factors. The list of general requirements for electronic information security [37] defines the most important risk factors that can have an impact on electronic information security:
a) inadvertent error, subjective error (errors in electronic information management, erasing of electronic information, incorrect presenting of electronic information, physical power failures of electronic information, failures of electronic information distribution over networks, software errors, incorrect operation, etc.);
b) intentional error (unauthorized use of the information system to hack an electronic information, destruction of electronic information, malfunctions for data distribution over networks, security holes, etc.); c) *force majeure*.

Analysis of the voter's device. One of the most insecure channels of Internet voting is the voter's computer, mobile phone or other mobile devices. Personal computers are poorly monitored and poorly protected against malware attacks. When it comes to remote voting, the computers that are used to record and process votes are outside the control of the institutional supervising the votes. Due to that, the election supervisors cannot do much about it for increasing the voters' attention to these problems [38].

Hackers are constantly scanning millions of computers looking for the easiest to invade. Jefferson et al [39] observes that "computers in Internet cafes and public libraries are still more insecure. Spyware and other programs can be installed in them". When voting at the workplace, voters' risk that wheel. Internet systems and browsers are not protected from malicious programs, which can be downloaded by users or other persons using this computer due to inadvertence. A malicious program installed or downloaded into voter's computer or mobile device without the voter's knowledge can hack the vote cast by the voter or can record the fact of voting. To check information where the e-ballot was fixed, voters could observe the inconsistencies if they had access to a trust computer. This situation is problematic, because allowing voters to confirm their votes could show the realized choice of e-voting.

If the falsification occurs during the sending of the e-ballot, election officials may have no way of distinguishing between the inconsistency of the e-ballot and user error" [38]. Therefore, the possibility cannot be ruled out that the remote voting platform is being used, voters can try to manipulate it: to present more than one vote, having the content of the vote verified, to sell it. That is, trying to exercise their rights to damage the voting system, change the election results, or change the reliability of the election results.

Problems of election security. When analysing the problem of election security, big attention is paid to external threats. This is not correct approach that should be followed, because it is easier for hackers to access the system from the inside. Three main groups of potential internal threats are distinguished [36].
1. Legal users of electronic voting systems. They can search for exploits or security issues in the electronic election system and, having enough technical knowledge and a sufficient list of interested persons provided to them, can use the electronic voting system. These actions are performed most often for financial gain.
2. Persons who may seek to use the privilege of administrators of electronic voting systems to use the functionality of electronic voting systems. Representatives of this group most often seek to use the employees of other organizations that are developing the electronic voting systems. Such employees must have sufficient knowledge and understanding of electronic voting systems. The main motivation of the perpetrators of these threats is financial gain or simply personal satisfaction, self-realization by performing illegal activities. Administrators of electronic voting systems of any level must be morally prepared for such actions by hackers (outside parties) if they are provided with all the information about security "holes". ".
3. Civil servants who have access to electronic voting systems but are not related to the acquisition of electronic voting systems. These persons can participate or lead the internal "attackers" of the electronic voting system. The reasons for which these persons may commit illegal acts are most often financial or simply unspecified personal goals.

The five main groups of potential external threats are presented in Ref. [40].
1. Alone hackers looking for possibilities to disrupt electronic voting systems just to get personal satisfaction by attacking or hacking the state system. In this way, the attack is a protest against government policy. These hackers are most often looking for possibility to access the data, damage it, or use it for personal gain, for example, in many cases, to sell for illegal disclosure.
2. Another group of hackers is different from alone hackers: criminal organizations or individual criminals. These groups, for example, information brokers, may want to have unauthorized access to electronic voting systems to use the resources of these systems for personal purposes.
3. Groups of protesting persons or so-called hacktivists may try to

influence their actions in relation to electronic voting systems with the aim of showing seriousness in using these systems for voting purposes. Main purpose is to damage these systems or to obtain data for personal purposes or damage the information contained in the voting system.

4. Foreign intelligence services may be interested in receiving information about a person. In the future, they could use this information for surveillance. These services could carry out the formation of the country's politics or manipulate the available voting information to influence the voting results.

5. Terrorist organizations may be interested in information about private individuals stored in electronic voting systems. These organizations, using the available knowledge, may be interested in, for example, organizing terrorist acts. They can use electronic voting systems and the information collected during voting to find out what the voting perspectives are. This way allows to influence the voting results and to obstruct the smooth voting process.

3. Implementation of E-voting

Internet voting (I-voting) is one of the types of electronic voting (E-voting). This means that person's voice is reproduced and/or calculated by a computer system. Necessary condition for I-voting must be satified: during online voting, voters cast their votes online using their personal devices. According to Valadkevičius [6], online voting faces two unique and complex challenges.

1. Election results often fundamentally determine the statehood for several years to the year, so this is an extremely important result. Due to this determination, there are always strong interests to destroy this process for the benefit of certain interests. Therefore, when testing election innovations, it is necessary to ensure comprehensive and reliable security systems that protect elections from possible manipulation.

2. Voters' scepticism of election innovations. The main mission of democratic elections is to ensure public trust that the government really represents the nation. It is the hope that the government elections will be conducted fairly, which creates the legitimacy of democratic government. However, innovations in the field of elections often require caution: transparency and explanations are required. Ignorance makes it easy to mistrust.

3.1. Benefits of Internet Voting

1. Voter turnout. Although many critics of Internet voting claim that there is no evidence that Internet voting increases significantly voter turnout, any increasing is evident. If one third of all voter's take part in election voted online, a 2.5-4% increase in election activity can be expected.

2. Validity of voting. I-voting would be extremely useful for Lithuanians abroad, living in the far corners of the world: in many Asian countries, in Latin America. I-voting would ensure that these voters could cast their vote in the elections of Lithuania Republic.

3. Accurate and unbiased counting of votes. When I-voting is implemented, the process of casting and counting votes would be centralized, monitored by competent observers, and pre-agreed rules would be made public. Voting results could be damaged only if outside hackers break into the system.

4. Ensure safe and reliable voting. The applied full verification system means that it is possible to verify and reliably make sure that each vote of any voter was accepted, credited and included according to following routines: i) cast as intended, ii) recorded as cast, iii) counted as recorded. These three steps formed the chain of the "journey" of the I-voice, and after proving the integrity of each chain, the integrity of the entire network is proven.

5. Increased level of vote encryption. I-voting could increase the security, help with voting at home and abroad. By voting online from home, disabled and elderly people will not have the physical contact to carriers of election ballots, and citizens from abroad will be not able to vote repeatedly. So, these threats will be negligible.

3.2. Risks of Internet Voting

It is considered that online security arguments are one of the main ones on which Internet voting is criticized. Below are the risks of online voting and possible ways to resolve them. This information is based on the analyses of the European Council, OSCE/OHIDR, IFES and other international organizations, including the good practices of Norway, Estonia, Switzerland, and Canada [41].

1. Falsification of votes. The I-vote, realized by I-voter, could be damaged or changed without the voter knowing. After counting procedure, election results are different than the voters intended. This risk could be analysed for three stages of online voting: casting, storing and counting. For casting, voter's computer is responsible for data transfer to the server. This risk can be eliminated by using the vote verification function, which allows the voter to make sure, using the remote device, that the vote went to the counting server without being hacked. For storing, vote storage server is responsible. This risk can be eliminated by keeping the cast vote data on several different remote servers, which would be synchronized. For counting, risk of errors can therefore be eliminated by copying data to several servers (mirror service). The second solution is to give the possibility to any voter to download all decrypted election data (without authentication of any voter) from the vote server.

2. Decryption of votes as a technical cut. The main risk of counting votes is that online voting data can be hacked, and voter information recorded in the ballot can be revealed. In legal acts, it is necessary to provide the protocols and standards for clear data transfer, processing and calculation.

3. Revealing the voting secret as a social cut. One of the main social risks associated with online voting is the purchase of votes and the announcement of votes in a certain social network. Therefore, the risk remains that the voter may be pressured or forced to vote after the end of the online voting period.

4. Lack of qualifications of election implementers. It is recommended that online voting projects adopt the standards that have been tested and publicly updated. When preparing the parameters and requirements of the future system for the suppliers and the institutions acquiring the system, it is necessary to be guided by the analyses and reports prepared by the relevant international organizations.

5. Public distrust and quality control. There are two most important factors that lead to public distrust: a) absence and (or) of a high-quality and secure online voting system; b) lack of appropriate information about this system. To solve first problem, several technical and operational security and quality assurance systems are required. To eliminate the second problem, it is necessary to ensure that essential information about the operation of the system is publicly available and accessible to the public. The proposed arrangements fully reveal the system's operating principles and mechanisms: a) detailed audit for system checking in detail, and the conclusion will be present to the public; b) open source software and open protocols allow all programmers to analyse source code and to estimate the security bugs of the system; c) election monitoring

must be organized, observers during the counting of votes would ensure that everything is carried out in the prescribed order.

Summarizing the possible threats, it can be pointed out that online voting is a high-risk project due to two reasons [41].

1. Due to the importance of certain elections for the statehood, there are strong interests to redirect the result for the benefit of individual interested groups.
2. Basic mission of democratic elections is to ensure the public's trust that the government elections were conducted fairly, which creates the legitimacy of democratic government. Innovations in the field of elections can easily cause disappointment among potential voters, so exceptional transparency is often required. When election innovations are implemented, it is necessary to ensure comprehensive and reliable security tools that protect against possible manipulation of elections and distortion of results. Only such tools can ensure high standard of transparency and publicity.

Proponents of online voting therefore hope to increase voter turnout, while critics fear that due to the current cyber security situation, the online voting system may be an easy target for attacks. Finally, online voting system may be aimed at to change election results. Additional problems about ensuring of anonymity are not yet solved.

4. Systems of Electronic Election

Various electronic voting systems have been developed and tested in many European countries. Outside of Europe, the USA and Brazil are currently engaged in electronic voting, while Mexico and Central and Latin American countries are considering it. According to the setting of clear goals of electronic voting, the countries of the world can be divided into three groups.

1. Israel, together with Scandinavian countries. These countries rely on the traditional elections using paper ballot. There are no political plans that include electronic voting.
2. Countries that have introduced or are introducing electronic voting machines, which do not have any plans to introduce remote electronic voting throughout the country (for example, the USA, Brazil, Russia). 3. Sweden, Canada, France, and Estonia. These countries are planning to introduce or have already introduced remote electronic voting throughout the country.

One of the first large-scale electronic voting systems was implemented in USA. Secure Electronic Registration and Voting System (SERVE), acquired by the US Department of Homeland Security department was planned to be used in 2004 for US voters abroad. However, Pentagon refused to use this system due to serious security threats. The security analysis [50] done by independent researchers has caused a lot of discussion, and conclusions state that since the risk of large-scale and successful attacks of hackers is so high, it is recommended to stop the development of SERVE. Moreover, similar systems should not be attempted in the future until the infrastructure of the Internet and personal computers has been fundamentally redesigned and improved, or until a fundamental security arrangement has been implemented.

4.1. Electronic Elections in Estonia

Many countries use electronic voting machines at polling stations, but Estonia did not choose this way. Electronic voting in the context of Estonia means remote voting over the Internet. The most important goal is to provide voters with the opportunity to vote and thereby increasing voter participation.

Internet voting system. Until now, Estonia is the only country that has introduced online voting in elections on a national scale. Internet voting was used in Estonia in the municipal elections (July 2005) and in parliamentary elections (2007). In January 2005 electronic voting system was tested In Tallinn, during public testing before the municipal elections. Also, local referendum about the location of the Freedom Monument was conducted using this system. In 2002 political agreement on the implementing of electronic voting in Estonia was concluded.

Legal framework of e-voting was started in 2002 after adoption of the Local Government Election Law, which allows voters to vote online on the website of the Central Election Commission during early voting.

In 2005, after the main election commission approved the online voting system, the law on the registration of the municipal election law was adopted, which formulates the voter's right to adjust his e-vote: a) by voting again on the Internet or b) at the polling station on the day of the election. This law is related to realization of the voting freedom.

The law was vetoed by the President Arnold Rüütel, arguing that the law created non-equivalent conditions for electronic and traditional voters, since online voters are allowed to change their votes, others do not have such an opportunity. After Parliament rejected the president's veto, he appealed to the Supreme Court regarding the constitutionality of the law. The Supreme Court rejected the resident's complaint, explaining that the law does not violate the Constitution and does not violate the equal rights of voters, as all voters have the right to vote online. The laws were finally approved only in September 2005. In 2005 9,317 voters voted online in the municipal elections in Estonia. It was 0.9% of registered voters or 2% of voters who participated in the elections.

During the election, there were no serious technical problems, apart from the fact that on the third day of voting, the electronic voting was disrupted for one hour due to the problems of certification service provided by *Sertifitseerimiskeskus AS*. No attacks that could cause system security problems were recorded. The auditors confirmed that the electronic voting system worked correctly, there were no malfunctions or problems that could raise suspicions about the correctness of voting and the trustworthiness of the system. In April 2007 30,275 voters voted online in the parliamentary elections [19].

Identification of voters. Online voting in Estonia is growing using an electronic identification (ID) card. In February 2006 the number of ID card holders was 65%, July 2007. - about 80% of adult recipients [43]. Electronic identification card is valid for all Estonian recipients since January 1, 2002. It is used for remote personal identification and electronic signature. Although there are currently 1 million electronic ID cards only 70,000 users are active users. This explains the relatively small number of people who voted online. In addition, those who wanted to vote on the Internet must be equipped by computer with Internet access, an ID card with a certified certificate and PIN code, a card reader and serial software.

Fig. 2 represents online voting system in Estonia [44] which is based on the "two-envelope" system, currently with a ballot. The voter's vote is encoded when sending it to the voting server. Encoded vote can be kept in an anonymous inner envelope, as an analogy with written voting. Therefore, the voter signs in with an electronic signature. This means that person identification data is presented in the inner envelope. Then, before the counting the votes, the encoded vote and the digital record with personal data are separated. Electronic votes are then decoded and counted.

Internet voting in Estonia has been recognized as successful. The

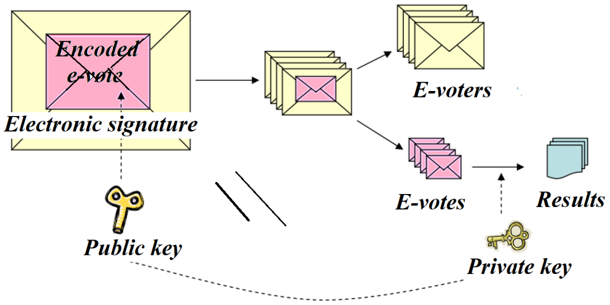

Fig. 2. Online voting system in Estonia.
Adapted according to Ref. [44].

OSCE/ODIHR report [45] states that the administration of the elections was transparent. It was stated that the Central Election Commission of Estonia tried to minimize the risk and ensure safety. However, the report notes that the scope of testing and auditing could have been greater. There is a discussion about possible problems when the number of online voters increases. The report contains recommendations on how to increase the security and reliability of online voting. The conclusions of the report state that "as long as the problematic aspects of online voting will not be effectively resolved, the government should seriously reconsider this question: should online voting be considered as a voting method, or should it be used to a limited extent or not at all? Or may be refused?".

If such an election scheme would be transferred to Lithuania it would be an important and positive arrangement. Usage of the online election system in Lithuania will automatically avoid threats related to fears about the secrecy of voting. Several opposite opinions exist: voters who do not use the online election system will be disadvantaged. When a situation arises, voters will obtain different rights: those who vote online will be able to change their choice, while those who only vote at the polling station will no longer be able to do so. This could be considered a weighty argument for politicians. However, let's not forget that "online elections will be relevant for each voter and only the choice of each voter, whether to use technology or not, determines this emergence of advantage [21].

Principles of voting on the Internet. In Estonia, Riigikogu election law intended for definition of online voting [46]. One of the main features of online voting is that the voter votes himself, and in the cases provided by law, the voter can change his vote.

Time interval. Voting can be done online for 7 days - from the 10th to the 4th until the election day. The possibility to correct the voice on the Internet is realized for all e-voters. During the online voting period, the voter can change his vote online - in this case, the last online vote is counted.

The supremacy of ballot voting. What is happens if the person previously voted online during the early voting period and then decided to go to the polling station and votes again using the regional ballot paper? According to e-voting rules, the vote cast online is invalid. Therefore, a voter can no longer correct (change) his vote online or using a paper ballot. On election day, votes cannot be changed online.

Similarities between online voting and traditional voting. I-voting is based on the provisions of election laws and basic election rules. Thus, voting is uniform and secret, only voters can vote, each person can cast only one vote. It must be impossible to check how the voter voted. Voting is safe, reliable, and proof. Voters should be able to cast their vote freely and without external pressure or influence.

Invitation to vote online for gifts to voters or other influence is prohibited. Also, collective online voting events are prohibited (Internet voting services, information centres, etc.). Such activities can be considered a violation of electoral freedom. The voter votes independently on the Internet. The use of mobile phone card belonging to another person for voting and corresponding transfer of card passwords (PIN codes) to another person are prohibited. To avoid security risks, only a known computer is used - either owned by the voter or a person whom the voter trusts.

4.2. Electronic Elections in Switzerland

Development of Internet voting. In 2000, Swiss federal government has decided to adopt an Internet voting project, which it supported with the argument that after adopting electronic voting, Switzerland could play the role of a leader and to demonstrate to other countries that the science of information technologies can serve in the implementation of the elements of direct democracy [57].

The main reasons for the adoption of online voting systems in Switzerland were related to the increase in the success of elections due to the significantly increasing number of elections and referenda, decreasing voter turnout, successful voting through the postal service and the positive influence of this voting method on voter turnout. The implementation of online voting was also determined by such factors as the high level of Internet penetration. 10% of Swiss citizens are abroad, and only 2% of them register to vote. In addition, the low level of voter turnout for people younger than 40 was recorded. Generally, public opinion data showed a high level of idea popularity to vote using Internet [47].

In 2000, Swiss Confederation has developed a centralized government structure that allowed it to maintain control over the Internet voting project. Federal government signed an agreement with three cantons (Geneva, Zurich and Neuchâtel), which voluntarily decided to acquire the Internet voting project. The federal government agreed to finance 80% of project costs until 2005, and the cantons agreed to slow down the Internet voting system and make it available free of charge to any of the remaining 23 cantons. Thus, the Swiss confederation would retain the right to control the project for an indefinite period.

In October 2011, 22 thousand Swiss expatriates had the opportunity to vote online in the recent federal elections. After this elections Swiss Confederation decided to grant the right to vote online to all voters living abroad. Priority and opportunity to vote online was guaranteed for voters from abroad are given [48].

Other arguments for the legalization of Internet voting are related to the improvement of vote counting systems, the immediate inspection of damaged ballots, and the acceptability of such a voting method to some voters.

The right to vote online. Since February 2014 all Swiss citizens living abroad have the right to vote online. The only requirement is to register for voting in those cantons that provides online voting. Such a right is guaranteed to voters from states belonging to the European Union and countries that have signed the Wassenaar Agreement. States ratifying the Wassenaar Agreement agree not to punish individuals for the use and use of both (civilian and military) devices and technologies. Cryptographic programs partly fall into the category of these two distinct tools and technologies. Thus, the Swiss government wants to protect its citizens from possible legal responsibility for the use of such programs in countries that have not signed the Wassenaar Agreement, thus limiting the possibility of on the Internet. The federal law allows foreign voters to vote in federal elections and referenda. The canton of Geneva granted such voters role rights in the cantonal legislature. For foreign voters to be included in the voter lists, they must register their place of residence at the Swiss consular office and renew this registration every four years [48].

Some voters living in Switzerland also can vote online in the cantons of Geneva and Neuchâtel. Other cantons implementing pilot projects for online voting are targeting voters from abroad. The long-term goal is to provide the possibility of online voting to all Swiss voters in the future. The Swiss Confederation (federal government) has set limits for each canton using Internet voting - no more than 30%. Voters in every canton that uses Internet voting can vote online. To avoid the above-mentioned arbitrariness, the government of the canton of Geneva has selected 15 municipalities, in which there is about a third of the voters of the entire canton. In these municipalities, all citizens can vote online without prior registration. Swiss voters abroad are not included in the 30% of voters. In addition, 30% of voter's registration does not apply to cantonal and self-governing elections or referenda. In 2020, 13 cantons offer online voting to voters: the cantons of Geneva, Neuchâtel and Zurich use their own online voting systems, and the remaining 10 cantons use one of the following the online voting system of these three cantons [48].

Internet voting system. After completing the so-called electronic ballot box removal procedure, the Geneva canton's online voting site is now open to the public. Then, the voter uses the Internet browser to connect to the Internet site [49] and edit the voting procedure. To activate the voting procedure, the voter enters his voting card number from identification field on the website and consults with the current legal information (prominent response for electoral laws, etc). In the next step, the voter fills in the electronic ballot, verifies the choices made in the ballot and enters secret data (password, date of birth and municipality of origin) in the authentication form. After completing these actions, the voter will be redirected to the confirmation page, which provides confirmation information about the successful saving of the cast vote in the electronic ballot box [48].

A single use voting card, necessary for every online vote, is sent to the voter by post. The voting card contains a unique voting card number that identifies the voter in the election system, regardless of the way he votes. The voting card number is used to identify the user to confirm his connection to the voting network. Voting card number represents the confidential information, and all transfers in any form must be provided in encrypted format [48].

Online voting ends at noon on Saturday, i.e. u. one day before the election day when voting starts at the polling station. The possibility of revoting via the Internet voting system of Geneva does not provide for the possibility of revoting via the Internet and other ways (in writing or on election day at the polling station). In the Geneva electoral system, there is unique list of voters for all three voting methods (online, through post-office and in the polling station), and due to that, no possibility to vote more than once.

In I-voting, voters are required to enter their municipality of origin and date of birth. These data are not available in public registers. The identity of origin is also indicated on the identity card and passport of a Swiss citizen. Also, the election organizing service (Service des votations et elections, SVE) organizes a telephone survey for 4000-8000 of voters who voted to make sure that the voters voted freely [48]. In case of voters activity 50%, the volume of respondents is 4-8%) .

In summary, the Internet voting system in Switzerland due to the voter identification mechanism would not be suitable for the case of Lithuania, as it would facilitate the possibility of reducing the speed of voting and voting for other persons. It would only be enough to know the date of birth of other voters, the municipality of origin and verify the voter card of another person. In addition, in Switzerland, there is no possibility to re-vote either online or in a traditional way.

Conclusions

The theoretical analysis of the development and application of cyber security management tools for electronic elections showed following statements.

1. Electronic elections shall be defined as any type of voting in which electronic means are involved. In the context of e-voting, it is important to distinguish between voting using electronic machines and electronic remote voting: Internet voting and electronic voting.
2. Any electronic voting system consists of six basic elements, which are known as traditional voting systems: voter registration, authentication, voting, vote control, calculation of events, audit.
3. For electronic voting systems to be attractive, they must acquire the following essential and undoubtedly important characteristics: universality and universal participation, freedom of choice, love, secrecy, immediacy, democracy. Models of electronic elections can be: one-phase model, two-phase and n-phase model.
4. Main causes of potential internal threats represent users of e-voting systems: legal users as e-voters, administrators of e-voting systems, civil servants who have access to e-voting systems.
5. The following groups of potential external threats are distinguished: individual hackers, criminal organizations, groups of protesting persons, foreign intelligence services, terrorist organizations.

Case analysis of the application of cyber security management tools and technologies in electronic elections showed following outcomes. Due to the best benefits of electronic voting, three different groups of countries can be distinguished:

a) main group of countries rely on the traditional "ballot" voting system, without any politicians considering electronic voting;

b) countries which has introduced electronic voting machines, but they do not have any plans to introduce remote electronic voting throughout the country;

c) Sweden, Canada, France, and Estonia have already introduced remote electronic voting throughout the country.

Lithuania has good opportunities to support Internet election research from other countries, to carry out continuous public education, to apply the latest security measures. There is a not negligible but slight threat, that public distrust of the state and its institutions may increase in case of cyber attack disrupts electronic voting system and damages the choices of voters.

Abbreviations

ATM	-	Automated Teller Machine
EMISARI	-	Emergency Management Information System
	-	and Reference Index
HAVA	-	Help America Vote Act
IFES	-	International Foundation for Electoral Systems
NJIT	-	New Jersey Institute of Technology
OSCE	-	Organization for Security and Co-operation in Europe
OHIDR	-	Office for Democratic Institutions and Human Rights
SERVE	-	Secure Electronic Registration and Voting System
SVE	-	Service des Votations et Elections

References

1. 2016 m. spalio 9 d. Lietuvos Respublikos Seimo rinkimai (in lith.) - https://www.vrk.lt/2016-seimo.
2. Galdikienė, L. () Kai pučia vėjas, reikia statyti malūnus (in lith.) - https://www.lb.lt/lt/naujienos/l-galdikiene-kai-pucia-vejas-reikia-statyti-malunus
3. Radžiūnas, V. () Kodėl pusė Lietuvos rinkėjų nenori dalyvauti rinkimuose? - https://m.klaipeda.diena.lt/naujienos/lietuva/politika/ kodel-puse-lietuvos-rinkeju-nenori-dalyvauti-rinkimuose-671568
4. Discusion: online voting is a long process that can start with voters abroad - https://www.delfi.lt/en/world-lithuanians/ discusion-online-voting-is-a-long-process-that-can-start-with-voters-abroad-84663155.
5. Agafonov, K. (2016) Apie elektroninį balsavimą paprastai (in lith.) - http://apzvalga.eu/apie-elektronini-balsavima-paprastai.html.
6. Valatkevičius, S. (2015) https://old.kurklt.lt/wp-content/uploads/2015/10/Balsavimo-internetu- %C4%AFgyvendinimo-ir-elektronini%C5%B3-apylinki%C5%B3-projektas.pdf
7. Kosowska, E. (2011) Frost & Sullivan, + https://www.newswiretoday.com/news/91994.
8. Štitilis, D. (2013) Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos (in lith.)- *Socialinės technologijos* 3(2013)189-207.
9. Information Technology Industry Council (ITI) - https://www.itic.org/about/.
10. EU Cybersecurity Strategy - https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
11. Warren, M.; Štitilis, D.; Laurinaitis, M. (2023) Cyber Lessons that the World Can Learn from Lithuania - In: European Conference on Cyber Warfare and Security (2023) 517-524
12. Lietuvos Respublikos kibernetinio saugumo įstatymas - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee.
13. Kiškis, M.; Petrauskas, R.; Rotomskis, I.; Štitilis, D. (2006) Teisės informatika ir informatikos teisė (in lith.) Textbook. - ISBN 9955-19-048-5 - Vilnius, Mykolo Romerio universitetas.
14. Jastiuginas, S. (2011) Informacijos saugumo valdymas Lietuvos viešajame sektoriuje (in lith.)- *Information & Media* 57(2011) 7-25 - https://doi.org/10.15388/Im.2011.0.3137
15. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection - https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114
16. Kiškis, M.; Kraujalytė, A. (2005) Informacinių technologijų įtaka teisiniams-politiniams procesams e-valdžios kontekste (in lith.) - *INVENT* (2005) 771-778.
17. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Council of Europe, Committe of Ministers. - https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/ Recommendations/00Rec(2004)11_rec_adopted_en.asp.
18. Enguehard, C.; Graton, J. (2008) Electronic Voting: the Devil is in the Details - https://hal.science/hal-00274635.
19. Ramonaitė, A.; Barcevičius, E.; Jurgelevičiūtė, D.; Medelis, Z.; Juozapavičius, M.; Jokubaitis, A.; Lipskis, D.; Kirvelytė, L. (2008) Elektroninio balsavimo galimybių studija - http://www.lnes.tspmi.vu.lt/wp-content/uploads/2021/12/Elektroninio-balsavimo-galimybiu-studija-6.pdf.
20. Janonis, T. (2012) Kuo skiriasi el. balsavimas nuo balsavimo internetu? - https://www.delfi.lt/archive/kuo-skiriasi-el-balsavimas-nuo-balsavimo-internetu.d?id=59528505.
21. Renner, R.L., Bechtold, R.M., Clark, C.W., Marbray, D.O., Wynn, R.L., Goldstein, N.H. (1974) EMISARI: A Management Information System Designed to Aid and Involve People. - In: Tou, J.T. (eds) Information Systems. - Springer, Boston, MA. - https://doi.org/10.1007/978-1-4684-2694-6_13
22. Rupp, C. (2004) E-Democracy in E-Austria - - https://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-2.pdf.
23. HAVA, Help America Vote Act, US Election Assistance Commision (2017) - https://www.eac.gov/about/help_america_vote_act.aspx.
24. Visvalingam, K.; Chandrasekaran, R. (2021) Secured Electronic Voting Protocol Using Biometric Authentication - *Advances in Internet of Things* 1 (2021) 38-50 - doi: 10.4236/ait.2011.12006.
25. Electronic voting in Switzerland - https://en.wikipedia.org/wiki/Electronic_voting_in_Switzerland.
26. Cabello Pardos, A.B.; Hernández Encinas, A.; Hoya White, S.; Martín del Rey, A.; Rodríguez Sánchez, G.(2007) A Simple Protocol for Yes-No Electronic Voting - *IJCSNS International Journal of Computer Science and Network Security* 7(2007)72-76.
27. Bogdan, J.; Veselaja, O. (2011) Analiz sushchestvujushchich sistem golosovanija (in rus.) - *Eastern-European Journal of Enterprise Technologies* 1 (2011)33-49.
28. Commission Implementing Regulation (EU) No 310/2014 - https://www.legislation.gov.uk/eur/2014/310/adopted.
29. Nathanael, P.; Tanenbaum, A. S. (2009) The Design of a Trustworthy Voting System - In: ACSAC '09: Proceedings of the 2009 Annual Computer Security Applications Conference - (2009) 507-517. - https://doi.org/10.1109/ACSAC.2009.54.
30. http://www.ssc.lt
31. Song, S.; Huang, R.; Cao, Y.; Wang, J. (2021) Cleaning timestamps with temporal constraints - *The VLDB Journal* 30 (2021)425-446 - doi:10.1007/s00778-020-00641-6
32. Limba, T.; Novikovienė, L. (2012) Elektroninio parašo ir laiko žymos įtaka elektroninių sutarčių apsaugai - *Socialinės technologijos* 2(2012)483-501.
33. Limba, T.; Agafonov, K. (2012) Models and Principles of Designing e-Voting Systems, Ensuring its Protection - *Socialines Technologijos* 2(2012).
34. Gritzalis, D. A. (2002) Principles and requirements for a secure e-voting system - *Computers & Security* 21(2002)539-556 - https://doi.org/10.1016/S0167-4048(02)01014-3.
35. International Working Group on Data Protection in Technology (IWGDPT) - https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Europa-Internationales/Berlin-Group.html.
36. Rössler, T. (2009) Electronic Voting Using Identity Domain Separation and Hardware Security Modules. - In: Godart, C., Gronau, N., Sharma, S., Canals, G. (eds) - Software Services for e-Business and e-Society. I3E - *IFIP Advances in Information and Communication Technology* 305(2009) - Springer, Berlin, Heidelberg. - https://doi.org/10.1007/978-3-642-04280-5_1.
37. Minimum Information Security Requirements for Systems, Applications, and Data - https://safecomputing.umich.edu/information-security-requirements.
38. Recommendations Report to the Legislative Assembly of British Columbia (2014) Independent Panel on Internet Voting - https://elections.bc.ca/docs/recommendations-report.pdf.
39. Jefferson, D.; Rubin, A.; Simons, B.; Wagner, D. (2004) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) - https://www.acm.org/binaries/content/assets/public-policy/usacm/e-voting/reports-and-white-papers/serve_report_full_paper.pdf.
40. Štitilis, D.; Klišauskas, V. (2015) Aspects of cybersecurity: the case of legal regulation in Lithuania - *Journal of Security and Sustainability issues* 5(2015)47-59

41. Rubikas, I.; Valatkevičius, S. (2015) Balsavimas Internetu. Geriausios užsienio praktikos ir taikymo Lietuvoje galimybės (in lith.) - Vilnius, 2015.
42. Donauskaitė, D. (2008) Balsavimo internetu klystkeliai (in lith.) - https://www.delfi.lt/news/ringas/lit/ddonauskaite-balsavimo-internetu-klystkeliai-17525311.
43. ID - https://www.id.ee/en/rubriik/e-estonia/
44. Maaten, E. (2004) Towards remote e-voting: Estonian case - In: Proceedings of Conference: Electronic Voting in Europe - Technology, Law, Politics and Society, - Workshop of the ESF TED Programme together with GI and OCG - Schloß Hofen / Bregenz, Lake of Constance, Austria
45. Alternative voting methods and arrangements - OSCE/ODIHR report. https://www.osce.org/files/f/documents/2/a/466794.pdf.
46. Elections of the Riigikogu - https://www.riigikogu.ee/en/introduction-and-history /riigikogu-tasks-organisation-work/elections-riigikogu/.
47. Barrat i Esteve, J.; Goldsmith, B.; Turner, J. (2012) International Experience with E-voting. Norwegian E-vote Project - https://www.parliament.uk/globalassets/documents/speaker/digital-democracy/IFESIVreport.pdf
48. Juknevičiūtė, D.; Skačkauskas, M. (2015) Balsavimas internetu: užsienio valstybių patirtis ir perspektyvos Lietuvoje - https://www.vrk.lt/documents/10180/556540/Balsification+internet.pdf /a5247fe6-d96e-437d-8135-5db76da1f66f.
49. https://www.evote-ch.ch/ge