Threats of the Implementation of E-Voting and Methods of Their Neutralization

Oleksandr Markovets and Mykola Buchyn

Lviv Polytechnic National University, Bandery Str. 12, 79013 Lviv, Ukraine

Abstract

The article analyzes the main potential threats that arise when using electronic voting, as well as possible ways to neutralize them. The authors reveal the concepts and basic systems of e-voting. Potential advantages and disadvantages of electronic expression of will are also analyzed. Considerable attention is paid to the potential threats of e-voting, which are differentiated by authors into 4 main groups, and ways to neutralize existing threats. Researchers offer their own formula for determining the level of threats when using e-voting, and therefore, depending on the results obtained on the basis of expert assessments, the expediency or inexpediency of implementing this type of will expression.

Keywords 1

Elections, e-voting, threats to e-voting, democracy, information security

1. Introduction

In the era of information society development information and communication technologies penetrate not only into the sphere of science and production, but become an integral part of all aspects of life of any modern society. The field of politics is no exception, where the results of scientific and technological progress have promoted to increase the level of involvement of individuals and social groups in political life, made it possible to transfer a significant part of political processes and public services into electronic form. Such phenomena as e-democracy, e-government, e-diplomacy etc., are becoming more and more relevant and attributive features of modern society.

One of the largest political processes, the election process, is no exception. Researchers, politicians and journalists have been talking for a long time about such phenomena as electronic elections and e-voting. Moreover, a number of countries around the world have begun the practical implementation of these phenomena, or are at the stage of planning and partial implementation of e-voting. However, the problem is that the rather euphoric attitude of most scholars and politicians to the implementation of e-voting leads to the fact that a whole range of problems and threats are ignored, without taking into account and solving which the implementation of e-voting can harm the democratic development of society and significantly reduce democratic potential of the election institute. Therefore, the study of threats of e-voting and finding out possible ways to neutralize them is considered as relevant and important.

2. Related Works

Considering that at the present stage, there is an intensive development of the information society and information and communication technologies, it is natural that this trend permeates all spheres of social life, including the sphere of politics. Therefore, it is logical that domestic and foreign researchers

SCIA-2022: 1st International Workshop on Social Communication and Information Activity in Digital Humanities, October 20, 2022, Lviv, Ukraine

EMAIL: oleksandr.v.markovets@lpnu.ua (O. Markovets); mykola.a.buchyn@lpnu.ua (M. Buchyn)
ORCID: 0000-0001-8737-5929 (O. Markovets); 0000-0001-9087-5123 (M. Buchyn)

pay close attention to the issue of electronic voting and ensure its security. At the same time, such studies are usually interdisciplinary because they require integrating scientific knowledge and theories from various social, humanities, and technical sciences.

Analyzing the state of scientific research on the security and threats of electronic voting, it is worth noting that in foreign science, much attention is paid to this topic, primarily by Latin American researchers. In particular, they try to determine the threats and risks inherent in electronic voting systems during the elections in Brazil, Ecuador, and Colombia, using the example of specific Latin American countries. Using a deductive method and analyzing the last three presidential election campaigns in the mentioned states, the researchers conclude that it is necessary to identify the electronic voting system's weaknesses to mitigate the potential risks to information security during elections. To do this, the authors suggest considering the culture, technological availability, and social conditions of each studied country [1].

It is also worth noting that similar studies were devoted to security problems during electronic voting in an individual Latin American country—for example, a study of security and threats in Brazil's electronic voting system [2]. Alternatively, about analyzing cyber security models suitable for use during the elections in Ecuador [3]. In the first case, the authors analyze the Brazilian electronic voting system through the prism of advantages (quick counting of votes and availability of results) and disadvantages (potential system failures and falsifications). Researchers emphasize that despite several security mechanisms, the Brazilian electronic voting system faces threats that could compromise the outcome of the vote [2]. In the second case, researchers analyze various cyber security mechanisms to protect information during elections and propose a cyber-security model that strengthens the information security of the electoral process [3].

It should also be mentioned research on the problem of electronic voting during the elections in Indonesia. In particular, researchers analyze this country's opportunities and problems associated with electronic voting. They highlight some disadvantages when implementing e-voting in Indonesia and the potential benefits that e-voting can bring to the country [4], [5].

Since one of the main problems during the implementation and use of electronic voting is the problem of information security, many studies are devoted to security issues and problems of cyber protection during electronic voting. Researchers, in particular, often emphasize that electronic voting has the potential to be the fastest, cheapest, and most efficient way to administer elections and count votes. At the same time, according to researchers, electronic voting is characterized by several security threats that can compromise electronic voting. Therefore, they require close attention and the use of means to minimize existing threats [6].

Researchers are also analyzing the security problem of electronic voting in intelligent communities. In particular, researchers using the example of elections in higher education institutions (which, in their opinion, are the most representative intellectual communities) analyze and propose their own secure electronic voting system that guarantees secrecy, integrity, and authenticity of votes [7].

Considerable attention of researchers studying electronic voting and ensuring its security is paid to the problem of cryptographic protection of electronic voting, in particular, with the help of blockchain technology. Researchers emphasize that in the conditions of the spread of the coronavirus pandemic, the relevance of electronic voting is increasing significantly. However, at the same time, the problems of security and transparency of electronic will-detection cause significant concern. The researchers believe that the blockchain technology proposed by them will make it possible to eliminate all the existing shortcomings and threats of electronic voting, ensuring at the same time the transparency of elections and the secrecy of voting: on the one hand, the result of will detection will be stored in a protected chain of blocks; on the other hand, all other information will be public and available to everyone, which will make the election process public and transparent [8].

Researchers also analyze information security during electronic voting through the prism of threats and mechanisms for neutralization. In particular, researchers pay considerable attention to international security standards during electronic voting and highlight the main security threats and ways to overcome them. Considerable attention is paid to the use of blockchain technology during electronic voting, which the authors consider an effective means of ensuring information security and secrecy of voting [9].

Some scholars propose to replace the traditional client-service architecture, which is usually used for e-voting and causes some difficult moments, with an e-voting system that involves protecting

information security with the help of distributed storage and blockchain technology. The proposed system includes a private blockchain network, a smart contract, and a web service. According to the authors, such a system can guarantee the integrity of voting results, secrecy, the possibility of verifying transactions, and the maximum endurance of the system about the load [10].

Researchers also pay attention to specific procedural points related to ensuring the security of electronic voting. In particular, it is about the electronic voting system, which uses voter identification mechanisms such as voter ID cards and fingerprints. According to the authors, such a double system of protection should protect the result of the expression of will and promote voters' trust in electronic voting [11].

Some researchers consider another option for ensuring the reliability of electronic voting to be the use of an advanced electronic voting protocol based on public key cryptography. This method involves encryption with a public key based on two pairs of certificates: one for citizens, the other for a particular independent structure (for example, it can be the National Center for Information Technologies), which will act as a trusted certification center for citizens and the government. Each of the two certificate pairs contains pairs of private (public) keys. According to the authors, such a protocol, on the one hand, makes it possible to vote from anywhere and, on the other hand, to comply with security laws, including identification, authentication, integrity, and anonymity [12].

Researchers also point to specific dilemmas inherent in electronic voting and the need to resolve them. For example, such a dilemma can be a choice between a system that allows verification of voting results (for example, it can be paper protocols of electronic voting results) and problems of security and anonymity of voting, which the mentioned protocols can violate [13].

Some scientific publications are devoted to analyzing specific already existing electronic voting systems. In particular, the Helios Voting electronic system, which the authors evaluate for compliance with the technical and security requirements recommended by the Council of Europe in 2017. The authors emphasize that their ultimate goal is conceptual and practical support for the gradual, secure, and protocol expansion of electronic voting [14]. Similar studies concern the electronic voting system Nvotes [15].

Some studies consider the problem of information security and protection of personal data in general, in particular - in mobile applications and social networks [16], [17] and identification of manipulative content [18]. Although such scientific intelligence is not directly related to electronic voting, it makes it possible to understand all the threats that can await us during the introduction of electronic voting.

In the context of our research, publications that analyze a broader topic - e-governance - are also important. In particular, researchers consider the problem of trust in e-government services and the introduction of mechanisms to solve this problem [19].

Summing up, we see that the problem of electronic voting, reliability and security has become the subject of scientific research by many Ukrainian and foreign researchers. At the same time, there are still no comprehensive and systematic studies that would involve a thorough analysis and identification of all existing threats to electronic voting, as well as their assessment with the aim of neutralizing existing threats and determining the expediency or impracticality of implementing electronic voting. Therefore, our research topic is relevant and requires a more comprehensive study.

3. Results and Discussion

3.1. Concepts and systems of e-voting

In our opinion, e-voting should be understood as the procedure of voting in elections, during which electronic information systems are used. Such systems can be used both during the act of expression of will and during the determination of voting results, or in two stages simultaneously. In the context of the above, it becomes obvious that e-voting may have its own realization options. So, we can talk about different models (systems) of e-voting.

Researchers single out the following main models of e-voting:

1. Remote e-voting. This type of e-voting provides for the possibility of carrying out an act of expression of will without the presence of a voter at the polling station. These include, first of all, Internet voting, less often – SMS voting. To date, the only country that has implemented remote Internet voting on a full-scale nationwide level is Estonia.

2. Polling place e-voting. This type of voting requires the presence of a person at the polling station during the act of expression of will. Polling place e-voting can be of 2 types:

- complete, in which electronic systems are used both during the expression of will and during the counting of votes (voting using electronic machines). This type of electronic voting is characteristic, for example, of the USA or Brazil;
- hybrid, which involves a combination of electronic and traditional expression of will (for example, voting takes place with the help of ordinary paper ballots, the result of which is then read and votes are counted by electronic means). Examples of this type of electronic voting can be Kazakhstan or France (in the latter case, this applies only to voting at foreign polling stations) [20].

We would like to note that in this publication we will consider e-voting in its remote version. This is due to the fact that we see this type of voting as the most convenient for voters and the one that best meets the current trends in the development of information and communication technologies. Therefore, we will consider the main disadvantages and threats of voting via the Internet.

3.2. Reasons and main potential advantages of implementation of e-voting

Many scholars point out that one of the main reasons that has caused politicians' attention to e-voting is the steady trend of declining electoral participation in many countries around the world, including in stable democracies. This problem is inherent, first of all, for local elections, but to a large extent it becomes a characteristic of modern national elections. At the same time, the researchers note, if earlier the category of absentees could include primarily representatives of marginalized social groups, at the present stage the reluctance to participate in elections has also become characteristic of other segments of the population. Young people show a special apathy to the elections in modern conditions. Therefore, apologists for e-voting point out that its implementation will allow to reduce level of absenteeism and increase political participation in general [21], [22].

In addition to the above-mentioned advantage, among the positive aspects of e-voting, researchers single out its convenience for voters in general and for certain specific categories of citizens. In this context, it should be noted that e-voting allows to vote without being tied to home or polling station. Therefore, it is advised to use it for expression of will at foreign polling stations, for voting of persons with disabilities, and so on. For other categories of citizens, e-voting is also quite profitable and convenient, because it allows to save time and resources.

In the short term, implementing e-voting can be pretty costly, but in the long run, it will pay off financially and save the state budget. Another advantage of e-voting is the speed and ease of counting votes. It is especially relevant for complex electoral systems, where traditional vote counting is considered one of the main shortcomings. The strengths of e-voting also include its environmental friendliness. It is about saving paper, which is used for numerous election documents (ballots, protocols, statements, etc.), saving electricity, etc. It can also be said that e-voting eliminates the impact of the human factor on elections, which can be negative and be caused by errors and deliberate falsifications.

3.3. Threats of implementation of e-voting

In addition to the above-mentioned positive characteristics and expected results, the implementation of e-voting can pose a number of threats. We see it appropriate to systematize the potential threats of e-voting into the following groups (Fig. 1):

1. threats to democracy;
2. threats of illegal interference;
3. threats of technological failure;
4. threats of legitimacy.

These e-voting threats can be formally represented as a tuple:

$$ET(EV) = \langle Dem(EV), Int(EV), Tech(EV), Leg(EV) \rangle, \quad (1)$$

where *Dem(EV)* – threats to democracy, *Int(EV)* – threats of illegal interference, *Tech(EV)* – threats of technological failure, *Leg(EV)* – threats of legitimacy.

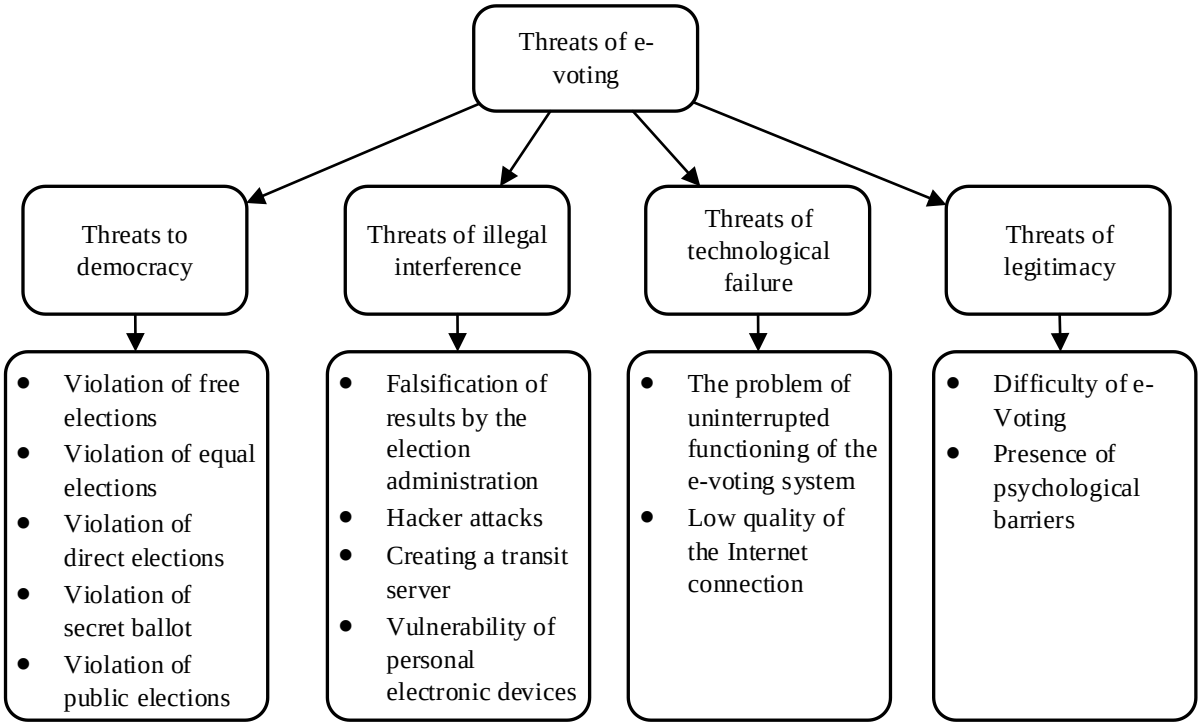

Figure 1. Threats of e-voting implementation

The first group of threats is related to understanding the essence and purpose of elections. Elections are an attribute, a catalyst and an indicator of democracy, without which the development of democracy is impossible. However, not every election can be considered democratic. In many cases, elections can play the role of a tool in the hands of undemocratic political forces to legitimize violence. Therefore, only elections that are held in accordance with universal international standards – democratic principles of elections – can be considered democratic.

These are, first of all, such basic principles as equality, universality, freedom, direct nature of elections and secrecy of the ballot. Without their observance, elections and voting (including e-voting) are detrimental to a democratic society. Therefore, it can be logically assumed that the implementation of e-voting can be appropriate and useful only when it will allow to provide for full compliance with the above-mentioned democratic principles [23].

The problem is that e-voting threatens to uphold most of the mentioned democratic election principles:

- the principle of free elections (there is a risk that the election results will be falsified by persons who administer e-voting systems; there is no guarantee that the voter will not be pressured by other persons – family members (so-called "family voting"), leadership, political forces, etc.;
- the principle of equal elections (e-voting produces a "digital divide" in society as a result of unequal access of individuals to information and communication technologies, and thus creates unequal opportunities to participate and influence elections; there is a threat of multiple voting of individuals both electronically and in combined version with traditional voting);
- the principle of direct elections (there is no guarantee that the act of will expression will be carried out by the person who has the right to participate in e-voting);
- the principle of secret ballot (there is a threat that the will expression will not be anonymous, and the result of the vote of a particular person will become a well-known fact and cause potential pressure and persecution of objectionable citizens);
- the principle of public elections (unlike the traditional voting at the polling station, where there is mutual control of all participants in the election process, during the e-voting the actions of electoral subjects are very difficult to control).

The threat to the observance of democratic principles can be described by a tuple of elements:

$$Dem(EV) = \langle FE(EV), EE(EV), DE(EV), SB(EV), PE(EV) \rangle, \quad (2)$$

where *EF(EV)* – indicator of compliance with the principle of free elections, *EE(EV)* – indicator of compliance with the principle of equal elections, *DE(EV)* – indicator of compliance with the principle of direct elections, *SB(EV)* – indicator of compliance with the principle of secret ballot, *PE(EV)* – indicator of compliance with the principle of public elections.

Threats of illegal interference are in the absence of guarantees that the operation of electronic systems during elections will not be interfered with by outsiders. Therefore, there is a danger that the result of the voter's electronic will expression will be ignored or distorted in the right direction by the falsifiers. The problem is aggravated, in particular, by the fact that, unlike traditional voting, where ballots can be counted in case of doubt about the reliability of the results, during e-voting, the result of the expression of will is only electronic. Therefore, recalculating the votes in case of failure of the electronic system is problematic.

E-voting can be influenced both by the authorities responsible for the effectiveness of e-voting and by outsiders, who, in particular through hacking attacks, may try to either distort the result of the vote or prevent its implementation. In the latter case, attempts to control the results of the vote may be made by domestic and foreign entities.

It is worth noting that the election practice essentially confirms the above. For example, the facts of Russian interference in the US elections in 2016 and subsequent years – in the elections and referendums of several European countries – have been proved. As a result, many countries around the world that had planned to take measures to implement e-voting or had already taken them abandoned it.

Another option for illegal interference in the operation of the e-voting system may be creating a fake (virtual, transit) server. Such a server can accumulate voting options of real voters, change them in the right direction and send the already falsified result to the real server of the election administration.

An essential condition for protection against outside interference is the security of personal electronic means, the problem of which can be an additional factor that will complicate the implementation of e-voting.

The threat of illegal interference can be described by a tuple of elements:

$$Int(EV) = \langle FoR(EV), HA(EV), FS(EV), SP(EV) \rangle, \quad (3)$$

where *FoR(EV)* – indicator of the probability of falsification of voting results, *HA(EV)* – indicator of the probability of a hacker attack affecting the electronic voting process, *FS(EV)* – indicator of the probability of using a fake server in the process of e-voting, *SP(EV)* – indicator of the security level of personal electronic devices.

Speaking about the threats of technological failure, it is worth mentioning the problem of uninterrupted functioning of the electronic system through which voting and counting of votes takes place. It is caused both by the imperfection of any electronic systems in general and by the lack of a unified approach to the quality and security requirements of e-voting systems.

The low quality of Internet connection can be a problem during e-voting. In particular, there may be a situation where a voter registered but did not have time to vote due to a disconnection. Alternatively, the voter managed to vote but did not receive confirmation that his or her vote was taken into account.

Such problems, in our opinion, should be considered in the context of counteracting multiple voting. This is because, on the one hand, it can be a speculative mechanism on the part of voters who will use contrived connection problems to be able to vote more than once. On the other hand, given the reality of these problems, this may be an obstacle to the exercise of the legal right to vote.

The threat of technological failure can be described by a tuple of elements:

$$Tech(EV) = \langle UT(EV), IC(EV) \rangle \quad (4)$$

where *UT(EV)* – indicator of uninterrupted functioning of e-voting systems, *IC(EV)* – indicator of Internet connection quality.

Threats of legitimacy of elections are primarily related to the existence of psychological barriers that prevent a person from perceiving e-voting and trusting its results. Threats of legitimacy are also related to the complexity of e-voting systems for the voter, as the level of voter confidence in e-voting will be largely determined by how well he or she understands how it works.

The threat of legitimacy can be described by a tuple of elements

$$Leg(EV) = \langle PB(EV), CS(EV) \rangle \quad (5)$$

where *PB(EV)* – indicator of the presence of psychological barriers to e-voting among the population, *CS(EV)* –indicator of complexity in using electronic voting systems.

3.4. Ways of neutralization the threats of e-voting

It is worth noting that each of the groups of threats of e-voting identified by us requires its own specific methods of counteraction. Let us first consider possible ways to neutralize threats to democracy (Fig. 2).

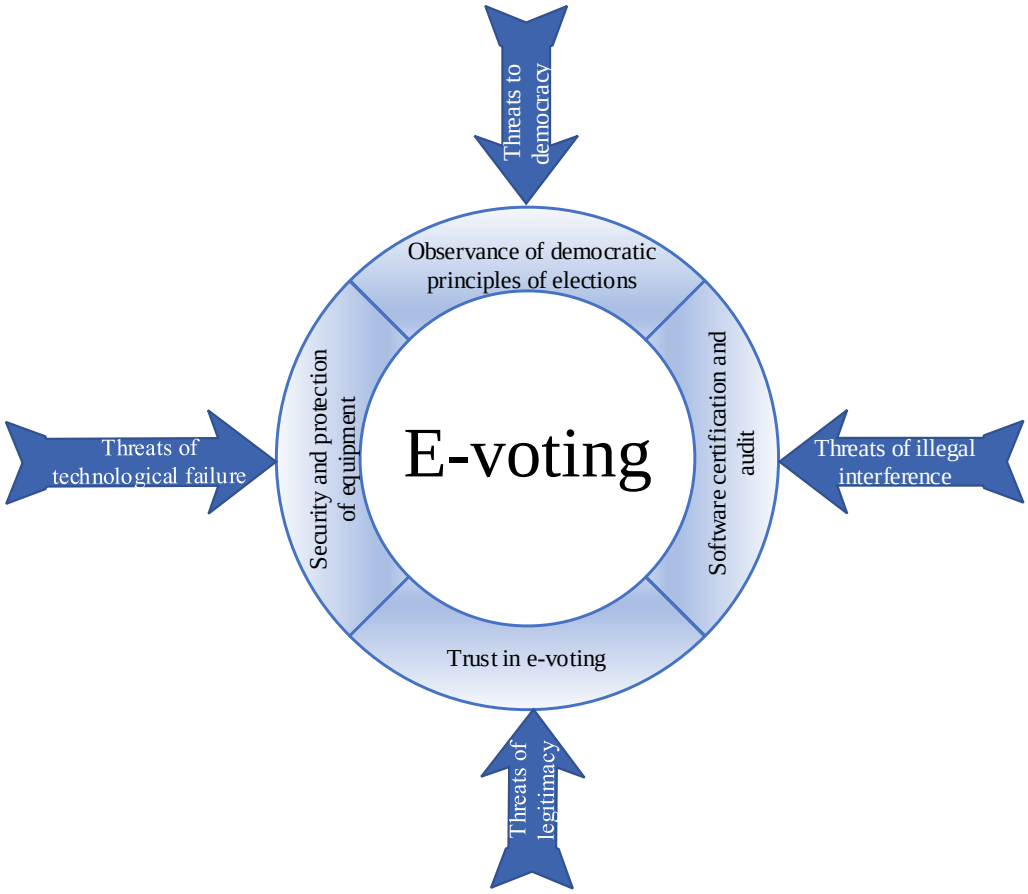

Figure 2. Impact of threats on e-voting and means of countering them

One of the ways to ensure reliable voter identification, which is an essential condition for adhering to the principle of direct elections, may be the use of an electronic signature. The voter can receive the electronic signature key in advance, once and repeatedly, for specific elections. In the first case, the voter can vote for the received key constantly in all subsequent elections. On the one hand, it is convenient but reduces the reliability of the received key and increases the risk of losing it. In the second case, the reliability of the key to the electronic signature is higher, but the convenience is leveled, because the voter is forced to spend time and effort on the eve of each election to obtain a new key.

A more reliable way to solve the problem of voter identification is to use an individual identification card (ID card). This card allows an electronic digital signature and has several levels of protection. It is issued to the voter once and makes it impossible for other persons to vote because the voter for identification must indicate a number of data known only to him (secret code, date, place of birth, etc.). Another essential advantage of the ID card is the ability to use it for other actions and services as a citizen.

Leveling the digital divide and creating equal possibilities for voters to influence voting results can be achieved through combined electronic and traditional voting during the elections. In order to prevent multiple voting (including the use of both traditional and e-voting by one person), it is essential to

identify and remove from the electoral roll at the polling station those who voted electronically. It is necessary to create a single electronic database of people who voted, which will be updated in real-time.

To ensure a secret ballot, the following ways of neutralizing the relevant threats are possible:

- the existence of a depersonalized voter list, which contains only the numbers of documents (ID cards) used for voting, and, at the same time, there is no other data that would allow to identify the person;
- the use of depersonalization servers that erase information that identifies the voter;
- the use of technology for "shuffling" ballots, in which e-ballots are read in any order, rather than as they are received;
- the use of protocols with a split result, in which ballots and voter data are divided between different bodies, which makes it impossible to falsify the results and violate the secrecy of the ballot;
- the use of protocols with a blind signature allows the voter to receive a ballot with a signed signature from an authorized person who, at the same time, does not know which of the voters received a particular ballot [23].

The threat of violating the principle of public elections is considered problematic for neutralization. In particular, unlike traditional voting at polling stations, it is almost impossible to monitor the voting process and count votes for e-voting comprehensively. Herewith, the principle of free elections is also under threat, as it is difficult to guarantee that the voter will not be pressured during the realization of the act of expression of will. At the same time, researchers emphasize that this threat can be partially neutralized by the implementation of voter "individual" control using an ID card.

The value of the threat to democracy during electronic elections is determined using the formula:

$$Dem(EV) = \big(k_1 * FE(EV) + k_2 * EE(EV) + k_3 * DE(EV) + k_4 * SB(EV) + k_5 * * PE(EV)\big)/100 \quad (6)$$

Each indicator *FE(EV), EE(EV), DE(EV), SB(EV), PE(EV)* belongs to a set of values from the interval [0;100], where 0 is a low threat, 100 is the highest threat of impact on e-voting. They are determined by political experts at the time of electronic elections. The value of the coefficients for each type of threat *(k_1,k_2,k_3,k_4,k_5)* is determined expertly, taking into account political, social and financial factors that are relevant in the territory where electronic elections are planned. Also, the following condition $k_1 + k_2 + k_3 + k_4 + k_5 = 1$ must be fulfilled for the coefficients

Neutralization of threats of interference in the course and results of e-voting implies, in particular, ensuring the autonomy of the e-voting system, which will guarantee a reduction of opportunities for interference in its work. Cryptographic protection is often used to ensure the autonomy and reliability of such electronic systems. Besides, it is important to increase the level of computer literacy of citizens, which will reduce the level of individual technical errors of voters. It is also important to increase the security of voters' personal computers.

The calculation of the threat of illegal interference during electronic elections is determined using the formula:

$$Int(EV) = \big(n_1 * FoR(EV) + n_2 * HA(EV) + n_3 * FS(EV) + n_4 * SP(EV)\big)/100. \quad (7)$$

The values of indicators *FoR(EV), HA(EV), FS(EV), SP(EV)* belong to a set [0;100], where 0 is a low threat, 100 is the highest threat of impact on e-voting. These values are determined by computer network security specialists based on the current state of information development of the state. The value of the coefficients for each type of threat *(n_1,n_2,n_3,n_4)* is determined expertly, taking into account political, social and financial factors that are relevant in the territory where electronic elections are planned. Also, the following condition $n_1 + n_2 + n_3 + n_4 = 1$ must be fulfilled for the coefficients.

Among the ways to neutralize the threats of technological failure of the e-voting system are the following:

- implementation of international certification of e-voting systems;
- conducting a preliminary audit of e-voting systems;
- installation of uninterruptible power supply equipment or installation of an independent electricity generator.

The value of the threat of influence on e-voting due to technological efficiency during the conduct of electronic elections is determined by the following formula:

$$Tech(EV) = \big(m_1 * UT(EV) + m_2 * IC(EV)\big)/100. \quad (8)$$

The values of indicators *UT(EV)* and *IC(EV)* are determined by technical staff based on information about the state of development of computer and electrical networks in the regions where e-voting is planned. These values should belong to the set [0;100], where 0 is a low probability of denying access to e-voting systems, 100 is a high probability of communication loss during voting. The value of the coefficients for each type of threat (m_1,m_2) is determined expertly, taking into account the importance of the impact of this indicator on conducting electronic elections. Also, the following condition $m_1 + m_2$ =1 must be fulfilled for the coefficients.

Neutralization of threats of legitimacy presupposes, first of all, conducting systematic educational activities among citizens aimed at better understanding the essence of e-voting and forming a positive attitude to its results. For this purpose, it is expedient to train relevant specialists.

The value of threats of the legitimacy of e-voting is determined by the following formula:

$$Leg(EV) = \big(l_1 * PB(EV) + l_2 * CS(EV)\big)/100. \quad (9)$$

The values of indicators *PB(EV)* and *CS(EV)* are determined on the basis of sociological surveys and the results of testing e-voting systems. These values should belong to the set [0;100], where 0 is a low threat of voter sabotage of e-voting, 100 is the highest threat of election failure due to the human factor. The value of the coefficients for each type of threat (l_1,l_2) is determined expertly, taking into account educational initiatives regarding e-voting in the state. Also, the following condition $l_1 + l_2$ =1 must be fulfilled for the coefficients.

At the same time, it should be understood that for some voters the increase in the level of trust in e-voting can be supported only by the positive experience of its testing in practice.

3.5. Prediction of the expediency of electronic voting

The proposed calculations allow to predict the expediency of electronic voting. Having analyzed each threat to e-voting, determining the values and coefficients of indicators of these threats, we can calculate the level of influence of this threat on the results of e-voting. Coefficients of indicators of threats of electronic voting are used to adjust the influence of a certain indicator on voting results depending on the social and political situation in the country. The indicators of each group of threats are determined by experts taking into account the specifics of the development of the political situation and the results of sociological surveys of citizens.

The formation of recommendations regarding the expediency of conducting electronic voting is carried out on the basis of the average arithmetic value of four groups of e-voting threats.

$$T(EV) = \big(Dem(EV) + Int(EV) + Tech(EV) + Leg(EV)\big)/4. \quad (10)$$

The threat assessment scale is proposed in Table 1.

Table 1

The threat assessment scale

T(EV)	Value of the threat
[0;0.20]	Low threat of influence on e-voting
[0.21;0.5]	A dangerous situation for e-voting
[0.51;1]	Impossibility of e-voting

Our proposed method of determining the level of threats during the introduction of electronic voting has not yet been tested by us in practice. This is due to the scale and complexity of this type of verification of the developed methodology, as well as the desire to analyze in detail the specifics of defining each of the groups of selected threats. Therefore, we consider it expedient to leave this area of work for our future practical studies, which will involve the analysis of specific cases of electronic voting, determining the level of existing threats, and, therefore, choosing the expediency/impracticality of conducting electronic voting.

4. Conclusions

In conclusion, it should be emphasized that our study showed: the implementation of e-voting is accompanied by a set of threats that could call into question the democratic nature of the institution of elections, destroy confidence in the mechanisms of democracy and even threaten the sovereignty of the state. Of course, the presence or absence of threats largely depends on the characteristics of the system used in e-voting, as well as on the effectiveness of the implementation of mechanisms to neutralize existing threats. With an integrated approach, the existing threats of e-voting can be largely neutralized. However, certain risks and threats will still be present.

At the same time, it should be noted that an ideal electoral system and ideal electoral procedures do not exist in principle. Traditional voting also has or could potentially have a range of threats that would call into question the democratic nature of elections, even in stable democracies. Therefore, the question of the expediency and prospects of the implementation of e-voting should, in our opinion, be considered not in the context of abandoning it, but in the context of effective neutralization of potential threats.

It is also worth noting the extremely important role of a high level of computer literacy and democratic electoral culture of all participants in the election process. This factor can be a reliable means of neutralizing many of these threats of e-voting, ranging from ensuring the democracy of e-voting to the absence of technical errors in voting and ensuring the functioning of the system.

5. References

[1] S. M. T. Toapanta, I. F. M. Saá, F. G. M. Quimi, and L. E. M. Gallegos, An Approach to Vulnerabilities, Threats and Risk in Voting Systems for Popular Elections in Latin America, ASTES Journal 4 (2019) 106–116. doi: 10.25046/aj040315.

[2] J. I. Pegorini, A. C. Souza, A. R. Ortoncelli, R. T. Pagno, and N. C. Will, Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Test, in: E. Loukis, M. Anne Macadar, M. M. Nielsen and M. Peixoto (Eds.), ACM International Conference Proceeding Series, Association for Computing Machinery, New York, United States, 2022, pp. 157–164. doi: 10.1145/3494193.3494301.

[3] S. M. T. Toapanta, M. A. Armijos, and L. E. M. Gallegos, Analysis of Cybersecurity Models Suitable to Apply in an Electoral Process in Ecuador, in: ACM International Conference Proceeding Series, ACM International Conference Proceeding Series, Association for Computing Machinery, New York, United States, 2020, pp. 84–90. doi: https://doi.org/10.1145/3375900.3375912.

[4] R. Samihardjo, Murnawan, and S. Lestari, E-Voting in Indonesia Election: Challenges and Opportunities, Review of International Geographical Education Online 11(2021). URL: https://rigeo.org/submit-a-menuscript/index.php/submission/article/view/1594.

[5] D. I. Sensuse, P. B. Pratama, and Riswanto, Conceptual Model of E-Voting in Indonesia, in: Proceedings of the 2020 International Conference on Information Management and Technology (ICIMTech), IEEE, Bandung, Indonesia, 2020, pp. 387–392. doi: 10.1109/ICIMTech50083.2020.9211156.

[6] A. Al-Ameen and S. Talab, The Technical Feasibility and Security of E-Voting, The International Arab Journal of Information Technology 10 (2013) 397–404. URL: https://iajit.org/PDF/vol.10,no.4/4313.pdf.

[7] V. Agate, M. Curaba, P. Ferraro, G. L. Re, and M. Morana, Secure e-Voting in Smart Communities, CEUR Workshop Proceedings 2597 (2020). URL: http://ceur-ws.org/Vol-2597/paper-01.pdf.

[8] K. Divya and K. Usha, Blockvoting: An Online Voting System Using Block Chain, in: Proceedings of the 2022 International Conference on Innovative Trends in Information Technology (ICITIIT), IEEE, Kottayam, India, 2022, pp. 1–7. doi: 10.1109/ICITIIT54346.2022.9744132.

[9] M. Buchyn, A. Helesh, and B. Shubyn, Information Security During Electronic Voting: Threats and Mechanisms for Ensuring, in: Proceedings of the 4th International Conference on Advanced Information and Communication Technologies (AICT), IEEE, Lviv, Ukraine, 2021, pp. 266–269. doi: 10.1109/AICT52120.2021.9628971.

[10] A. Bhawiyuga, A. Basuki, and N. W. Tiera, An Ethereum Based Distributed Application for Ensuring the Integrity of Stored E-Voting Data, in: ACM International Conference Proceeding Series, New York, USA, 2021, pp. 235–239. doi: 10.1145/3479645.3479706.
[11] R. K. Megalingam, G. Rudravaram, V. K. Devisetty, D. Asandi, S. S. Kotaprolu, and V. V. Gedela, Voter ID Card and Fingerprint-Based E-voting System, Inventive Computation and Information Technologies, volume 336 of Lecture Notes in Networks and Systems, Springer, Singapore, 2022, pp. 89–105. doi: 10.1007/978-981-16-6723-7_8.
[12] H. M. Almimi, S. A. Shahin, M. Sh. Daoud, M. Al Fayoumi, and Y. Ghadi, Enhanced E-Voting Protocol Based on Public Key Cryptography, in: Proceedings of the 2019 International Arab Conference on Information Technology (ACIT), IEEE, Al Ain, United Arab Emirates, 2019, pp. 218–221. doi: 10.1109/ACIT47987.2019.8990991.
[13] J. Budurushi, S. Stockhardt, M. Woide, and M. Volkamer, Paper Audit Trails and Voters' Privacy Concerns, in: Proceedings of the International Conference on Human Aspects of Information Security, volume 8533 of Lecture Notes in Computer Science, Springer Cham, 2014, pp. 400–409. doi: 10.1007/978-3-319-07620-1_35.
[14] L. Panizo Alonso, M. Gascó, D. Y. Marcos del Blanco, J. Á. Hermida Alonso, J. Barrat, and H. Aláiz Moreton, E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting, IEEE Transactions on Emerging Topics in Computing 9 (2021) 161–173. doi: 10.1109/TETC.2018.2881891.
[15] D. Y. Marcos del Blanco, D. Duenas-Cid, and H. Aláiz Moretón, 'E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes', in Lecture Notes in Computer Science(, Cham, 2020, vol. 12455, pp. 147–166. doi: 10.1007/978-3-030-60347-2_10.
[16] B. F. Alrashidi, A. M. Almuhana, and A. M. Aljedaie, The Effects of the Property of Access Possibilities and Cybersecurity Awareness on Social Media Application, in: A. Alfaries, H. Mengash, A. Yasar, and E. Shakshuki (Eds.), Communications in Computer and Information Science, volume 1097 of Advances in Data Science, Cyber Security and IT Applications, Springer Cham, 2019, pp. 57–68. doi: 10.1007/978-3-030-36365-9_5.
[17] A. Peleshchyshyn, V. Vus, O. Markovets, and R. Pazderska, Methods and algorithms for performing separate operational tasks for the protection of the state information space, CEUR Workshop Proceedings 2588 (2020) 392–403. URL: http://ceur-ws.org/Vol-2588/paper33.pdf.
[18] A. Peleshchyshyn and S. Albota, Contradictory Statement as a Basis for Conflict Resolution Strategies, CEUR Workshop Proceedings 2588 (2020). URL: http://ceur-ws.org/Vol-2588/paper28.pdf.
[19] A. Bayaga, M. Kyobe, and J. Ophoff, Criticism of the role of trust in e-government services, in: Proceedings of the 2020 Conference on Information Communications Technology and Society (ICTAS), IEEE, Durban, South Africa, 2020, pp. 1–6. doi: 10.1109/ICTAS47918.2020.233973.
[20] N. Melnykova, M. Buchyn, S. Albota, S. Fedushko, and S. Kashuba, The Special Ways for Processing Personalized Data During Voting in Elections, in: N. Shakhovska, M. O. Medykovskyy (Eds.), Proceedings of the Conference on Computer Science and Information Technologies, volume 1080 of Advances in Intelligent Systems and Computing, Springer, Cham, 2020, pp. 781–791. doi: 10.1007/978-3-030-33695-0_52.
[21] N. Kersting, Electronic voting and democracy in Europe, Political Science 4 (2007) 123–144.
[22] N. Kersting and H. Baldersheim (Eds.), Electronic Voting and Democracy. A Comparative Analysis, Palgrave Macmillan London, London, 2004. URL: https://link.springer.com/book/10.1057/9780230523531.
[23] M. A. Buchyn, Demokratychni vybory v Ukraini: pryntsypy, mekhanizmy ta tekhnolohii realizatsii [Democratic elections in Ukraine: principles, mechanisms and technologies of implementation], Lviv Polytechnic Publishing House, Lviv, Ukraine, 2016.