

Problems and Prospects of the Neutralization of Threats of E-Voting in Ukraine

Oleksandr Markovets ^{1,†}, Mykola Buchyn ^{1,*,†}, Vasil Sprinsyan ^{2,†} and Vira Liubchenko ^{3,†}

¹ Lviv Polytechnic National University, Bandery Str. 12, 79013 Lviv, Ukraine

² Odesa Polytechnic National University, 1 Shevchenko Ave., Odessa, 65037, Ukraine

³ Hochschule für Angewandte Wissenschaften Hamburg, Ulmenliet 20, Hamburg, 21033, Germany

Abstract

The article contains an analysis of the problems and prospects of the neutralization of threats that impede the introduction of electronic voting in Ukraine. On the basis of the conducted expert survey, an expert assessment of the influence of each threat, developed by the authors, to the introduction of e-voting during the election process in Ukraine has been shown. The researchers demonstrate the position of experts on the possibility of neutralization of existing threats as a condition for the implementation of electronic voting and conducting elections in Ukraine in accordance with the democratic standards. With the results of the expert survey and the author's formula, the level of potential neutralization of threats when using e-voting in Ukraine is estimated.

Keywords

Elections, e-voting, expert survey, threats to e-voting, mechanisms for neutralization of threats, democracy, Ukraine.

1. Introduction

We live in the era of information society, in the period of rapid development of information and communication technologies. Their comprehensiveness leads to the fact that information and communication technologies penetrate into all spheres of human life without an exception. They bring significant conveniences, facilitating faster and easier obtaining of information, optimizing all processes and mechanisms, making them faster, clearer and more transparent.


At the same time, the information society and information and communication technologies pose a number of security and information threats. In particular, this includes the growth of possibilities for spreading disinformation and large-scale manipulations by several orders of magnitude. Another side effect of the development of information society and information and communication technologies is the emergence of hacking, cyberattacks and cybercrime. In

SCIA-2024: 3rd International Workshop on Social Communication and Information Activity in Digital Humanities, October 31, 2024, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

✉: oleksandr.v.markovets@lpnu.ua (O. Markovets); mykola.a.buchyn@lpnu.ua (M. Buchyn); sprinsyan@op.edu.ua (V. Sprinsyan); vira.liubchenko@haw-hamburg.de (V. Liubchenko)

 0000-0001-8737-5929 (O. Markovets); 0000-0001-9087-5123 (M. Buchyn); 0000-0003-1099-4718 (V. Sprinsyan) 0000-0002-4611-7832 (V. Liubchenko)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

addition, the penetration of information technology into all spheres of social life destroys privacy and makes personal life more public.

The field of politics is no exception to the rule. Information and communication technologies also play an important role in political processes, as they make communication and interaction between the government and citizens more efficient and transparent. Such phenomena as e-government and e-democracy are becoming quite common in the political sphere. Therefore, a logical step would be to use information and communication technologies more widely in the field of politics during the implementation of the largest and most important political process - elections. Even now, information and communication technologies are broadly used to create and update the state register and voter lists; to conduct election campaigning; to inform voters about the course and results of the election race; to nominate and register candidates; to effectively administer the election process, etc.

In the context of the above, it seems quite logical to actualize the problem of wider introduction of information and communication technologies during the key stage of the electoral process - the stage of voting and vote counting. Thus, the issue of implementing e-voting is an urgent one both for Ukraine and for the world in general. However, it is necessary to understand that electronic voting (given the key role of the institute of elections in shaping the political elite and determining the future vector of society's development) is also characterized by a larger level of various threats. After all, the opportunity to distort the results of the will expression and change the course of state development is very attractive for political forces within each country and for external political forces. In this context, it becomes obvious that neglecting the existing threats caused by the introduction of electronic voting can not only deal a devastating blow to democracy, but also substantially change the direction of the state's socio-political development.

It is worth noting that the problem of using electronic voting during elections is an extremely relevant issue for Ukraine. This can be explained, in addition to global trends, by additional factors, including the high level of progress in the domestic IT sector; availability of information and communication technologies; development of information and communication infrastructure; the state policy of digitalization of the state declared by the current Ukrainian government; the socio-political and military situation, which does not enable elections to be held in the traditional way in times of war, etc.

The last factor, at the same time, outlines a clear understanding of a whole range of threats, in particular, external ones, which become very relevant in the case of the introduction of e-voting in Ukraine. They are related to the Russia-Ukraine war in which information warfare is an important element. This leads to the obvious conclusion that the e-voting system that is to be introduced in Ukraine will almost certainly be subject to Russian hacker attacks, complemented by large-scale disinformation and manipulation by the Russian Federation. Besides external threats of electronic voting, there are also internal threats: a low level of democracy; threats from various socio-political groups seeking to influence the outcome of e-voting; technological threats and problems of the e-voting system; low level of trust among citizens to the results of electronic voting, etc.

Consequently, it can be stated that the introduction of electronic voting in Ukraine is a logical but dangerous prospect, as it is characterized by numerous security threats, both external and internal. Without studying the existing threats and mechanisms for their neutralization, the introduction of e-voting could result in catastrophic consequences. This is why the problem

of prospects and possibilities of neutralizing existing threats from the introduction of electronic voting in Ukraine requires additional investigation, especially expert assessment. After all, on this basis, it would be possible to draw conclusions about the expediency and prospects of using electronic voting in Ukraine during elections.

2. Related Works

The paper is a continuation and is based on a number of authors' publications: «Threats of the Implementation of E-Voting and Methods of Their Neutralization», «Threats and Perspectives of the Implementation of E-Voting in Ukraine», «Russian information-psychological special operations in Ukraine and peculiarities of system design for their countermeasures», «Information Security During Electronic Voting: Threats and Mechanisms for Ensuring», in which the authors consider the prospects of e-voting in Ukraine in the context of the main threats, of both external and internal nature. The researchers created a formula to calculate the level of security (and, accordingly, the level of threats) of electronic voting. The formula is based on 4 groups of threats of e-voting: threats to democracy; threats of illegal interference; threats of technological failure; threats of legitimacy. The mentioned groups of threats also serve as indicators that will influence the decision to implement (or not to implement) electronic voting in a particular country in general and in Ukraine specifically [1].

Moreover, in one of the previous articles, the authors tested the validity of the formula for calculating the level of security (threat level) characterizing e-voting with the help of experts by conducting an expert survey. The results of the expert survey not only confirmed the validity of the author's formula for calculating the level of threats to electronic voting. They allowed us to outline the prospects for further scientific research on the issue, particularly, the study of opportunities and mechanisms for neutralization of existing security threats [2]. Therefore, our article contains a thorough analysis of another expert survey aimed at analyzing the existing threats to the implementation of electronic voting in Ukraine in terms of prospects and the possibility of their neutralization. The present article also offers certain mechanisms for neutralization of existing threats from the introduction of electronic voting in Ukraine.

In addition, the authors used some preliminary ideas connected, in particular, with information security when using e-voting, threats and mechanisms for their neutralization, such as the usage of blockchain technology [3]; the necessity to comply with democratic election principles while using e-voting [4]; the existence of external threats to e-voting related to Russian aggression against Ukraine and the enemy's use of information and psychological special operations [5], etc.

In general, the issue of electronic voting and security threats associated with its usage is highly relevant. Therefore, this issue has become the object of scientific attention of many Ukrainian and foreign scholars. It should be noted that both the problem in general and related scientific researches, in particular, have a clearly expressed interdisciplinary character. First of all, this is because different aspects of the issue of security threats of electronic voting are the objects of investigation by different sciences: elections, democracy and voting are studied primarily within the framework of political and legal studies; electronic voting is the subject of research (in addition to political science) also in technical sciences, in particular, the science of information technology; security issues of electronic voting and problems of their neutralization have become the subject of research in the frame of information security; the

level of public perception of electronic voting and its results is impossible without qualitative sociological research, etc. So, a comprehensive and qualitative study of e-voting should be interdisciplinary in nature, and thereby involve researchers from different sciences.

In our opinion, the main modern studies on e-voting, existing threats to its use and mechanisms for neutralization can be divided into several groups. The first group includes scientific works that address the issues of elections, e-government and e-voting in general. The second group of scientific studies is devoted to certain aspects of the use of electronic voting. The third group of scientific sources is dedicated to security threats of e-voting. The fourth group of sources includes publications that discuss potential mechanisms for neutralizing security threats of electronic voting. The fifth group of scientific studies involves the analysis of electronic e-voting through the prism of its functioning in specific foreign countries.

The first group of scientific sources comprises a number of scientific articles that deal with such general issues as practical experience of e-government development [6]; the interconnection between elections and democracy [4], [7]; assessment of existing e-voting systems according to the Council of Europe recommendations [8], [9]; e-government services and the problem of trust in them [10], etc.

The second group of scientific papers refers to different aspects of e-voting, in particular, the processes of preserving the integrity of e-voting data [11]; the problem of ensuring confidentiality when using e-voting [12]; the issue of using the blockchain during electronic voting [13], etc.

The third group of research sources includes works that provide a general analysis of security threats of electronic voting [1] analyze the expert assessment of the level of impact of existing threats due to the introduction of electronic voting [2]; study the technical capabilities and security of electronic voting systems [14]; examine the problem of electronic voting security in smart communities [15]; analyze the possibility of forming a secure and decentralized e-voting system [16]; study methods and algorithms for performing operational tasks aimed at protecting the state information space [17]; emphasize the significance of information security awareness for the reliable use of social networks [18], etc.

The fourth group of scientific papers is devoted to the study of certain mechanisms for neutralizing threats of electronic voting. Namely, these are mechanisms such as the use of blockchain technology [3]; the use of an e-voting protocol based on public key cryptography [19]; the use of paper audit of e-voting results [20]; the use of voter ID cards and fingerprint technology during e-voting [21], etc.

The fifth group of scientific papers comprises the works of scholars related to the practical experience of foreign countries regarding the peculiarities and problems of using electronic voting during elections. By the way, these are mainly Latin American scholars who study the mentioned issue on the example of the region as a whole [22], as well as at the level of specific Latin American countries or countries of other regions. In the latter case, it is worth highlighting, primarily, studies of the peculiarities and problems of using electronic voting in states such as Brazil [23], Indonesia [24], [25] or Ecuador [26].

To sum up, we can conclude that there is a significant scientific interest of both Ukrainian and foreign researchers in the problem of electronic voting, which is logical given the relevance of the issue and its compliance with the trends of the modern world. At the same time, the issue of neutralizing security threats of e-voting as a condition for its effective implementation in Ukraine has, to some extent, remained beyond the attention of researchers. Another interesting

aspect of the study of the issue is conducting an expert survey and obtaining an expert assessment of the possibilities and prospects for neutralizing existing threats to the introduction of electronic voting in Ukraine. Considering the above, the relevance of the issue necessitates a more thorough examination.

3. Results and Discussion

3.1. Features of the expert survey on determining the prospects and possibilities of neutralization of security threats from the implementation of electronic voting

As mentioned earlier, the publication is a continuation of the authors' previous articles, in which they developed their own methodology for calculating the level of security threats that will be present in the case of electronic voting during elections [1], and also tested the validity of the formula based on an expert survey. At the same time, the expert survey not only showed the relevance of the author's formula for estimating the level of threats to e-voting, but also made it clear that further scientific research is needed, particularly in the area of expert assessment of the possibilities and prospects for neutralizing existing threats of e-voting as a condition for holding elections in accordance with democratic standards [2].

As a result, in order to assess the possibilities and prospects for the neutralization of security threats of e-voting in Ukraine, the authors conducted another anonymous expert survey. It was conducted using a Google form and lasted for 4 months – from March to June 2024. The internal structure of the expert community that participated in the survey was similar to last year's survey. Five categories of experts took part in the survey: scientists; analyst experts; public and political figures and politicians; members of public organizations; and information technology specialists. The only difference between the structure of the expert community and the last year's survey was the doubling of the number of experts: 50 experts participated in the 2023 survey, while the number of experts in this year's survey reached 100. At the same time, the proportion of different categories of experts remained unchanged: scientists accounted for half (50%) of the total number of respondents; analyst experts and members of NGOs accounted for 12% of respondents each; the number of public and political figures and politicians reached 16%; information technology specialists accounted for 10% of respondents.

The purpose of involving scientists in the survey was to obtain a scientific and research justification for the possibility and prospects of neutralizing security threats of electronic voting in Ukraine. The authors pursued a similar goal in the case of engaging analyst experts in the survey. Besides, in this case, there was an awareness that analyst experts, unlike scientists, would assess the problem of neutralizing threats of e-voting not only from the viewpoint of scientific theory, but also from the viewpoint of taking into account the context of various aspects of socio-political processes taking place in our country. The aim of involving public and political figures and politicians in the survey was to obtain an analysis of the practical side of neutralizing the security threats of electronic voting, and, as a consequence, to determine the level of readiness of the Ukrainian political elite to effectively combat the threats of electronic voting.

The main purpose of involving such a category of respondents as members of public organizations in the expert survey was to obtain a comprehensive assessment of the possibilities and prospects for neutralizing security threats of e-voting. This is due to the fact that members

of public organizations assess socio-political phenomena and processes from different perspectives: from the viewpoint of their democratic nature, from the viewpoint of impartiality and the viewpoint of their own practical experience. Finally, the main purpose of involving information technology specialists in the expert survey was to assess the technical capabilities to neutralize security threats of electronic voting in Ukraine.

We also used certain criteria and methods to select respondents for the expert survey. For instance, scholars were selected according to their field of scientific interest, which had to be related to elections and democracy. In order to do this, we conducted a research on their publications in Google academy using certain keywords: “elections”, “democracy”, “e-voting”, “e-governance”, etc. Similar criteria were applied to the selection of analyst experts, although the search was not based on publications in the Google Academy, but on the search for the mentioned keywords in their posts on the social networks Instagram and Facebook.

By choosing respondents from the category of public and political figures and politicians, we were guided by the following selection criteria: party affiliation of the respondents (ensuring the presence of both ruling and opposition politicians) and the scope of the respondents' activities (ensuring the presence of politicians at the national, regional and local levels). The process of involving members of public organizations in the survey was based on such a criterion as the engagement of public organizations in the issues of elections and democracy. Accordingly, we involved members of such international and national NGOs as the International Foundation for Electoral Systems (IFES), the Committee of Voters of Ukraine and the Civil Network OPORA in the expert survey. The criteria for selecting the latter category of respondents were their practical work in the sphere of information technology.

This systematic approach to the selection and engagement of respondents allowed us to conduct a comprehensive expert survey and receive answers to questions from both theoretical and practical perspectives; from both scientific and analytical perspectives; from both the perspectives of decision-makers and electoral stakeholders; to take into account political, security, and technical problems of electronic voting and neutralization of its threats, etc.

For communication with respondents, we used a variety of communication channels that took into account the characteristics of both the respondents themselves and the availability of contact information. Thus, we used the following main communication channels in our interaction with respondents: e-mail; messengers of social networks such as Facebook and Instagram; Telegram; Viber; WhatsApp, etc. Systematized and visualized information about the features of the expert survey is presented in Table 1.

Table 1

Features of the expert survey on determining the possibilities and prospects for neutralizing threats of e-voting in Ukraine

Category of respondents	Scientists	Analyst experts	Public and political figures and politicians	Members of public organizations	Information technology specialists
Category characteristics	Scholars studying the issues of elections, democracy and e-voting	Experts analyzing and publishing analytical materials on the problems	Political subjects who can make decisions on the implementation of electronic voting and	Members of IFES, Committee of Voters of Ukraine, Civil	Practitioners working in the field of development and implementation

		of elections, democracy and e-voting	countering its threats	Network "OPORA"	of information technologies
Selection criteria and method	Keyword search of publication titles in Google Academy	Keyword search of post titles in social networks	Party affiliation (government and opposition) and scale of activity (national, regional or local)	Activity related to democracy and elections	Practical work in the sphere of information technology and information security
Purpose of involvement	Comprehensive scientific assessment of the possibility and prospects of neutralizing threats of e-voting	Theoretical assessment of the possibility and prospects of neutralizing the threats of electronic voting in the context of the analysis of socio-political processes	Analysis of the practical side and assessment of the political will to neutralize threats of e-voting	Assessment of the possibility of neutralizing threats of e-voting from the perspective of democracy, impartiality and practical experience	Assessment of technical capabilities to neutralize threats of e-voting
% of respondents	50 %	12 %	16 %	12 %	10 %
Number of respondents	50	12	16	12	10

3.2. Expert assessment of the impact of e-voting threats

It is worth noting that we used some results of the 2023 expert survey as indicators that will allow us to verify the second expert survey of 2024. For example, the following results of the previous expert survey of 2023 were valuable to us:

- determining the timeframe within which e-voting can be introduced in Ukraine. Since the vast majority of respondents (78.6%) in the 2023 expert survey expressed confidence that e-voting in Ukraine could be introduced within 3-10 years, this also meant that they were confident that most of the security threats of e-voting could be neutralized within this timeframe;
- determining the level of threats to electronic voting in Ukraine. As the results of the 2023 expert survey revealed that the current level of threats to e-voting was average (0.45 according to the author's formula), this meant that the introduction of e-voting in Ukraine is possible, but only after neutralization of the key existing threats [2].

Therefore, having analyzed the results of the current 2024 expert survey, we will try to compare them with the aforementioned results of the 2023 expert survey. This will allow us to verify the results and identify their level of validity.

The current expert survey is based on the results of the authors' previous studies, which singled out 4 groups of threats of electronic voting: threats to democracy; threats of illegal interference; threats of technological failure; threats of legitimacy [1], [2].

Within these groups, 15 direct threats of e-voting were identified:

- falsification of electronic voting;
- pressure on voters;
- unequal access of voters to electronic voting;
- the possibility of multiple voting;
- the possibility of voting by other persons;
- violation of secret ballot;
- inability to control compliance with the law during electronic voting;
- falsification of electronic voting results by the election administration;
- hacker attacks on the electronic voting system;
- the possibility of creating a transit server;
- vulnerability of voters' personal electronic devices;
- the problem of uninterrupted functioning of the electronic voting system;
- low quality of the Internet connection;
- difficulty of electronic voting;
- the presence of psychological barriers to the perception of electronic voting.

The conducted expert survey on threats to electronic voting and opportunities to neutralize them consists of two parts. In the first part of the survey, experts were asked to determine the level of impact of each threat of electronic voting. Furthermore, the respondents had to define this level of threat impact both in general, without reference to a specific situation or country, and in the case of potential introduction of electronic voting in Ukraine.

According to the results of the expert survey, respondents determined the level of negative impact of e-voting threats by assigning a value from 1 (the negative impact of the e-voting threat is the least) to 15 (the negative impact of the e-voting threat is the greatest). Thus, the higher the numerical value assigned to a particular threat due to the survey results, the more dangerous the negative impact of this threat. The range of obtained results could potentially have a value from 100 (the minimum negative impact of the threat of electronic voting that could occur if all 100 experts assigned a value of 1 to such a threat) to 1500 (the maximum negative impact of the threat of electronic voting that could occur if all 100 experts assigned a value of 15 to such a threat). The results of the expert survey are shown in Table 2:

Table 2

Level of experts' assessment of the negative impact of e-voting threats

Threats of e-voting	Impact in general	Place of threat in general	Impact in Ukraine	Place of threat in Ukraine
Falsification of electronic voting	968	1	932	1
The possibility of multiple voting	894	2	858	2
Pressure on voters	834	3	792	6

Hacker attacks on the electronic voting system	816	4	834	3
The possibility of voting by other persons	804	5	796	5
Unequal access of voters to electronic voting	776	6	798	4
Violation of secret ballot	766	7	762	7
Inability to control compliance with the law during electronic voting	698	8	730	8
Vulnerability of voters' personal electronic devices	672	9	656	11
The possibility of creating a transit server	650	10	722	9
Falsification of electronic voting results by the election administration	616	11	684	10
The problem of uninterrupted functioning of the electronic voting system	554	12	562	12
The presence of psychological barriers to the perception of electronic voting	538	13	442	14
Low quality of the Internet connection	482	14	440	15
Difficulty of electronic voting	432	15	492	13

Some important conclusions can be drawn from the results of the expert survey on the level of negative impact of threats of electronic voting:

1. According to experts, the major threats in the context of electronic voting (both in general and in the case of Ukraine) are related to the possibility of falsification of voting results (both in general and in terms of aspects related to falsification, such as multiple voting, pressure on voters, voting by other persons, etc.), as well as hacker attacks on the electronic voting system and its results.
2. In contrast, the least dangerous (both in general and in the case of Ukraine), according to experts, are the threats of e-voting connected with the technical features of the electronic voting system, as well as threats connected with the perception of e-voting by voters. This is why such threats as the difficulty of electronic voting, low quality of Internet connection, uninterrupted functioning of the electronic voting system, psychological barriers to the perception of electronic voting results, etc., were recognized by experts as the least dangerous.
3. The impact of threats to e-voting in Ukraine does not differ significantly from the impact of threats to e-voting in general. Most of the threats received approximately the same assessment among the expert community as in the case of the introduction of e-voting

in Ukraine and in the case of e-voting in general. The gradation (place) of threats to e-voting is similar, with some exceptions, both in general and in Ukraine.

4. At the same time, there are some slight differences in the assessment by certain experts of the negative impact of e-voting threats in the case of Ukraine and in general, which, in our opinion, is related to the specifics of domestic socio-political processes in general and the Russia-Ukraine war, which has a considerable impact on the level of threats of e-voting and the prospects for its implementation in our country.
5. The main differences in the assessment of threats of electronic voting in general and in the case of Ukraine are as follows:
 - according to experts, a more possible threat for Ukraine is the negative impact of hacker attacks on the e-voting system and its results than in the case of the introduction of e-voting in general, without reference to the country. This is logical, especially given the Russia-Ukraine war and the fact that the electronic voting system in Ukraine is likely to be subject to hacker attacks by the Russian Federation;
 - for Ukraine, contrary to the introduction of e-voting in general, in the opinion of experts, the threats associated with the falsification of e-voting results are less dangerous. In particular, experts believe that the possibility of falsifying the results of electronic voting in general is less dangerous in Ukraine. Furthermore, according to experts, some of the other threats related to falsifications are less dangerous (possibility of multiple voting; pressure on voters; possibility of voting by other persons; violation of the secret ballot, etc.). This seems to be a relatively unexpected result of the expert survey, considering the lack of stable democracy in Ukraine;
 - at the same time, experts consider certain threats related to the falsification of voting results (unequal access of voters to electronic voting; falsification of voting results by the election administration; the possibility of creating a transit server) to be more dangerous in Ukraine compared to the situation with the introduction of electronic voting in general. The first two examples, in our opinion, can be explained by the state of war and the concentration of authorities in the power vertical. The third example (the threat of creating a transit server) is obviously related to Ukraine's negative electoral practice, when an attempt to falsify the voting results in 2004 during the presidential election in Ukraine has already taken place;
 - according to experts, the lack of control over the state of compliance with the law during e-voting, as well as the greater difficulty of e-voting for voters, are more dangerous for Ukraine compared to the threats of e-voting in general;
 - experts suggest that threats such as the vulnerability of voters' personal electronic devices, psychological barriers to the perception of electronic voting, and low quality of Internet connection are less dangerous for Ukraine compared to threats of electronic voting in general.

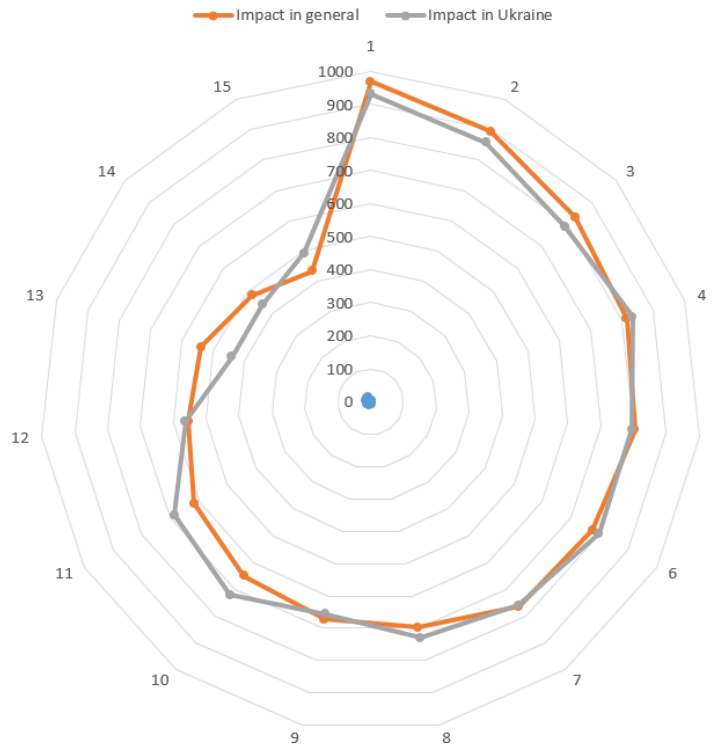


Figure 1: Comparative analysis of the results of an expert survey on the negative impact of electronic voting threats in Ukraine and in general

3.3. Expert assessment of opportunities and prospects for neutralization of threats of e-voting

The second part of the expert survey is devoted to identifying opportunities and prospects for the neutralization of threats of electronic voting in Ukraine. Importantly, the assessment of the impact of e-voting threats conducted in the first part of the survey was used to determine the final state of threats that, in the opinion of experts, will remain after the application of mechanisms for their neutralization.

In the second part, the experts were asked to analyze each of the 15 threats of e-voting in terms of the possibility of their neutralization in Ukraine. Respondents had the opportunity to choose one of three options: “the threat of e-voting in Ukraine can be neutralized completely” (*Pi*), “the threat of e-voting in Ukraine can be neutralized partially” (*PPi*) and “the threat of e-voting in Ukraine cannot be neutralized” (*INi*). The results of the expert survey are shown in Table 3.

Table 3
Expert assessment of the possibilities of neutralizing the threats of electronic voting in Ukraine

Threats of electronic voting in Ukraine	Place of threat	Pi	PPi	INi
Falsification of electronic voting	1	26	46	28
The possibility of multiple voting	2	46	42	12

Hacker attacks on the electronic voting system	3	10	58	32
Unequal access of voters to electronic voting	4	36	50	14
The possibility of voting by other persons	5	34	38	28
Pressure on voters	6	22	44	34
Violation of secret ballot	7	30	48	22
Inability to control compliance with the law during electronic voting	8	26	38	36
The possibility of creating a transit server	9	30	50	20
Falsification of electronic voting results by the election administration	10	30	44	26
Vulnerability of voters' personal electronic devices	11	30	48	22
The problem of uninterrupted functioning of the electronic voting system	12	36	48	16
Difficulty of electronic voting	13	46	44	10
The presence of psychological barriers to the perception of electronic voting	14	38	48	14
Low quality of the Internet connection	15	46	50	4

For a better visualization, we consider it expedient to depict the results of an expert assessment of the possibilities of neutralizing the threats of electronic voting in Ukraine in the form of a diagram (see Figure 2).

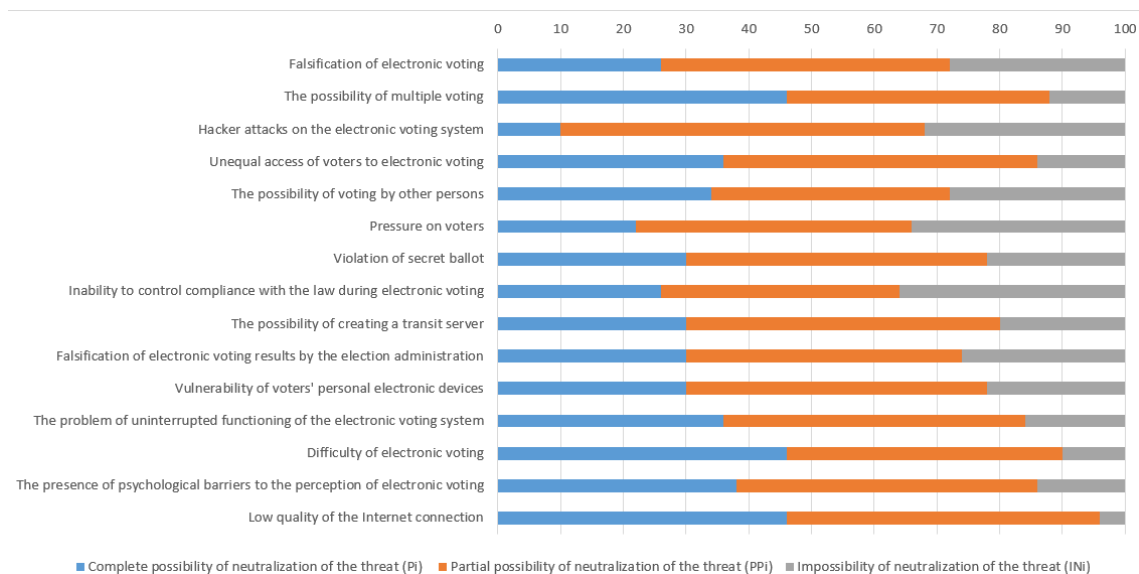


Figure 2: Expert assessment of the possibilities of neutralizing the threats of electronic voting in Ukraine.

Having examined the results of the expert survey, we propose to introduce into scientific circulation and calculate such a notion as the “The level of potential neutralization of electronic voting threats in Ukraine”. It is determined by the following formula:

$$L = \sum_{i=1}^{15} Ln_i, \quad (1)$$

where L – is the level of potential neutralization of threats to electronic voting in Ukraine; Ln_i – is the level of impact of neutralizing a specific threat on the security of electronic voting. To calculate the level of influence of neutralization of a specific threat, we use the formula:

$$Ln_i = \frac{K_i * L_i}{\sum_{i=1}^{15} K_i * L_{max}} * 100, \quad (2)$$

where L_i – is the level of potential neutralization of a specific threat to electronic voting in Ukraine; K_i – is the coefficient of a specific threat to electronic voting in Ukraine, L_{max} – is the level of influence that corresponds to 100% neutralization of the threat

Meanwhile, the level of potential neutralization of a specific threat of electronic voting in Ukraine will be calculated using the formula:

$$L_i = \frac{(P_i + 0.5 * PP_i)}{N} * 100, \quad (3)$$

where P_i – is the level of possibility of complete neutralization of a specific threat to electronic voting; PP_i – is the level of possibility of partial neutralization of the threat to electronic voting. L_i is in the range from 0 (all experts believe that this threat to electronic voting in Ukraine cannot be neutralized) to 100 (all experts believe that this threat to electronic voting in Ukraine can be completely neutralized).

K_i is determined depending on the ranking of a specific threat to electronic voting in Ukraine according to the results of the expert survey and is in the range from 1 (the threat ranks last in terms of negative impact) to 15 (the threat ranks first in terms of negative impact). Such logic is based on the understanding that neutralization of, for example, the most significant threat will have much greater impact on the security of electronic voting than neutralization of the least significant threat.

We also propose to gradate the level of possibility of neutralization of both a specific threat of e-voting and the level of possible neutralization of threats of e-voting in general. Therefore, we consider it appropriate to distinguish three levels of neutralization of threats of electronic voting:

High level (75-100) corresponds to the level in which most of the threats to electronic voting can be neutralized, allowing for the implementation of electronic voting in Ukraine without any concerns.

Average level (50-74) corresponds to the level in which existing threats to electronic voting in Ukraine are partially neutralized. This level is not a reason to reject the introduction of e-voting. However, in this case, appropriate control, security, and verification of e-voting results should be ensured. Only after that, a decision should be made on the further usage or refusal to use electronic voting in Ukraine.

Low level (0-49) corresponds to the level at which the main threats to e-voting have not been largely neutralized. This makes e-voting impossible to use without harming democracy. Therefore, the presence of this level will mean the need to reject the implementation of e-voting in Ukraine.

The results of the expert survey and the calculation of the level of potential neutralization of threats of electronic voting in Ukraine on their basis are shown in Table 4.

Table 4

Possibilities and prospects of threat neutralization of electronic voting in Ukraine

Threats of electronic voting in Ukraine	K_i	L_i	Level of threat neutralization	Ln_i
Falsification of electronic voting	15	49	Low	6,13
The possibility of multiple voting	14	67	Average	7,82
Hacker attacks on the electronic voting system	13	39	Low	4,23
Unequal access of voters to electronic voting	12	61	Average	6,10
The possibility of voting by other persons	11	53	Average	4,86
Pressure on voters	10	44	Low	3,67
Violation of secret ballot	9	54	Average	4,05
Inability to control compliance with the law during electronic voting	8	45	Low	3,00
The possibility of creating a transit server	7	55	Average	3,21
Falsification of electronic voting results by the election administration	6	52	Average	2,60
Vulnerability of voters' personal electronic devices	5	54	Average	2,25
The problem of uninterrupted functioning of the electronic voting system	4	60	Average	2,00
Difficulty of electronic voting	3	68	Average	1,70
The presence of psychological barriers to the perception of electronic voting	2	62	Average	1,03
Low quality of the Internet connection	1	71	Average	0,59
The level of potential neutralization of electronic voting threats in Ukraine (L)				53,23

As we can see, the result of the expert survey conducted in 2024 is quite relevant and correlated with the results of the previous expert survey conducted in 2023. The average level of neutralization of electronic voting threats obtained from the results of the 2024 expert survey fully corresponds to the average level of current threats of electronic voting, which was determined based on the results of an expert survey in 2023. In two cases, the results of the expert survey show that not only as of today, but also in the future, the threats of electronic voting will not lose their relevance. Therefore, the introduction of electronic voting in Ukraine requires a balanced approach and is possible only after neutralizing the key threats that call into question the credibility and democracy of the results of electronic voting.

An analysis of the prospects and the possibility of neutralizing the threats of electronic voting in Ukraine would be incomplete without taking into account one more aspect - the Russian-Ukrainian war. It is important in view of the fact that in the conditions of large-scale hostilities and the legal regime of martial law, it is impossible to hold elections. Moreover, in the conditions of war, the possibilities of preparing for post-war elections are also limited. Therefore, while the Russian-Ukrainian war continues, there are no adequate opportunities to neutralize the threats of electronic voting, which will automatically make the prospect of its implementation in our country more difficult. In addition, the possibility of neutralizing the threats of electronic voting in Ukraine will directly depend on the duration of the war and its results. For example, a complete victory over the enemy will make it possible to return all sovereign territories of Ukraine under control, eliminate external threats to electronic voting,

and thus contribute to the introduction of electronic voting. And, on the contrary, a partial victory or a stalemate situation will make the prospects for the introduction of electronic voting in Ukraine much more problematic.

As it has already been said, the average level of opportunities to neutralize the threats of electronic voting provides grounds for the introduction of electronic voting in Ukraine, however, on the condition that the main threats are neutralized. Therefore, it becomes important to develop mechanisms to neutralize the threats of electronic voting as a condition for its safe implementation in Ukraine. Since this may be a problem for a new in-depth study, we consider it expedient to single out the most important mechanisms for neutralizing the threats of electronic voting only in general terms, namely:

- raising the level of electoral awareness and culture of all participants of the election process;
- development of countermeasures against hacker attacks on the electronic voting system;
- use of blockchain technology to protect electronic voting systems and election data;
- popularization of the idea of electronic voting in order to increase the level of trust in its results;
- independent external audit of electronic voting systems;
- improving the quality of Internet communication and expanding access to the Internet;
- ensuring the autonomy and uninterrupted functioning of the electronic voting system, etc.

4. Conclusions

Summarizing, we can see that according to the results of the expert survey, the main threats of e-voting that have the most negative impact on the security of electronic voting are threats related to the possibility of falsification of the results of e-voting, as well as threats of hacker attacks on the e-voting system. Instead, experts believe that threats related to the technical features of e-voting, as well as threats related to the perception of e-voting by voters, have much less negative impact.

The extrapolation of the expert survey results on the formula developed by the authors to determine the level of potential neutralization of threats of electronic voting in Ukraine showed that all existing threats can be neutralized only partially, although the level of correlation of the possibility of neutralizing threats may vary significantly depending on the specific threat.

The results of the expert survey showed that the level of potential neutralization of specific threats of electronic voting in Ukraine is either low (the number of experts who tend to believe that such threats cannot be neutralized is higher than the number of experts who tend to believe that such threats can be completely neutralized) or average (there is a slight advantage of the number of experts who believe that such threats to electronic voting can be completely neutralized over the number of experts who believe that such threats cannot be neutralized).

The total level of potential neutralization of e-voting threats in Ukraine amounts to 53.23, which is only to a small extent above the lower limit of the average level. This means that most threats of e-voting will be relevant in Ukraine in the future. Although after applying mechanisms to neutralize threats of e-voting, we should not refuse to implement e-voting in

Ukraine, but in this case, we should be cautious. Proper control, security, and verification of voting results must be ensured during e-voting. Only based on the results of such an audit and the application of a balanced approach a decision should be made on the further usage or refusal to use electronic voting in Ukraine.

We also want to emphasize that the prospects for neutralizing the threats of electronic voting depend on two important factors: the level of development of democracy in Ukraine and the results of the Russian-Ukrainian war. On the one hand, a high level of development of democracy always creates conditions (publicity, mutual control, high level of consciousness and culture, etc.) that contribute to the democratization of the election process in general. Therefore, we can safely assume that under such conditions, some of the threats of electronic voting will be automatically neutralized or at least their negative impact will be reduced. On the other hand, the possibility of introducing electronic voting in Ukraine (and holding elections in general) directly depends on how long the Russian-Ukrainian war will last and what its results will be.

References

- [1] O. Markovets and M. Buchyn, 'Threats of the implementation of e-voting and methods of their neutralization', in CEUR Workshop Proceedings, Lviv, Ukraine, 2022. Vol. 3296: Proceedings of the 1st International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA-2022), pp. 29–39.
- [2] O. Markovets and M. Buchyn, 'Threats and Perspectives of the Implementation of E-Voting in Ukraine', in CEUR Workshop Proceedings, Lviv, Ukraine, 2023. Vol. 3608: Proceedings of the 2nd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA-2023), pp. 34–44.
- [3] M. Buchyn, A. Helesh, and B. Shubyn, 'Information Security During Electronic Voting: Threats and Mechanisms for Ensuring', in 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), 2021, pp. 266–269. doi: 10.1109/AICT52120.2021.9628971.
- [4] M. Buchyn, 'Peculiarities and problems of measuring the level of democratic elections', *Balkan Social Science Review*, 2023, vol. 21, pp. 105–125. doi: 10.46763/BSSR2321105b
- [5] O. Markovets, M. Buchyn, A. Kovalchuk and T. Basyuk, 'Russian Information-psychological Special Operations in Ukraine and Peculiarities of System Design for Their Countermeasures', in CEUR Workshop Proceedings, Lviv, Ukraine, 2023. Vol. 3608: Proceedings of the 2nd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA-2023), pp. 108–128.
- [6] O. Tsebenko, N. Lukach, Y. Zavada and O. Stadnichenko, 'Model for Assessing Development of E-Government in Eastern Partnership Countries', *Studies in Systems, Decision and Control*, 2022, Vol. 421, pp. 425–447.
- [7] N. Kersting and H. Baldersheim, *Electronic Voting and Democracy. A Comparative Analysis*. London: Palgrave Macmillan London, 2004. Accessed: Aug. 26, 2022. [Online]. Available: <https://link.springer.com/book/10.1057/9780230523531>
- [8] 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*, vol. 9, no. 1, pp. 161–173, 2021, doi: 10.1109/TETC.2018.2881891.

- [9] 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.
- [10] A. Bayaga, M. Kyobe, and J. Ophoff, 'Criticism of the role of trust in e-government services', in *2020 Conference on Information Communications Technology and Society (ICTAS)*, 2020, pp. 1–6. doi: 10.1109/ICTAS47918.2020.233973.
- [11] 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, NY, USA, 2021, pp. 235–239. doi: 10.1145/3479645.3479706.
- [12] A. Alshehri, G. Srivastava, W. Rajeh, M. Alrowaily and M. Almusali, 'Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain', *Applied Sciences*, 2023, Vol. 13 (2). doi: 10.3390/app13021096.
- [13] 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 (ICITIT)*, 2022, pp. 1–7. doi: 10.1109/ICITIT54346.2022.9744132.
- [14] A. Al-Ameen and S. Talab, 'The Technical Feasibility and Security of E-Voting', *The International Arab Journal of Information Technology*, vol. 10, no. 4, pp. 397–404, 2013, [Online]. Available: <https://iajit.org/PDF/vol.10,no.4/4313.pdf>
- [15] V. Agate, M. Curaba, P. Ferraro, G. L. Re, and M. Morana, 'Secure e-Voting in Smart Communities', in *CEUR Workshop Proceedings*, 2020, vol. 2597. [Online]. Available: <http://ceur-ws.org/Vol-2597/paper-01.pdf>
- [16] A. B. Pedin and N. Siasi, 'Secure and Decentralized Anonymous E-Voting Scheme' in *ACMSE 2023 - Proceedings of the 2023 ACM Southeast Conference*, 2023, pp. 172–176. doi: 10.1145/3564746.3587107
- [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', in *CEUR Workshop Proceedings*, 2020, vol. 2588, pp. 392–403. [Online]. Available: <http://ceur-ws.org/Vol-2588/paper33.pdf>
- [18] B. F. Alrashidi, A. M. Almuhan, and A. M. Aljedaie, 'The Effects of the Property of Access Possibilities and Cybersecurity Awareness on Social Media Application', in *Advances in Data Science, Cyber Security and IT Applications*, Cham, 2019, vol. 1097, pp. 57–68. doi: 10.1007/978-3-030-36365-9_5.
- [19] 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 *2019 International Arab Conference on Information Technology (ACIT)*, 2019, pp. 218–221. doi: 10.1109/ACIT47987.2019.8990991.
- [20] J. Budurushi, S. Stockhardt, M. Woide, and M. Volkamer, 'Paper Audit Trails and Voters' Privacy Concerns', in *Lecture Notes in Computer Science*, Cham, 2014, vol. 8533, pp. 400–409. doi: 10.1007/978-3-319-07620-1_35.
- [21] 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', in *Lecture Notes in Networks and Systems*, Singapore, 2022, vol. 336, pp. 89–105. doi: 10.1007/978-981-16-6723-7_8.

- [22] 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*, vol. 4, no. 3, pp. 106–116, 2019, doi: 10.25046/aj040315.
- [23] J. I. Pegorini, A. C. 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 Tests', in *ACM International Conference Proceeding Series*, Athens, Greece, 2022, pp. 157–164. doi: 10.1145/3494193.3494301.
- [24] R. Samihardjo, Murnawan, and S. Lestari, 'E-Voting in Indonesia Election: Challenges and Opportunities', *Review of International Geographical Education Online*, vol. 11, no. 6, Art. no. 6, 2021, Accessed: Aug. 26, 2022. [Online]. Available: <https://rigeo.org/submit-a-manuscript/index.php/submission/article/view/1594>
- [25] 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)*, 2020, pp. 387–392. doi: 10.1109/ICIMTech50083.2020.9211156.
- [26] S. M. T. Toapanta, M. A. 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*, Barcelona, Spain, 2020, pp. 84–90. doi: <https://doi.org/10.1145/3375900.3375912>.