Threats and Perspectives of the Implementation of E-Voting in Ukraine

Oleksandr Markovets and Mykola Buchyn

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

Abstract

The article contains an analysis of the problems and prospects of the implementation of electronic voting in Ukraine through the prism of assessing potential threats. An expert survey has been conducted on the threats of implementing electronic voting during elections in Ukraine, which is based on the author's methodology for calculating the level of electronic voting security. Based on the expert assessment of 4 groups of security threats have obtained as a result of the expert survey, the author's assessment of the feasibility and prospects of the implementation of electronic voting in Ukraine was made.

Keywords

Elections, e-voting, expert survey, threats to e-voting, democracy, information security, Ukraine.

1. Introduction

Information and communication technologies are becoming an attribute of the modern development of any civilized society, penetrating to a greater or lesser extent in all spheres of social life without exception. They create many new opportunities to make our lives more convenient and comfortable, information more accessible, and industry and production more efficient. At the same time, the development of information and communication technologies creates many security threats, ranging from increasing the possibilities of disinformation and manipulation to cybercrime and hacker attacks.

The political sphere is no exception to this rule, where the use of information and communication technologies makes it possible to make the process of communication and interaction between the government and society more effective and transparent. Today, such phenomena as e-government and e-democracy are becoming an integral attribute of modern socio-political development. In this context, the implementation of e-voting during elections becomes an urgent problem. At the same time, e-voting is characterized by a larger level of security threats, which can be explained by the key role of the election institution not only in the formation of the political elite, but also in determining the future vector of social development. Therefore, neglecting security threats in the context of the implementation of e-voting can not only destroy democracy, but also radically change the vector of socio-political development of the country.

For Ukraine, the problem of implementing e-voting is extremely urgent, taking into account the significant development of information and communication technologies and the course of digitization of the country declared by President V. Zelensky. At the same time, significant security threats are extremely relevant in the context of the implementation of e-voting in Ukraine. On the one hand, they are related to Russian aggression against Ukraine, which potentially makes the future e-voting system an object of Russian hacker attacks, especially in conditions of total disinformation and manipulation by Russia. On the other hand, the low level of democratic development of the states

SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, November 9, 2023, 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)

increases the level of threats from the implementation of e-voting in Ukraine, which can potentially contribute to the possibility of certain political forces using e-voting for the realization of their own political goals and falsification of the voting results.

Therefore, the issue of the implementation of e-voting in Ukraine is relevant and requires comprehensive research in the context of possible security threats. The problem requires a complex expert assessment with the aim of analyzing the level of existing security threats and determining, on the basis of this, the expediency or impracticality of implementing e-voting in Ukraine.

2. Related Works

The work is based on and continues the publication of the authors entitled "Threats of the Implementation of E-Voting and Methods of Their Neutralization", in which the authors consider the main threats that may arise to the authorities in the context of the implementation of e-voting during elections. Having singled out 4 groups of threats to e-voting (threats to democracy; threats due to illegal entry; threats to technological integrity; threats to legitimacy), the authors proposed a formula for calculating the level of security (threat level) for e-voting, which should become an indicator for making a decision on implementation or refusal to implement e-voting in a particular country.

The author's idea provided that the proposed formula for calculating the security level (threat level) for e-voting is determined on the basis of conducted expert surveys. Therefore, our article contains a comprehensive analysis of the conducted expert survey on the feasibility of implementing e-voting in Ukraine in view of the existing security threats [1].

The work also used some previous author's ideas related to special methods of personal data processing during elections" [2], as well as information security during e-voting, threats and mechanisms for their neutralization, in particular, by using blockchain technology [3].

Given the relevance of the research, the issue of e-voting and neutralization of security threats that potentially accompany the use of electronic vote detection systems has become the object of considerable attention from both Ukrainian and foreign scientists. As a rule, characterizing the existing research on e-voting in general, it is worth noting their interdisciplinary nature. After all, the study of e-voting and the existing threats to its implementation requires an understanding of both the technical features of the functioning of e-voting systems and the informational features of the modern world. In addition, given the fact that the institution of elections is a political category and an attribute of democracy, its professional assessment is impossible without the involvement of political science researchers in the analysis. Therefore, a qualitative and comprehensive study of e-voting should be interdisciplinary and, as a rule, involves the cooperation of scientists - representatives of various sciences and fields of knowledge.

Scientific researches devoted to the study of the problem of e-voting and the threats of its implementation can be conditionally divided into two groups. The first group includes scientific works that consider the problems of e-voting in general, or individual aspects of electronic expression of will. The second group includes the study of e-voting on the examples of specific foreign countries.

The first group includes, in particular, scientific articles devoted to such problems as: technical capabilities and security of e-voting [4]; the problem of e-voting security in smart communities [5]; mechanisms for ensuring the integrity of stored e-voting data [6]; assessment of the e-voting system based on recommendations of the Council of Europe [7], [8]; methods and algorithms for the performance of individual operational tasks related to the protection of the state information space [9]; the relationship between elections and democracy in general, as well as the influence of information and communication technologies on the effectiveness of election procedures and the level of democracy [10], [11]; peculiarities, problems and perspectives of the functioning of e-democracy and e-government [12], [13]; knowledge about cyber security and their influence on the use of information and communication technologies in general, and the use of social networks, in particular [14], etc.

The first group of sources also includes a number of scientific articles devoted to the problems of e-voting and the mechanisms of their solution. It is, in particular, about the analysis of such problems of e-voting and ways to solve them, as the use of blockchain technology during e-voting to strengthen the security of voting [15], [16]; use of an advanced e-voting protocol based on public key cryptography [17]; the problem of confidentiality of elections and paper verification of results during the use of e-voting [18], [19]; the problem of using the voter's ID card and fingerprint technology during e-voting [20], etc.

The second group of scientific works includes researches that relate to the specifics and problems of using e-voting during elections on the example of individual countries or regions. In this context, it is worth mentioning, first of all, Latin American researchers who most actively cover this issue on the example of Latin American countries. Among them, there are works that relate to the analysis of e-voting in a whole set of countries in the region, in particular, they contain an analysis of the threats and risks of existing e-voting systems in such Latin American countries as Brazil, Ecuador, and Colombia. The authors emphasize the need to take into account cultural, technological accessibility and social conditions in the studied countries when using e-voting [21]. It is also worth mentioning the research on e-voting systems in individual countries, such as Ecuador [22], Brazil [23] or Indonesia [24], [25].

In conclusion, we can state that the problem of e-voting is relevant and has become the subject of research by many scientists from various fields of science, especially in the context of the reliability and security of e-voting. However, modern science still lacks a comprehensive analysis of the threats of e-voting, as well as an expert assessment and calculation of the level of threats, which could be used as an indicator for making a decision on the implementation of e-voting or refusal to use it. In view of what has been said, the subject of our article is relevant and needs more thorough research.

3. Results and Discussion

3.1. Peculiarities of the expert survey on determining the level of threats to the implementation of e-voting

As already mentioned, this publication is an empirical continuation of the authors' previous article, in which they proposed their own methodology for calculating the level of threats that may be present in the event of the implementation of e-voting [1]. In order to calculate the level of threats to the implementation of e-voting using the example of Ukraine, the authors developed and conducted an anonymous expert survey using a Google form, which lasted 3 months - from April to June 2023. 50 experts who are citizens of Ukraine and represent 5 categories of respondents took part in the survey:

1. Scientists. The purpose of involving this category of experts was to obtain a scientific (theoretical) justification of the feasibility of introducing e-voting through the prism of existing security threats. The selection of this category of respondents was based on searching for keywords in the titles of their scientific publications in Google Academy. Such keywords were "electronic voting", "electronic elections", "electronic democracy", "electronic governance", "elections", "democracy". This category of respondents was the most numerous (given the importance of thorough scientific research as a condition for effective implementation of e-voting) and included 25 experts (50%).
2. Analyst experts. The involvement of this category of respondents was also aimed at obtaining a theoretical assessment of the feasibility of introducing e-voting and the presence of security threats. However, analyst experts, unlike scientists, in our opinion, to a greater extent assess the threats of e-voting in the context of the analysis of related socio-political processes in the state. The selection of this category of respondents took place according to a principle similar to that of scientists, but based on the analysis of their posts on social networks such as Facebook and Instagram. 6 analyst expert (12%) took part in the survey.
3. Public and political figures and politicians. This category of respondents was involved in an expert survey with the aim of analyzing the practical side of the implementation of e-voting, as well as taking into account the level of probability of making an authoritative decision regarding the implementation of e-voting in Ukraine. During the selection of this category of respondents, we tried to take into account the political preferences of the respondents (their affiliation to the government and the opposition), as well as the level of

their activity (national and local). In total, 8 respondents from this category (16%) took part in the expert survey.

4. Members of public organizations. This category of respondents was involved in an expert survey in order to obtain a comprehensive assessment of the feasibility of implementing e-voting from the standpoint of the level of democracy, non-involvement and taking into account practical experience. The criteria for selecting this category of respondents was the relevance of the sphere of activities of public organizations to democracy and elections. Among the organizations whose members took part in the expert survey were the Committee of Voters of Ukraine, the Public Network "OPORA" and the International Foundation for Electoral Systems (IFES). 6 members of the mentioned public organizations (12%) took part in the expert survey.
5. Information technology specialists. The involvement of this category of respondents was determined by the need to assess the technical possibilities for the implementation of e-voting and to determine the level of informational threats characteristic of the e-voting system. 5 IT specialists (10%) took part in the expert survey.

This selection and coverage of expert respondents enabled the authors to obtain answers to various aspects of the implementation of e-voting and security threats: theoretical significance and practical value of the implementation of e-voting; political aspects that will determine the likelihood of e-voting implementation and technical issues related to its use; the impact of e-voting on the level of democracy, etc.

Communication with the respondents took place through various communication channels, depending on the characteristics of the respondents and available contact information. The main communication channels were the following: e-mail; social networks Facebook and Instagram; Viber; Telegram; WhatsApp etc.

Table 1.
Peculiarities of conducting an expert survey on the identification of threats to the implementation of e-voting

Category of respondents	Criteria and method of selection	Purpose of engagement	Number of respondents	% of respondents
Scientists	Keyword search of titles of scientific publications in Google Academy	Comprehensive scientific (theoretical) assessment of the feasibility of implementing e-voting	25	50 %
Analyst experts	Keyword search of post titles on Facebook and Instagram	Theoretical assessment of the feasibility of implementing e-voting in the context of the analysis of social and political processes	6	12 %
Social and political figures and politicians	Belonging to the government or the opposition. Level of activity (national or regional)	Analysis of the practical side and assessment of the probability of implementing e-voting in Ukraine	8	16 %
Members of public organizations	The relevance of the sphere of activity of public organizations to democracy and elections	Comprehensive assessment of the feasibility of implementing e-voting from the standpoint of the level of democracy,	6	12 %

Information technology specialists	Activities related to information technologies and information security	non-involvement and taking into account practical experience Assessment of technical capabilities and determination of the level of information threats for the implementation of e-voting	5	10 %

3.2. Expert assessment of the expediency and features of the implementation of e-voting in Ukraine

An expert survey on threats to the implementation of e-voting can be conditionally divided into two parts. The first one is devoted to general questions regarding the expediency, prospects and features of the implementation of the e-voting system in general, and in Ukraine, in particular. The second part contains an expert assessment of the level of danger of each of the security threats that will potentially appear in the event of the implementation of e-voting. In general, the authors, while conducting an expert survey, set themselves the final goal - to calculate the level of threats to the implementation of e-voting in Ukraine, which will be the basis for justifying the final expediency or impracticality of using this type of voter expression of will.

The first part of the survey has an auxiliary character, and also partially performs a verification role in relation to the second part of the survey. The results of respondents' answers to the first (general) part of the survey will make it possible not only to tentatively check the validity of the formula proposed by the authors, but also to understand the expediency and validity of its individual components.

According to the results of the survey, 42% of respondents (21 responses) were against the implementation of e-voting in Ukraine. Instead, 58% (29 responses) expressed their support for the idea of implementation e-voting in Ukraine.

If analyzed in terms of categories of respondents, the highest level of support for the implementation of e-voting in Ukraine was observed among public and political figures and politicians - 75%. In our opinion, this can be explained by the lack of a comprehensive understanding of the threats of e-voting and political expediency (the idea of introducing e-voting is popular among voters, so it can contribute to obtaining image bonuses for those politicians who will promote this idea.

From the obtained result, it can be assumed that the high level of support among politicians for electronic voting in Ukraine can potentially contribute to its implementation in our country. After all, it is the politicians who will make the final legislative decision regarding the application / non-application of this type of expression of will in Ukraine.

Instead, representatives of public organizations turned out to be the biggest opponents of the idea of implementing e-voting in Ukraine - 66.6%. This, in our opinion, can be explained by the fact that the mentioned category of respondents is most thoroughly familiar with all the nuances and problems that accompany e-voting. More detailed information on the level of expert support for e-voting is presented in Table 2.

Table 2.
The level of experts' support for the idea of implementing e-voting in Ukraine

Category of respondents	Proponents of e-voting (number)	Proponents of e-voting (%)	Opponents of e-voting (number)	Opponents of e-voting (%)
Scientists	15	60 %	10	40 %

Analyst experts	4	66,6 %	2	33,3 %
Social and political figures and politicians	6	75 %	2	25 %
Members of public organizations	2	33,3 %	4	66,6 %
Information technology specialists	2	40 %	3	60 %
Total	29	58 %	21	42 %

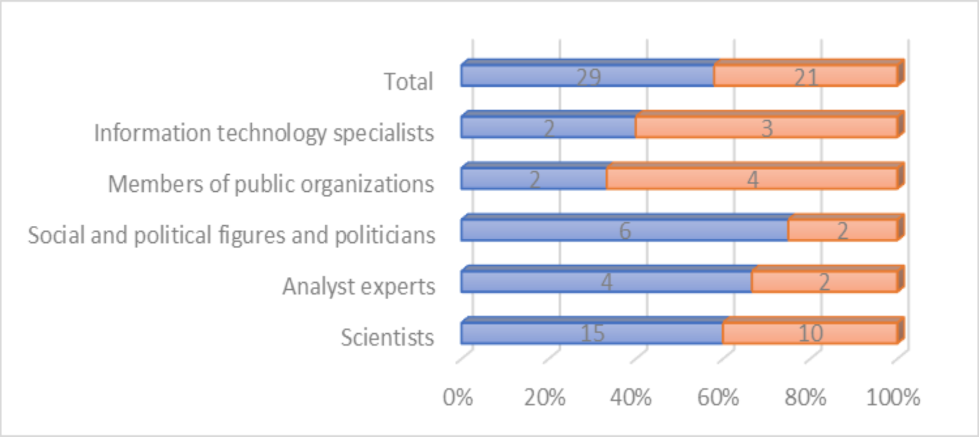

Figure 1: Distribution of experts

Among the 29 experts who supported the idea of introducing e-voting in Ukraine, the majority consider it expedient to introduce such a variant of e-voting as completely remote voting using a smartphone or laptop. 18 experts (62.1%) spoke in favor of this type of e-voting. Instead, 6 respondents (20.7%) supported the idea of voting on a special electronic machine that will be placed at the polling station. Another 5 experts (17.2%) consider it expedient to use the system of optical scanning of ballots in Ukraine.

Table 3.
Level of expert support for specific types of e-voting in Ukraine

Type of e-voting	Support level (quantity)	Support level (%)
Remote voting using a smartphone or laptop	18	62,1 %
Voting on a special electronic machine at the polling station	6	20,7 %
System of optical scanning of ballots	5	17,2 %
Total	29	100 %

In the context of the research of the problem of the implementation of e-voting in Ukraine, it was important for us to get an expert opinion on the time frame within which it is possible to use the e-voting system in Ukraine. The answers of 28 respondents (1 of the respondents who expressed support for e-voting did not answer this question) who supported the idea of introducing e-voting in Ukraine were distributed as follows: 5 (17.9%) respondents believe that e-voting in It can be implemented in Ukraine in 1-2 years; 11 respondents each (39.3%) supported the idea of introducing e-voting in Ukraine in a period of either 3-5 years or 6-10 years; 1 more respondent (3.6%) expressed the opinion that it will take more than 10 years to implement e-voting in Ukraine.

Table 4.
Time frames for the implementation of e-voting in Ukraine.

The period required for the implementation of e-voting in Ukraine	Respondents (number)	Respondents (%)
1-2 years	5	17,9 %
3-5 years	11	39,3 %
6-10 years	11	39,3 %
More than 10 years	1	3,5 %
Total	28	100 %

24 experts also answered questions about the shortcomings of e-voting, which stand in the way of its implementation in Ukraine. Respondents consider opportunities for correction of voting results by the Ukrainian authorities to be the biggest obstacle to the implementation of e-voting in Ukraine. This option was supported by 21 experts (87.5%). Experts consider the next most significant obstacle to be the presence of external threats that can nullify the result of willpower. 19 experts (79.2%) voted for this option. Interestingly, one of the experts additionally pointed out the possibility of cyber-attacks from the Russian Federation as one of the threats to e-voting. However, this threat, in our opinion, can be considered a component of external threats in general, which was one of the options proposed to experts as part of the survey of options.

Other disadvantages of e-voting, according to experts, are much less significant obstacles to the implementation of e-voting in Ukraine. In particular, the difficulty of understanding e-voting by Ukrainian voters was noted by 9 (37.5%) experts as an obstacle. Another 8 respondents (33.3%) consider the lack of necessary technological equipment an obstacle to the implementation of e-voting in Ukraine. 2 experts (8.3%) consider the excessive cost of this type of expression of will to be a problem for the use of e-voting in Ukraine.

Table 5.
Obstacles to the implementation of e-voting in Ukraine.

Obstacles to the implementation of e-voting in Ukraine	Respondents (number)	Respondents (%)
Possibilities for adjustment of voting results by the Ukrainian authorities	21	87,5 %
The presence of external threats that can neutralize the result of willpower	19	79,2 %
The difficulty of understanding e-voting by Ukrainian voters	9	37,5 %
Lack of necessary technological equipment	8	33,3 %
Excessive cost of e-voting	2	8,3 %
The possibility of cyber-attacks from the Russian Federation	1	4,2 %

In addition, 47 experts out of 50 answered questions about the potential benefits that the state and voters will receive from the implementation of e-voting in Ukraine. In particular, experts consider the speed of vote counting to be the greatest advantage of e-voting. This option was supported by 37 experts (78.7%). Another 34 respondents (72.3%) supported the idea that the e-voting system is convenient for voters. Other advantages of e-voting proposed by the authors have a slightly lower level of support among experts. In particular, 21 experts (44.7%) consider the advantage of e-voting to be increased turnout at elections; 17 experts (36.2%) – financial profitability of the e-voting system; 15 experts (31.9%) - positive impact of e-voting on ecology; 14 experts (29.8%) – reducing opportunities for falsifications and errors.

Table 6.
Advantages of the implementation of e-voting in Ukraine.

Advantages of the implementation of e-voting in Ukraine	Respondents (number)	Respondents (%)
Speed of vote counting	37	78,7 %
Convenience for voters	34	72,3 %
Increase in turnout at elections	21	44,7 %
Financial profitability	17	36,2 %
Positive impact on ecology	15	31,9 %
Reducing opportunities for falsification and errors	14	29,8 %

Experts were also able to offer their options for the advantages of e-voting. In particular, one of the experts attributed the prevention of falsifications to the advantages of e-voting, as well as the possibility for voters who cannot be at the polling station on the day of voting to express their will. Another expert noted that e-voting has advantages not only for voters, but also for the state. In addition, 3 experts believe that e-voting has no advantages at all. At the same time, 2 of them additionally justify their position: one sees that the reason for this is the criminal Ukrainian authorities; another justifies the lack of advantages of e-voting by the frequent changes in the electoral legislation in Ukraine.

3.3. Expert assessment of threats to e-voting

The second part of the expert survey aimed to find out the opinion of the respondents regarding the level of danger of each of the specific threats of e-voting, which were divided into 4 groups: threats to democracy; threats due to illegal interference; technical serviceability threats; threats to legitimacy.

According to the formula for calculating the level of e-voting threats developed by the authors [1], experts assessed the level of influence (danger) of each of the 13 e-voting threats in the range from 0 to 100, where 0 is the absence of e-voting danger, and 100 is the maximum level of e-voting danger. In addition, the experts had to establish coefficients for determining the threats of e-voting, which were calculated in the range from 0 to 1, where the greater the value of the coefficient, the more negative and significant was the impact of a specific threat on the implementation of e-voting. At the same time, within each of the specified groups of threats, the sum of the coefficients had to be 1.

Summary data on experts' assessment of the level of threats to e-voting are given in Table 6.

Table 7.
The results of the expert assessment of the threat level of e-voting in Ukraine.

Threats of e-voting: ET(EV)	Level of impact of threats (0-100)	Value of coefficients (0-1)
Threats to democracy Dem(EV)		
Violation of the principle of free elections: FE(EV)	54,4	0,23
Violation of the principle of equal elections: EE(EV)	45,34	0,18
Violation of the principle of direct elections: DE(EV)	49,36	0,2
Violation of the principle of secret voting: SB(EV)	48,64	0,17
Violation of the principle of public elections: PE(EV)	52,3	0,22
Threats due to illegal interference: Int(EV)		
Falsification of e-voting results by the election administration: FoR(EV)	49,5	0,24
Hacker attacks on the e-voting system: HA(EV)	57,58	0,29
The possibility of creating a transit server: FS(EV)	48,38	0,24
Vulnerability of voters' personal electronic devices:	47,2	0,23

SP(EV)		
Threats to technical serviceability: Tech(EV)		
The problem of uninterrupted functioning of the e-voting system: UT(EV)	43,6	0,53
Low quality of the Internet connection: IC(EV)	38,6	0,47
Threats to legitimacy: Leg(EV)		
Difficulty of e-voting: PB(EV)	36,64	0,46
Psychological barriers to the perception of e-voting: CS(EV)	40,56	0,54

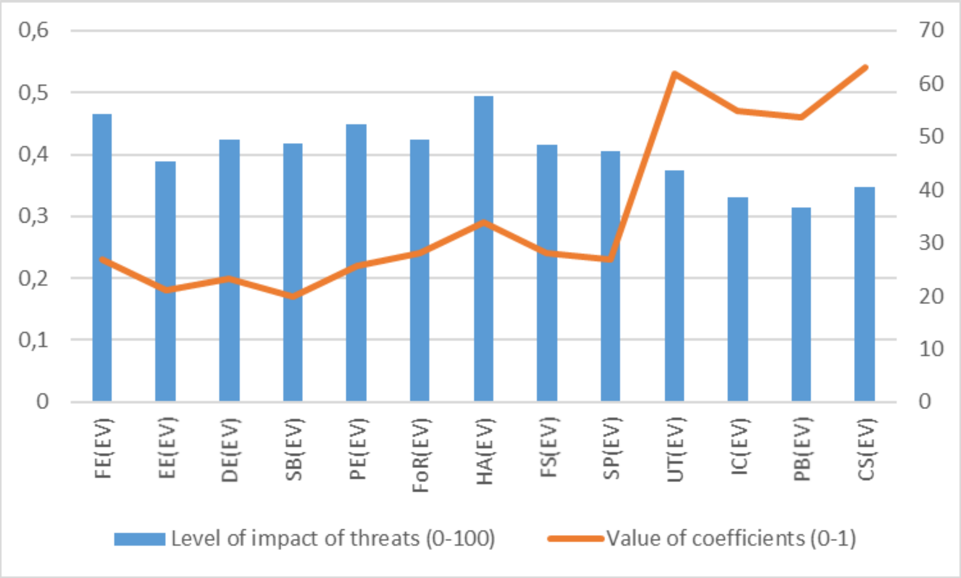

Figure 2: A graph comparing the dependence of the Level of impact of threats on the Value of coefficients

As we can see, according to experts, the most dangerous in the context of the implementation of e-voting in Ukraine are such threats as hacker attacks on the e-voting system, as well as violations of free and public elections. Instead, the least negative impact in the context of the use of e-voting in Ukraine, according to experts, will be the complexity of e-voting, the quality of the Internet connection and psychological barriers to the perception of e-voting.

3.4. Calculation of the threat level of e-voting in Ukraine

Having received the results of an expert survey on threats to the implementation of e-voting, based on the methodology developed in the previous publication [1], we will first calculate the level of each of the 4 groups of threats to e-voting, and then determine the general level of threats that could potentially appear in the context of implementation in Ukraine e-voting.

Level of threats to democracy:

Dem(EV) = (0,23x54,4+0,18x45,34+0,2x49,36+0,17x48,64+0,22x52,3)/100 = 0,5

Level of threats due to illegal interference:

Int(EV) = (0,24x49,5+0,29x57,58+0,24x48.38+0,23x47,2)/100 = 0,51

Level of threats regarding technical serviceability:

Tech(EV) = (0,53x43,6+0,47x38,6) / 100 = 0,41

Level of threats to legitimacy:

Leg(EV) = (0,46x35,64+0,54x40,56) / 100 = 0,38

Having determined the level of expert assessment of each of the groups of threats to e-voting, we can calculate the overall level of threat, which will be potentially characteristic of Ukraine in the event of the implementation of e-voting:

ET(EV) = (0,5+0,51+0,41+0,38)/4 = 0,45

In the previous publication, the authors established the gradation of the level of danger of e-voting, distinguishing 3 levels of security:

Level 1 (values from 0 to 0.2) – low threat of negative impact of e-voting. In this case, the implementation of e-voting is possible and will not cause any significant threats.

Level 2 (values from 0.21 to 0.5) is an average level of danger regarding the implementation of e-voting. In this case, the use of e-voting is possible provided that the most important shortcomings and threats are eliminated.

Level 3 (values from 0.51 to 1) – high level of danger, which makes it impossible to implement e-voting [1].

The aforementioned gradation of e-voting security levels will be applied to the analysis of the results of the expert survey. The characteristics of the level of threats in the context of the implementation of e-voting in Ukraine are depicted in more detail in Table 8.

Table 8.

Characteristics and consequences of calculating the level of threats to the implementation of e-voting in Ukraine

Threats of e-voting in Ukraine	Value	Threat level	Possible actions regarding the implementation of e-voting
Threats to democracy Dem(EV)	0,5	Average	Implementation is possible after elimination of key shortcomings and threats
Threats due to illegal interference: Int(EV)	0,51	High	Implementation is impossible
Threats to technical serviceability: Tech(EV)	0,41	Average	Implementation is possible after elimination of key shortcomings and threats
Threats to legitimacy: Leg(EV)	0,38	Average	Implementation is possible after elimination of key shortcomings and threats
Threats of e-voting in total: ET(EV)	0,45	Average	Implementation is possible after elimination of key shortcomings and threats

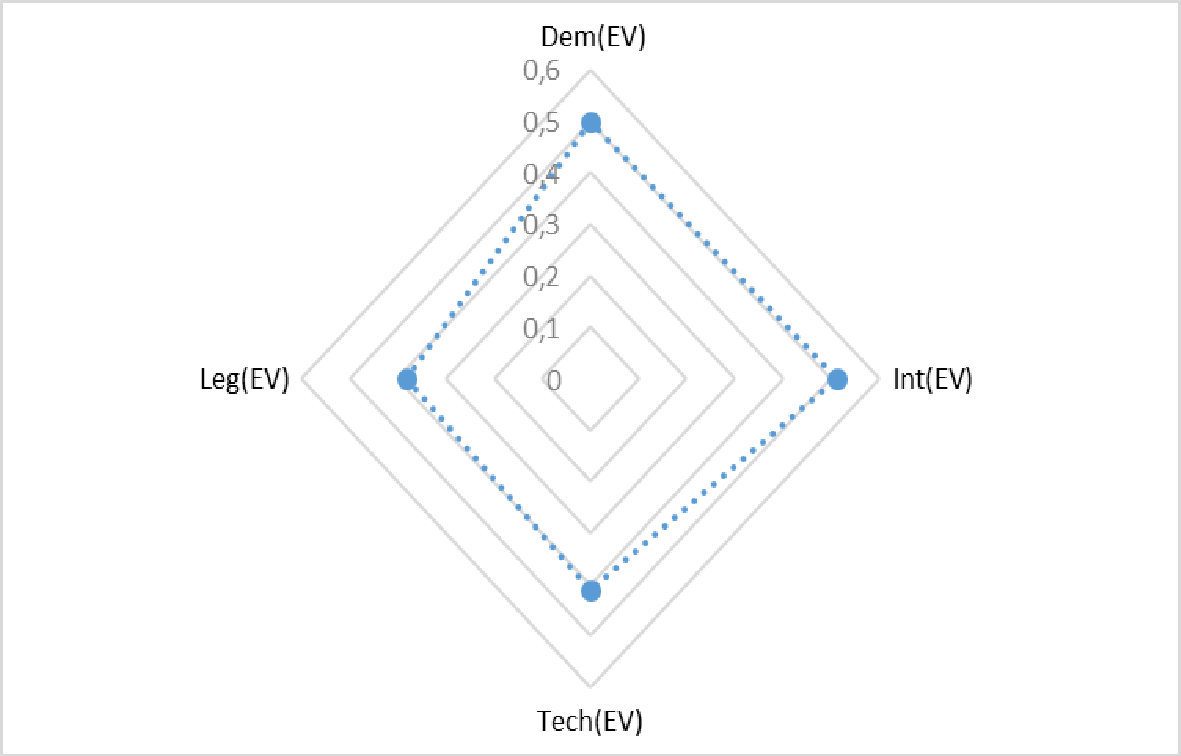

Figure 3: The results of an expert survey of threats to the implementation of e-voting

4. Conclusions

Summarizing, we can see that according to the results of an expert survey of threats to the implementation of e-voting in Ukraine, the situation regarding the use of e-voting is quite ambiguous. On the one hand, the general level of threats to e-voting is average, which does not prevent, according to the defined gradation, the possibility of its implementation in practice.

On the other hand, the general level of threats to the implementation of e-voting in Ukraine, although average, is close to the upper limit of its value. Moreover, one group of e-voting threats (threats to democracy) is at the extreme upper value of the medium level (0.5), while the other group of threats (threats due to illegal interference) reaches the minimum value (0.51) of the high level of e-voting threats.

The results of the experts' answers contained in the first (general) part of the study showed the relative validity of the methodology proposed by the authors for calculating the level of threats from the introduction of e-voting in Ukraine. Such results of the expert assessment of the level of threats to e-voting in Ukraine correlate to some extent with the general attitude of experts to the idea of introducing e-voting. The fact that 42% of experts opposed the implementation of e-voting in Ukraine, in our opinion, roughly corresponds to the upper limit of the average level of danger of the implementation of e-voting. Also, the obstacles identified by experts that stand in the way of the introduction of e-voting in Ukraine are to some extent correlated with the assessment of the level of threats from the introduction of voting using e-voting systems in our country.

The results of an expert calculation of the level of threats to the implementation of e-voting in Ukraine showed that the system of e-voting is quite dangerous in Ukrainian realities. Therefore, the implementation of e-voting in Ukraine is possible only after a thorough and comprehensive analysis of all existing threats, the development of effective mechanisms for their neutralization and the comprehensive application of these mechanisms in practice.

Since the first two groups of threats (threats to democracy and threats due to illegal interference) are the most threatening in the context of the implementation of e-voting in Ukraine, it can be assumed that the level of threats to the use of the e-voting system will become significantly lower in two cases. First, the level of threats to democracy will be greatly reduced by raising the political consciousness and culture of citizens and representatives of the authorities. In this case, the authorities will be less inclined to falsify the results of e-voting, and ordinary citizens will have more control over the actions of the authorities, reducing opportunities for abuse.

Secondly, the neutralization of the external threat from Russia will significantly reduce the opportunities for illegal interference in the process and results of e-voting. Therefore, the democratization of Ukrainian society and the victory over the Russian aggressor can significantly reduce the level of threats to the implementation of e-voting in Ukraine in the future.

5. References

[1] O. Markovets, M. Buchyn, Threats of the implementation of e-voting and methods of their neutralization, CEUR Workshop Proceedings 3296 (2022) 29-39. URL: https://ceur-ws.org/Vol-3296/paper3.pdf.

[2] 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. Medykovskyy (Eds.), Advances in Intelligent Systems and Computing IV. CSIT 2019, volum 1080 of the Advances in Intelligent Systems and Computing, Springer, Cham. https://doi.org/10.1007/978-3-030-33695-0_52.

[3] M. Buchyn, A. Helesh, 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), Lviv, Ukraine, 2021, pp. 266-269. doi: 10.1109/AICT52120.2021.9628971.

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

[5] V. Agate, M. Curaba, P. Ferraro, G. L. Re, M. Morana, Secure e-Voting in Smart Communities, CEUR Workshop Proceedings 2597 (2020) 1-11. URL: http://ceur-ws.org/Vol-2597/paper-01.pdf.

[6] A. Bhawiyuga, A. Basuki, 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.

[7] L. Panizo Alonso, M. Gascó, D. Y. Marcos del Blanco, J. Á. Hermida Alonso, J. Barrat, H. Aláiz Moreton, E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting, IEEE Transactions on Emerging Topics in Computing 9(1) (2021) 161–173. doi: 10.1109/TETC.2018.2881891.

[8] D. Y. Marcos del Blanco, D. Duenas-Cid, H. Aláiz Moretón, E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes, in: R. Krimmer et al. (Eds.), Electronic Voting, E-Vote-ID 2020, volume 12455 of Lecture Notes in Computer Science, Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-60347-2_10.

[9] A. Peleshchyshyn, V. Vus, O. Markovets, 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.

[10] N. Kersting, H. Baldersheim, Electronic Voting and Democracy. A Comparative Analysis. Palgrave Macmillan London, London, 2004. URL: https://link.springer.com/book/10.1057/9780230523531.

[11] M. Buchyn, Peculiarities and problems of measuring the level of democratic elections, Balkan Social Science Review 21 (2023) 105–125. doi: 10.46763/BSSR2321105b.

[12] A. Bayaga, M. Kyobe, J. Ophoff, Criticism of the role of trust in e-government services, in: 2020 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2020, pp. 1-6, doi: 10.1109/ICTAS47918.2020.233973.

[13] O. Tsebenko, N. Lukach, Y. Zavada, O. Stadnichenko, Model for Assessing Development of E-Government in Eastern Partnership Countries, Studies in Systems, Decision and Control. 421 (2022) 425-447.

[14] B. F. Alrashidi, A. M. Almuhana, 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, volume 1097 of Communications in Computer and Information Science, Springer International Publishing, Cham, 2019, pp. 57–68. doi: 10.1007/978-3-030-36365-9_5.

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

[16] A. Alshehri, G. Srivastava, W. Rajeh, M. Alrowaily, M. Almusali, Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain, Applied Sciences13 (2) 2023. doi: 10.3390/app13021096.

[17] H. M. Almimi, S. A. Shahin, M. Sh. Daoud, M. Al Fayoumi, Y. Ghadi, Enhanced E-Voting Protocol Based on Public Key Cryptography, in: 2019 International Arab Conference on Information Technology (ACIT), Al Ain, United Arab Emirates, 2019, pp. 218-221. doi: 10.1109/ACIT47987.2019.8990991.

[18] J. Budurushi, S. Stockhardt, M. Woide, M. Volkamer, Paper Audit Trails and Voters' Privacy Concerns, in: T. Tryfonas, I. Askoxylakis. (Eds.), Human Aspects of Information Security, Privacy, and Trust, HAS 2014, volume 8533 of Lecture Notes in Computer Science, Springer, Cham. doi: https://doi.org/10.1007/978-3-319-07620-1_35.

[19] A. B. Pedin, N. Siasi, Secure and Decentralized Anonymous E-Voting Scheme in: Proceedings of the ACM Southeast Conference, 2023, pp. 172-176. doi: 10.1145/3564746.3587107.

[20] R. K. Megalingam, G. Rudravaram, V. K. Devisetty, D. Asandi, S. S. Kotaprolu, V. V. Gedela, Voter ID Card and Fingerprint-Based E-voting System, in: S. Smys, V. E. Balas, R. Palanisamy (Eds.), Inventive Computation and Information Technologies, volume 336 of Lecture Notes in Networks and Systems, Springer, Singapore, 2022, pp. 89–105. doi: https://doi.org/10.1007/978-981-16-6723-7_8.

[21] S. M. T. Toapanta, I. F. M. Saá, F. G. M. Quimi, L. E. M. Gallegos, An Approach to Vulnerabilities, Threats and Risk in Voting Systems for Popular Elections in Latin America, ASTES Journal 4 (3) (2019) 106–116. doi: 10.25046/aj040315.

[22] S. M. T. Toapanta, M. A. A. Armijos, L. E. M. Gallegos, Analysis of Cybersecurity Models Suitable to Apply in an Electoral Process in Ecuador, in: Proceedings of the ACM International Conference Proceeding Series, Barcelona, Spain, 2020, pp. 84–90. doi: https://doi.org/10.1145/3375900.3375912.

[23] J. I. Pegorini, A. C. C. Souza, A. R. Ortoncelli, R. T. Pagno, N. C. Will, Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Tests, in: Proceedings of the ACM International Conference Proceeding Series, Athens, Greece, 2022, pp. 157–164. doi: 10.1145/3494193.3494301.

[24] R. Samihardjo, Murnawan, S. Lestari, E-Voting in Indonesia Election: Challenges and Opportunities, Review of International Geographical Education Online 11(6) (2021). URL: https://rigeo.org/submit-a-menuscript/index.php/submission/article/view/1594.

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