ONLINE VOTING AS AN ELEMENT OF CYBERSECURITY OF MEGACITIES

Ksenia A. Ivanova

University of Tyumen, Tyumen, Russia

The subject. The author explores the possibility of online voting during the elections from the perspective of urban security.

The purpose of the paper is to confirm or disprove hypothesis that introduction of online voting in the elections in large cities contributes to the growth of the electorate's confidence and reduction of absenteeism, but only if cybersecurity of metropolises is ensured. The methodology of the study includes general scientific methods (analysis, synthesis, description) and the method of comparative law.

The main results and scope of their application. The very essence of online voting involves the use of a dedicated Internet platform and digital devices. This method has many ad- vantages, including the ability to attract many people, the convenience and reliability of the whole process, as well as the automatic calculation of results. However, the issue of online voting in large cities directly affects the problem of ensuring their cybersecurity. Electronic voting can be subject to certain risks like any Internet procedure. Some of them have their own offline counterparts, such as the sale of votes. Others are unique to the digital envi- ronment, such as cyber violations and DDoS-attacks.

Conclusions. Electronic voting helps to solve the problem of low voters' turnout, unites communities, universities, companies and people. This new process must be protected from any potential threats to security.

An inefficient voter authentication procedure can adversely affect the reliability of the en- tire online voting system. Hacking the authentication system can lead to fraud and theft of data and votes. The blockchain system provides effective protection against such hacks and cyberattacks. It would be effective if it was possible to download a special anti-virus pro- gram from the election commission website to clean the user's computer from malicious content or at least check the presence of viral content. The license key of such a program may be valid only for the period of the elections. The decision against forcing an electronic vote for a particular candidate can be made by an online voting system that allows you to change your choice several times. We need well-thought-out training and advanced training programmes for state and municipal employees, including programmes for initial technical training, to reduce security risks. It is necessary to train possible users of the online voting system, since the security of a computer or smartphone, the absence of virus programs, as well as the timeliness of voting are in the area of responsibility of online voters.

Online voting may not be the only way a voter can express his or her will. It is always necessary to keep the possibility of classical voting by paper ballots.

31

1. Implementation of online voting

The use of modern technology in elections has become a trend worldwide. Elections are being modernized by incorporating digital technologies at various stages of the electoral process, including training of polling station staff, the compilation of voter lists, voter registration, and the distribution and counting of votes [1; 2; 3; 4; 5]. Knowledge of these developments can be used to determine what works and what does not in relation to their further implementation, and to answer pressing questions about the impact of technology on elections, for example, whether the adoption of online voting can increase the percentage of voter participation or strengthen voter confidence in elections [6, p. 65; 7, p. 46]. The development of electronic democracy also actualizes the problem of information security [8, p. 40]. Also, the issue of online voting in large cities directly affects the problem of ensuring their cybersecurity.

Internet voting is one of the trends of modernization of elections, which has become popular in Europe, Latin America and North America. At the local level, municipalities in Canada have been using online voting in more elections than anywhere else in the world since 2014 [9, p. 27].

2. Experiment on introduction of electronic voting in Moscow

On a similar trend responded and Russian law-making. On February 26, 2019, draft law No. 654402-7 "On conducting an experiment on the organization and implementation of remote electronic voting in the elections of deputies of the Moscow city Duma of the seventh convocation" was submitted to the State Duma of the Russian Federation, currently approved by deputies in the first reading. The bill received 23 responses from the state authorities of the Russian Federation – 10 from the legislative (representative) bodies and 13 from the executive authorities of the Russian Federation. All feedback is positive.

The main task of the bill is to create additional conditions for Muscovites to exercise active suffrage through the introduction of modern technologies in the electoral process. The voting procedures and mechanisms of objective consideration of Muscovites' opinion in the elections of deputies of the Moscow city Duma of the seventh convocation have been developed. The voter at the polling station of which the experiment will be held will have the right to choose the format of their participation in the elections: remote electronic voting or traditional voting.

To apply for participation in electronic voting, the voter must have full access to the subsystem "Personal account" of the Portal of state and municipal services of the city of Moscow, that is, have a confirmed account. The application may be submitted by the voter not earlier than 45 days and not later than three days before the day of voting. The application may be withdrawn by the voter within the same period.

In the near future, the capital's parliament is waiting for the introduction of the relevant city bill. At the same time, the task of the Moscow City Duma will be to detail the voting procedure within the framework defined by the draft Federal law, which allows for a unique experiment in remote electronic voting. It is planned to significantly strengthen the monitoring of the electronic voting. In addition to the Corps of observers of the Public chamber of Moscow and observers from candidates and political parties, the Moscow city election Committee will be given the opportunity to involve representatives of public organizations in the observation. It should be noted that the precinct election commissions in any case will print out "electronic ballots". This will make it possible, if necessary, to recalculate them manually .

Advantages of electronic voting are obvious: you can vote in any convenient place and at any convenient time on the day of voting [10, p. 10; 11, p. 34]. Voters who are not in Moscow or permanently reside abroad, as well as those who will not be able to visit the polling station on the day of voting, will be able to take part in the elections. In particular, this applies to people with disabilities [12, p. 81]. For remote voting, you only need a mobile device.

In addition, electronic voting will increase the number of those wishing to vote – at the expense of active Internet users [13, p. 5]. And most importantly, the results of the experiment will help to identify key areas for further work to improve the electoral legislation and the introduction of modern

technologies in the electoral process.

3. Risks and opportunities of online voting for the safety of cities

Due to the obvious advantages, as well as the development of digital society, it can be predicted that the introduction of electronic voting will soon be widespread [14, p. 40]. Therefore, it is important to study the world experience, as well as try to foresee and prevent possible risks that such introduction of technologies may entail for the safety of cities.

A similar issue can be seen in Ontario, Canada. In 2003, a dozen Ontario municipalities introduced remote e-voting [7, p. 45], and it has since become more popular: in the provincial municipal elections to be held this October, 194 of the 444 municipalities will allow voters to vote remotely - and in 80% of these municipalities, e-voting will be the only option available .

E-voting also allows municipalities to have large voting Windows. For example, in Stratford, 24-hour voting will take place from 12 to 22 October.

Another advantage of online voting is that it requires less cost to attract employees than traditional voting. In Canada, there has long been a tendency to reduce those who want to work in the elections as an organizer or observer. Municipalities do not have sufficient funds to attract high-paying employees, and the work is temporary. The introduction of electronic voting can solve this problem.

Users of this technical capability also respond positively. Data collected in the framework of the project "Voting via the Internet" and published in the report of the Centre for electronic democracy , showed that of the 33 000 people, 95 percent of voters on the Internet was satisfied with this process. Only 68 percent of those who voted in the traditional way felt the same way.

However, in addition to the undoubted advantages, there are certain risks of widespread introduction of online voting. However, concerns can be expressed about the pace at which cities are adopting new technologies, especially if e-voting is the only method of voting.

A significant change in the future of the electoral composition can be identified as possible risks. According to the results of a large-scale study conducted in 2016 , the center for electronic democracy suggests that the method of electronic voting is popular among people with higher digital literacy, higher education and higher incomes than the so-called "paper voters".

Accordingly, in those cities, especially in small ones, where electronic voting becomes the only way, there is an actual exclusion of part of the electorate from the electoral pool, while this part of the population is poorer and less educated.

There is therefore a risk that the preferences of urban policies vary considerably in accordance with these varying characteristics. The elimination of paper bulletins can provide a systematic institutional advantage to politicians of a certain ideology, that is, the actual establishment of meritocracy.

Also, despite the blockchain technology, there is still a risk of online voting security.

Dean Smith, President of Intelivote Systems Inc. – a company working with a majority of Ontario municipalities offering online voting in elections – recognizes that electronic voting carries certain risks. According to him, at each election someone tries to manipulate the system, and not always hackers. For example, some ordinary people try to vote twice.

It is also possible interruptions in service, which handle can be even harder than cyberattacks and cyberfraud. Their sources are difficult to predict and prevent – for example, bad weather or a sudden surge in democratic activity. (On the final day of online voting, voters contributed to a significant slowdown in the Stratford system in 2010, as most of them decided to vote in the last remaining hours.)

It is for security reasons that the Guelph city Council (Ontario, Canada) refused to vote online in the municipal elections in 2018. According to the city Council, the results of online voting in 2014 showed that security significantly increases the cost of elections, and at the same time, does not guarantee the integrity of such elections.

Vulnerability to cyberattacks was also identified in such cities of the Ontario region, Canada as Pickering, Cambridge, Oshawa, Ottawa-Carlton. They also question the possibility of online voting in the upcoming municipal elections in

October 2018.

In my view, since online voting is fairly new, the Ontario municipal elections showed that many cities were simply not sufficiently prepared for this form of election. Based on the previous surveys it was revealed that city officials know how to respond to such threats as tornadoes or floods, none of the interviewed local communities of Ontario has no plan in case the elections will be disrupted because of electronic violations . The problem is compounded by the fact that some municipalities do not even know where the servers they use for online voting are located.

In my view, since online voting is fairly new, the Ontario municipal elections showed that many cities were not sufficiently prepared for this form of election. Based on the previous surveys it was revealed that city officials know how to respond to such threats as tornadoes or floods, none of the interviewed local communities of Ontario has no plan in case the elections will be disrupted because of electronic violations. The problem is compounded by the fact that some municipalities do not even know where the servers they use for online voting are located.

Another risk of online voting is the possibility of compulsion to participate in it. Such a risk arises because the voter does not come personally to the polling station, therefore, it is impossible to check in what conditions he makes his choice and who influences him at this moment.

In addition, there is a risk of tracking. Electronic voting may allow entities to identify threats to participants via their devices or IP addresses that compromises anonymity of people. It is crucial to address this issue on any online voting platform, as the likely disclosure of identity may even endanger a person's life.

4. Conclusions on the possibilities of online voting and prevention of risks to the safety of cities

It is obvious that electronic voting is the future in the world of accelerated technology development. That is why it is necessary for governments to establish common voluntary standards and guidelines for electronic voting

throughout the country. Elections are the cornerstone of democracy, so "patchwork" legal regulation here, in my opinion, is impossible.

Therefore, the CEC of the Russian Federation, unlike Canada, took the right step to conduct the experiment in Moscow by adopting a framework Federal law establishing the basic principles and the procedure for online voting. At the same time, the subjects of the Russian Federation are given the opportunity to take into account local specifics by adopting regional acts.

An inefficient voter authentication procedure can adversely affect the reliability of the entire online voting system. Numerous security incidents involving electronic banking and online payments have shown that hacking into the authentication system can lead to fraud and data theft. Online voters may be exposed to this type of risk if their devices are infected with malicious code that steals login credentials, or if they fall under a phishing Scam simulating a registration or voting form. Both scenarios can lead to stealing of votes. Regardless of the approach used to authenticate and identify the user, it must rely on robust security mechanisms.

In this case, the blockchain system provides effective protection against such hacks and cyberattacks. However, it would be effective if it was possible to download a special anti-virus program from the website of the CEC of the Russian Federation, which allows to clean the user's computer from malicious content or at least check the presence of viral content. The license key of such a program may be valid only for the period of the elections.

Forcing a vote can be another problem. It is difficult to understand the real intentions of a person who votes remotely using his smartphone. In this case, the solution may be an online voting system that allows you to change your choice several times. The last choice of the voter will be considered final. This approach can also solve the problem of selling votes. Trading signs of a potential sale of votes completely disappear if a person easily changes his choice.

Also, the need for effective training of city officials organising the vote, including online. Most of the risks faced by Canadian cities arose from

either a misperception by employees about online voting or a lack of information. To prevent this from happening, we need verified training and advanced training programs for state and municipal employees, including programs for initial technical training.

The mechanism of response in the event of an unforeseen situation, such as a system crash or cyberattack should be carefully thought out, it should be clear and familiar to everyone responsible for conducting online voting.

In addition, it is necessary to train possible users of the online voting system, since the security of a computer or smartphone, the absence of virus programs, as well as the timeliness of voting are in the area of responsibility of online voters. Therefore, the increase of legal awareness and conscious attitude in elections is especially necessary in the world of high technology, where a person's personality is hidden behind the lines of a computer program. Users who do not have sufficient computer skills may be given the opportunity to learn.

And of course, online voting may not be the only opportunity for voters to Express their will. It is always necessary to keep the possibility of classical voting with the help of ballots.

The world is changing, and the number of Internet users is constantly growing. More and more people prefer to do business, communicate and solve their daily tasks on the Internet. Electronic voting is the next logical step in the evolution of the traditional voting process. This helps to address the problem of low voter turnout and ensures that people who are unable to vote offline for any reason are still able to Express their opinions. Electronic voting brings together communities, universities, companies and people. It remains for us to protect this new process from any potential threats so that the world can take full advantage of it.

35

REFERENCES

1. Antonov Ya.V. E-democracy as a constitutional and legal phenomenon. *Gosudarstvennaya vlast' i mestnoe samoupravlenie = State power and local self-government*, 2016, no. 11, pp. 13–17. (In Russ.).

2. Tarasov A.M. Information technologies and their application in the electoral process. *Vestnik Akademii prava i upravleniya = Bulletin of the Academy of law and management*, 2010, no. 19, pp. 23–52. (In Russ.).

3. Churov V.E. Development of electronic technologies in the electoral system of the Russian Federation, in: *Pravo tsifrovoi administratsii v Rossii i vo Frantsii,* collection of scientific materials of the Russian-French international conference, February 27–28, 2013. Moscow, the Institute of State and Law of the RAS Publ., Kanon+ Publ., Reabili-tatsiya Publ., 2014, pp. 15–20. (In Russ.).

4. Moshkina (Pogodina) N.A. The role of information technologies in attracting young people to participate in the electoral process. *Gosudarstvennaya vlast' i mestnoe samoupravlenie = State power and local self-government*, 2013, no. 1, pp. 26–29. (In Russ.).

5. Skokova Yu.A. Transformation of civil practice for election observation in Russia. *Grazhdanskoe obshchestvo v Rossii i za rubezhom = Civil society in Russia and abroad*, 2013, no. 2, pp. 15–20. (In Russ.).

6. Shul'ga-Morskaya T.V. Electronic voting: experience and prospects of Switzerland and Russia. *Advokat = Lawyer*, 2013, no. 3, pp. 57–72. (In Russ.).

7. Chebotarev V.E., Konovalova E.I. The use of electronic means of voting during election campaigns: the expe-rience of foreign countries and Russia. *Yuridicheskii mir = Judicial world*, 2012, no. 8, pp. 44–47. (In Russ.).

8. Chebotareva A.A. Information security of personality in the global information society: theoretical and legal aspects. *Rossiiskaya yustitsiya = Russian justice,* 2016, no. 8, pp. 39–42. (In Russ.).

9. Ahmatova A.A. E-government: a new world for a new "I". *Administrativnoe pravo = Administrative law*, 2011, no. 3, pp. 25–28. (In Russ.).

10. Kireeva E.Yu. Transformation of mechanisms of participation of civil society institutions in the renewal of power. *Konstitutsionnoe i munitsipal'noe pravo = Constitutional and municipal law*, 2016, no. 1, pp. 9–12. (In Russ.).

11. Kuryachaya M.M. Electronic voting as a stage of development of direct democracy. *Konstitutsionnoe i mu-nitsipal'noe pravo = Constitutional and municipal law*, 2017, no. 11, pp. 31–35. (In Russ.).

12. Sovetnikov I.V. *Abuse of rights in the electoral process*, Cand. Diss. Moscow, 2006. 195 p. (In Russ.).

13. Antonov Ya.V. Political and legal problems of development of mechanisms of electronic democracy in the Russian Federation. *Rossiiskaya yustitsiya = Russian justice*, 2017, no. 7, pp. 5–8. (In Russ.).

14. Gornostaeva E.O. Foreign experience of electronic voting in elections. *Konstitutsionnoe i munitsipal'noe pravo = Constitutional and municipal law*, 2008, no. 21, pp. 39–40. (In Russ.).

INFORMATION ABOUT AUTHOR

Ksenia A. Ivanova – PhD in Law, Associate Professor, Constitutional and Municipal Law Department
University of Tyumen
6, Volodarskogo ul., Tyumen, 625003, Russia
e-mail: k.a.ivanova@utmn.ru
RSCI SPIN-код: 6610-9218; AuthorID: 695216