Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (31-44)

Hacker Attacks on Electronic Election and Vote Counting Systems: Estimation of Damages and Methods of Protection

Brunela Kullolli[1]

Abstract

The purpose of this study is to find the most effective and cost-efficient ways to improve the security and stability of electronic election and vote counting systems, as well as to identify the main targets of intruders and vulnerabilities of the system to prevent possible attacks. This paper describes the main types and of hacker attacks and their mechanism, assesses the consequences of damage to the structures of electronic elections in the United States, France, Germany, Northern Macedonia, and Indonesia. The vulnerabilities of electronic election systems were investigated and the technology for their detection during development and testing was provided. Recommendations were given on the implementation of preventive work to reduce the risks of hacker attacks. The study explained the motives of the crimes committed in the cyberspace of electronic election systems.

Keywords: Cybersecurity; Cyber Defence; Computer Forensics; Remote Electronic Voting; Internet Voting

Introduction

At the local government elections in October 2005, Estonia introduced the possibility of electronic voting in the world. Then, 9,317 voters used the new method of participation in the elections. This amounted to about 2% of their total number, which at that time was a fairly high indicator (Madise & Martens, 2006). Over time, electronic voting began to be actively used in other states. However, such a system is not exceptionally reliable and has been subjected to repeated hacker attacks. The relevance of this study lies in the investigation of the electronic voting system, as well as its advantages and disadvantages. The originality of this paper lies in the search for new ways to solve the problem of cyberattacks on electronic voting systems.

To estimate the degree of protection of the electronic election system, in 2019, participants of Def Con in Las Vegas, USA, a major annual conference of hackers, were invited to test their skills on voting machines to identify weaknesses that can be exploited by attackers. In a matter of minutes, the devices were hacked, and hackers turned them into game consoles (Derysh, 2019; Savchenko, 2022; Metelskyi & Kravchuk, 2023).

[1] Doctor of Law, Department of Justice, Aleksander Moisiu University of Durres, Durres, Albania. kullollibrunela4@gmail.com

When considering the issues of low reliability of electronic election systems and the problem of the human factor, one should cite the case when an error in the counting of votes almost brought victory to the Labour Party in the elections in Scotland in 2007. Due to incorrect counting in a computer file by tired workers, labourists could win the parliamentary elections in Scotland (Hencke & Johnson, 2007).

There have been more serious incidents in the history of electronic voting. The US Senate Intelligence Committee claims that electronic voting systems in all 50 states were subjected to a large-scale attack by Russia in the 2016 presidential election (Sanger & Edmondson, 2019). To prevent interference in the structure of electronic voting, it is necessary to introduce new security technologies.

Article by N. Stedmon (2020) on the investigation of the impact of cybersecurity threats on the US elections in 2020 examines blockchain technology, which is used in electronic voting systems. As a result, it was found that blockchain technology allows for solving some problems of electoral systems (Teplytskyi, 2021). The author also concluded that the cybersecurity measures taken in the US elections were sufficient to prevent attackers from influencing the results and the voting process.

The existing electronic voting schemes work using various encryption algorithms. This is problematic since the administrator of the central server of the accounting chamber has all the powers. The administrator cannot always be trusted, and the contents of the ballot can be forged or falsified. To solve these problems, Korean researchers C.H. Roh and I.Y. Lee (2020) also suggest using blockchain technology for electronic voting. The authors claim that this will ensure the reliability and integrity of the data. In this paper, the authors propose an electronic voting system that will increase reliability by guaranteeing secret voting. The described system can meet all the security requirements of the system and improves the performance of the algorithm in comparison with existing analogues. U. Jafar et al. (2021) from the National University of Malaysia also raised this issue. It was found that blockchain systems can increase the speed of the operation. However, weaknesses were found that need to be improved in the future.

This system is considered more deeply by researchers from the Sorbonne University in the article by A. Benabdallah et al. (2022), which is an overview of the most indicative solutions for electronic voting based on blockchain technology. The authors suggest various solutions utilising the technology, for instance, creating a voting application using blockchain on smartphones.

There is a technology of quantum key distribution, which is considered in the joint work of Indian and American researchers S. Gupta et al. (2021). The paper describes the architecture, design, and limitations of a voting system with quantum key distribution and blockchain protection. The authors of the study examined the weaknesses of such a structure and developed a special approach that will improve the security of the electronic voting system.

The publications described above do not consider all possible scenarios of hacker attacks and which vulnerabilities are used for hacking. Cases of attacks on electronic voting systems and ways to prevent them need to be considered more scrupulously. The purpose of this study is to find the most effective and affordable technologies and ways to improve the security of electronic election systems. To figure out the possible targets of the attackers in the future, it is necessary to analyse the damage caused by hacker attacks in the history of electronic elections. It is required to identify vulnerabilities in the system of electronic election and vote counting systems, to make recommendations on improving the reliability of systems.

Materials and methods

The methodology of this study is based on the analysis and comparison of existing cybersecurity technologies described in modern publications in the field of electronic election systems and vote counting. The main types of attacks are highlighted, the mechanism of their action is described, and the degree of damage to the structures of remote elections is estimated on the example of many countries. The motives of the crimes committed in cyberspace are explained. Recommendations on preventive maintenance to reduce the risks of hacking are provided. The most effective and available methods of protection are analysed and compared.

The first stage of this study provides a general overview of the functioning of electronic election systems. Their main advantages over the usual format of elections with paper ballots are highlighted. These include expanding the coverage of voters among the population, reducing the costs of conducting an election campaign, reducing the risks of human interference and election fraud during vote processing, and summing up. The authors explained the structure of electronic voting in a simplified form. They also considered the available forms of electronic voting systems and ways of their operation. The main disadvantages of the remote format are indicated. This includes the lack of monitoring of the voting process by election commission staff, the unreliability of the software of voters’ devices.

The second stage of the study provides the methods of attacking modern computer systems and ways to prevent them. The principle of denial of service (DoS) and distributed denial of service (DDoS) attacks in electronic voting systems are explained in detail. Such vulnerabilities in electronic election systems as injections, broken authentication, incorrect security settings, disclosure of confidential data, cross-site scripting, unsafe deserialization are described (Cherniha & Serov, 2006). The authors propose ways to eliminate said vulnerabilities, including scanning technologies for vulnerabilities in electronic voting systems during development and testing. The paper also presents cases of hacking or their attempts during voting in different countries of the world, citing as an example the presidential and parliamentary elections in Ukraine in 2014 and 2019, the US presidential elections in 2016, the 2018 midterm elections in Georgia, USA, regional elections in Indonesia of the same year. The study estimated the consequences of the damage caused in cases of a successful attack. Approaches to improving software security are proposed and a comparative characteristic of the described methods is provided. Furthermore, the main goals of intruders in the electronic voting system are described.

The third stage considers the efficiency of blockchain since this it is one of the most well-known currently applied technology. The authors give a brief description of the functioning of this structure. This description elaborates on the problems of electronic election systems that were solved precisely because of this technology, and other advantages are presented in more detail. The vulnerabilities of the blockchain system and possible ways of hacker attacks are highlighted.

The fourth stage of the study presents recent publications, where the authors give general recommendations on reducing the risks of election fraud and other violations during the election campaign, perfecting the user interface to improve usability, improving security and secrecy standards, and managing cybersecurity in electronic election systems and vote counting.

Results and Discussion

Electronic voting has many advantages. This enables people with disabilities to vote independently, easily, and secretly (e.g., audio ballots for visually impaired voters), allows voters to cast their vote remotely regardless of location, promotes faster counting of votes and announcement of final election results, and introduces multilingual ballots. This must ensure long-term economic efficiency by saving time for employees of polling stations, postal fees, and printing costs. On the one hand, while reducing human intervention, electronic voting helps prevent fraud at polling stations during vote processing and summing up. In a simplified form, the electronic voting system is divided into the following subsystems: voter registration, documentation, verification, voter management, voting, processing of election results, and summary. All operations will be sent to the central database. Both the database and the application are hosted on the same server (Nwankwo & Njoku, 2020).

Electronic voting can take various forms. There is remote voting using personal devices (smartphones, laptops) and at polling stations using special voting machines. Ballots can be transmitted via isolated computer networks, via the Internet, or telephones (Adanbekova et al., 2022). The most usual form is online voting. The voter (respondent) receives an electronic ballot on the corresponding website (a form for voting on possible answers) and votes, indicating their answer option. Voting through an electronic ballot is confirmed at the expense of the user's registration data (Tatsyi et al., 2010; Hratsiotova et al., 2020). They can be as follows: an identification network address and parameters of the device and voting software, a private digital signature, and fingerprints (Mazakov et al., 2020; Aliaskar et al., 2022).

The organisation of a remote form using personal devices is quite complicated. The voter's devices cannot always be trusted, as many of them contain malicious software. Furthermore, election commission employees cannot monitor and control the process of remote voting, since a voter can cast their vote at home or in any other place. The development and implementation of a tamper-proof remote voting system is a challenging task. Voting at polling stations using special electronic machines eliminates these previously mentioned disadvantages. Such a machine must have a reliable operating system and anti-hacking mechanisms.

There are three main ways in which modern computer systems are most often attacked: user error, configuration error, or software error. An example of a user error is a malicious link in an email that a person may inadvertently open. The electronic voting system should be designed in such a way that if a user makes a mistake, such a vote will not be counted. Configuration errors are more difficult to handle. As a measure to counter manipulation, it is necessary to introduce a requirement that the configuration is approved by at least two officials responsible for voting. One official responsible for the conduct of voting should not be able to rig votes. They can also be eliminated by training employees of the accounting chamber, as well as automatic and manual testing of the system.

Software bugs are often difficult to detect and prevent. This can lead to dire consequences, which are used by attackers to violate the integrity of the entire system. In general, there are three approaches to improving software security. The first is to improve software development tools up to formal code verification. The second approach is to ensure the security of supply (i.e., reliable software vendors, open-source software). The third involves compliance with the principles of development: proper testing and design of a stable system that can ensure the continuation of work in case of any errors that occur. All these measures reduce the probability of software failures, but they are expensive (Bradshaw et al., 2022).

The main targets of hacker attacks on electronic voting systems are the procedures for voter registration, voting, counting, transmission, and aggregation of results. This also includes websites for publishing results and other online services, corporate and personal accounts, communication systems. Hacker attacks on the electoral process can be general or selective. Thus, participants in the electoral process may involuntarily become victims or become predetermined targets of hackers. General attacks do not require much complexity. This type of attack can be carried out by attackers with limited resources. These include DoS attacks, hacking of websites, as well as malware and ransomware attacks. The principle of the DoS attack is to fill Internet resources with an enormous number of requests (Maraj et al., 2017; Abdymanapov et al., 2021). As a result, the maintenance of websites slows down or becomes unavailable for use. General attacks do not penetrate the system, do not cause data changes, and cannot gain access to confidential information of the polling station. The damage is caused by the fact that systems damaged by attacks become inoperable. DoS attacks can also be directed at communication systems to complicate data transmission or completely disrupt communication between users. For instance, they may block or overload mobile phones, communication channels, and devices of key election commission employees. During the 2018 regional elections in Indonesia, attempts were made to hack the web page of the election results of the General Election Commission. The Telegram and WhatsApp accounts of leading election administration officials were also attacked through weaknesses in messenger systems. The hackers' main goal was to disrupt the electoral process.

A DoS attack can be stopped fairly quickly if it comes from a single source. Blocking DDoS attacks is more time-consuming because they come from many sources at once. To resist such attacks, powerful computing resources are required. DDoS attacks are relatively simple to implement. They are perhaps the most common type of cyberattack. This form of attack is common for election commissions. This type of attack was used during the presidential and parliamentary elections in Ukraine in 2014. The attackers interfered with the transmission of the results by the district election commissions. DDoS attacks, malware, and phishing attacks were carried out. A few weeks before the presidential elections in 2019, such a DDoS attack was launched against candidates and the Central Election Commission. However, the attackers were unable to falsify the election results since the election commission had installed proper protective mechanisms (Mentukh & Shevchuk, 2023; Sopilko, I., & Rapatska, 2023).

Hacking websites is associated with damage to their appearance and content. Changing the appearance is usually aimed at damaging the image of candidates. Such attacks may be aimed at publishing false information or changing election results. They use weaknesses in the site code to gain access to the server, but most do not affect the information system and internal data of the institution under attack. The hacking of election websites leads to the leakage of personal data when disclosing voter registers. About a month before the 2019 presidential elections in Northern Macedonia, the most valuable information and communication systems of the State Election Commission were malfunctioning. As a result, publications of minutes of meetings, instructions, decisions, voter data, and registers of complaints were distributed. According to the election commission, the systems affected by the GEFEST 3.0 malware included file servers and email servers. This also affected the availability of the voter register and the database of civil servants used to appoint election commissions (Borysova et al., 2019; Van der Staak & Wolf, 2019).

As an example of a violation in the counting of votes, electronic voting systems with direct recording can be cited, which demonstrates their vulnerability to hacking and malfunctions. Despite the growing evidence of the system's unsuitability, some US states continue to use them in local government elections, as well as state and federal elections. Using nonparametric statistics, evidence was found that hacker attacks in the US state of Georgia during the midterm elections in 2018 forced the electronic system not to register a substantial number of votes. The indicators of understatement of votes were associated with ethnicity, and in those precincts where the percentage of black voters was higher (Ottoboni & Stark, 2019; Shariy, 2019). In the same state, a security specialist discovered a vulnerability, as a result of which it became possible to download and potentially change the register of 6.7 million voters on an unsecured election server, instructions and passwords for employees of polling stations to log in to systems used for voter verification (Lomzhets et al., 2021; Zetter, 2018).

Since the Internet is a global network, attacks can arise from anywhere, and their sources are often hidden. Even carefully monitored systems with updated software and the use of security tools (e.g., antivirus software) may be vulnerable. Attackers can find weaknesses in software and systems that will facilitate unauthorised access, reading and changing data, and blocking access to authorised users. To estimate the consequences of such interference, one of the US intelligence reports on the 2016 presidential election can be cited as an example.

According to the report, a large volume of confidential e-mail messages was stolen from the Democratic National Committee and then published through WikiLeaks, which, according to the US intelligence community, was orchestrated by the Russian military intelligence agency Main Intelligence Directorate (GRU). Some messages were so confidential to high-ranking party personnel that they led to resignations, recriminations between supporters of candidates H. Clinton and B. Sanders, and negative mentions in the media. The same group of hackers penetrated the systems of the Illinois Election Commission, stealing information about 500,000 voters, including names, addresses (Nakashima & Harris, 2018; Vilks & Bergmanis, 2018).

During the 2016 elections in France and Germany, attackers released information such as internal emails stolen from political parties and candidates to damage their credibility (Mueller, 2019; Limba et al., 2017). The Hiscox Cyber Readiness Report (2018) notes that attackers use such weak links in the security system as injections, broken authentication, disclosure of confidential data, Extensible Markup Language (XML) External Entity (XXE) (a web vulnerability in the security system that allows an attacker to interfere with the processing of XML data by an application). This also includes merging, incorrect configuration of the security system, cross-site scripting (XSS) – a web vulnerability that allows an attacker to compromise user interaction with an unprotected application, monitoring, unsafe deserialization, use of components with known vulnerabilities, and insufficient logging (Okrój & Jatkiewicz, 2023). Next, the authors propose taking a closer look at some of them.

Attackers can use broken authentication for unauthorised access to functionality and data, such as access to other users, viewing confidential documents, and changing user data and access rights (Abba et al., 2017; Sϕhoel et al., 2018). Incorrect security settings are the most common issue. This is usually the result of an insecure default configuration, incomplete or special configuration, configuration errors in the HyperText Transfer Protocol (HTTP) header, and error messages containing confidential information (Jefferson, 2019; Srokosz et al., 2018). Cross-site scripting can occur when an application inserts fake data into a web page without verification, or updates web pages using data entered through the browser. XSS is used by attackers to execute scripts in the victim's browsers that can intercept access, remove web pages or redirect users to malicious sites (Khanpara et al., 2022; Wang et al., 2018). Unsafe deserialization causes remote code execution. It can be used to carry out the following types of attacks: replay attacks, injection attacks, and privilege escalation attacks (Leite & Albuquerque, 2018).

To prevent such attacks, Zed Attack Proxy (ZAP) technology is used. This tool can automatically scan for vulnerabilities in web applications when they are being developed and tested. ZAP works on the principle as if an attacker had entered the system from the outside to obtain data or to carry out an attack (Kurniawan et al., 2017; Shrivastava et al., 2021). The structure of Arachni technology is similar to ZAP and can also be used to identify vulnerabilities in web pages. Therewith, ZAP works more efficiently than Arachni, as discovered by Indonesian researchers I. Riadi and P. Raharja (2019) from the Faculty of Information Systems of Ahmad Dahlan University. Notably, these programs are free, which may partially solve the issue of the excessive cost of preventing cyberattacks.

Another important concept is “cyber hygiene”. This includes the degree of training and awareness of users on how to support system operability and online security, and the originality of the organisation’s technologies, including regular testing and maintenance. The term also includes security principles to combat developing cyber threats, verification, and control of personnel with access to confidential systems to reduce the risk of internal attacks (Omurzakova et al., 2022). The Permanent Election Commission of Romania has implemented cyber hygiene training programs for political parties to protect internal information, as well as data that the commission gives to parties (Estehghari & Desmedt, 2010; Van der Staak & Wolf, 2019).

Blockchain technology appears in many modern publications on the cybersecurity of electronic election systems (Vilks et al., 2022). Conventional electronic voting systems use a centralised scheme. The centralised administration of these systems manages the entire voting process and has partial or full control over the database and the system itself. This creates some problems, accidental or intentional, such as possible database fraud and double voting. Many of these problems have been solved thanks to blockchain technologies, without access rights in new voting systems. However, the classical consensus method requires a certain amount of computing power during each voting operation. This substantially affects power consumption, reduces efficiency, and increases system latency. The use of a blockchain with access rights increases the efficiency and reduces the energy consumption of the system, mainly due to the rejection of the typical consensus protocols used in blockchains. The use of smart contracts provides a secure mechanism that guarantees the accuracy of voting results and makes the vote-counting procedure public and protected from fraudulent actions, as well as helps preserve the anonymity of votes. Its use in electronic voting systems can help mitigate some of these problems. In the joint work of Mexican, Cuban, and Indonesian researchers C. Denis González et al. (2022), a system is proposed that provides high reliability through corporate blockchain technology, providing secret voting. Furthermore, the authors present some solutions to the problem of security and reliability using a flexible network configuration.

Conclusions

Electronic voting is an ambiguous way of conducting elections. On the one hand, it speeds up the election procedure and votes to count and allows expanding the coverage of voters. However, the system is at substantial risk of a hacker attack. Election results may be falsified, and personal data of candidates, election commission employees, or voters may be publicly available. The reasons for these actions on the part of intruders and the consequences of such interventions were examined in detail using real examples from the history of electronic elections. As such examples, the study considered hacker attacks during the 2016 US presidential election and the hacking of information and communication systems of the State Election Commission of Northern Macedonia in 2019. The authors presented the case of hacker attacks on the voting systems with direct recording, which were used during the midterm elections in Georgia, USA, in 2018. As the practice of conducting electronic elections shows, the attackers have intentions not only to distort the results of the voting, but also to steal the data of candidates, voters, or election administration employees, as it was during the regional elections in Indonesia in 2018.

A crucial factor in ensuring security is preventive work, such as, e.g., cyber hygiene training programs for employees of polling stations. To prevent cyberattacks, it is necessary to provide the system with reliable protection. To better understand possible hacker attacks, the study investigated the main goals of hacker attacks, such as to cause damage to the electronic election and vote-counting systems. Specifically, subject to such attacks are the procedures for registering voters, voting, counting votes, transmitting, and aggregating results. Methods of countering these attacks based on the efficiency and cost-effectiveness of technologies have been described. The study does not include all existing variants of protection technologies and does not provide recommendations for improving the reliability of the most vulnerable places of the electronic election and vote counting system. In the future, it is necessary to find weaker links in the system and create more effective protection technologies.

References

Abba, A.L., Awad, M., Al-Qudah, Z., & Jallad, A.H. (2017). Security analysis of current voting systems. In *International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. Retrieved from https://doi.org/10.1109/ICECTA.2017.8252006

Abdymanapov, S.A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy expert system of information security risk assessment on the example of analysis learning management systems. *IEEE Access*, *9*, 156556-156565.

Adanbekova, Z.N., Omarova, A.B., Yermukhametova, S.R., Khudaiberdina, G.A., & Tynybekov, S.T. (2022). Features of the conclusion of a civil transaction on the internet. *International Journal of Electronic Security and Digital Forensics, 14*(1), 19-36.

Aliaskar, M., Mazakov, T., Mazakova, A., Jomartova, S., & Shormanov, T. (2022). Human voice identification based on the detection of fundamental harmonics. In: *ENERGYCON 2022 - 2022 IEEE 7th International Energy Conference, Proceedings*. Riga: Institute of Electrical and Electronics Engineers.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. *IEEE Access*, 10, 70746-70759.

Borysova, V.I., Ivanova, K.Y., Iurevych, I.V., & Ovcharenko, O.M. (2019). Judicial protection of civil rights in Ukraine: National experience through the prism of European standards. *Journal of Advanced Research in Law and Economics, 10*(1), 66-84.

Bradshaw, S., Hilt, K., Jardine, E., Kerschbaum, F., Klinger, U., Pal, M., & Wark, W. (2022). Next-generation technology and electoral democracy: Understanding the changing environment. Retrieved from https://www.cigionline.org/publications/next-generation-technology-and-electoral-democracy-understanding-the-changing-environment/

Cherniha, R., & Serov, M. (2006). Symmetries, ansätze and exact solutions of nonlinear second-order evolution equations with convection terms, II. *European Journal of Applied Mathematics*, *17*(5), 597-605.

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O., & Sosa-Gómez, G. (2022). Electronic voting system using an enterprise blockchain. *Applied Sciences*, 12(2), 531.

Derysh, I. (2019). Hackers can easily break into voting machines used across the U.S., play Doom, Nirvana. Retrieved from https://www.salon.com/2019/08/14/hackers-can-easily-break-into-voting-machines-used-across-the-u-s-play-doom-nirvana/

Estehghari, S., & Desmedt, Y. (2010). Exploiting the client vulnerabilities in Internet e-voting systems: Hacking Helios 2.0 as an example. Retrieved from http://www.usenix.org/events/evtwote10/tech/full_papers/Estehghari.pdf

Gupta, S., Gupta, A., Pandya, I.Y., Bhatt, A., & Mehta, K. (2021). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, 80, 3363-3370.

Hencke, D., & Johnson, B. (2007). Counting error almost gave Labour Scottish election victory. Retrieved from https://www.theguardian.com/politics/2007/jun/20/scotland.devolution

Hiscox Cyber Readiness Report. (2018). Retrieved from https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Hratsiotova, H., Tkach, K., & Pulcha, D. (2020). Introduction of electronic elections in Ukraine in a pandemic state. Foreign experience. *ECONOMICS: Time Realities*, 51(5), 14-20.

Jafar, U., Aziz, M.J.A., & Shukur, Z. (2021). Blockchain for electronic voting system – Review and open research challenges. *Sensors*, 21(17), 5874.

Jefferson, D. (2019). The myth of “secure” blockchain voting. Retrieved from https://verifiedvoting.org/the-myth-of-secure-blockchain-voting/

Khanpara, P., Patel, S., & Valiveti, S. (2022). Blockchain-based e-voting technology: Opportunities and challenges. In *7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 855-861). Coimbatore: IEEE.

Kurniawan, A., Riadi, I., & Luthfi, A. (2017). Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework. *Journal of Theoretical & Applied Information Technology*, 95(6), 1363-1371.

Leite, G.S., & Albuquerque, A.B. (2018). An Approach for Reduce Vulnerabilities in Web Information Systems. In *Intelligent Systems in Cybernetics and Automation Control Theory* (pp. 86-99). Cham: Springer.

Limba, T., Agafonov, K., Paukštė, L., Damkus, M., & Plėta, T. (2017). Peculiarities of cyber security management in the process of internet voting implementation. *The International Journal Entrepreneurship and Sustainability Issues*, 5(2), 368-402.

Lomzhets, Y., Dmytruk, I., & Dubinskyi, I. (2021). Electronic (online) voting in Ukraine: Realities and prospects. *SHS Web of Conferences*, 100, 03007.

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In *Electronic Voting 2006 – 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting* (pp. 15-26). Bonn: German Informatics Society.

Maraj, A., Jakupi, G., Rogova, E., & Grajqevci, X. (2017). Testing of network security systems through DoS attacks. In: *2017 6th Mediterranean Conference on Embedded Computing, MECO 2017 - Including ECYPS 2017, Proceedings* (Article number 7977239). Bar: Institute of Electrical and Electronics Engineers.

Mazakov, T.Z., Jomartova, S.A., Shormanov, T.S., Ziyatbekova G.Z., Amirkhanov, B.S., & Kisala, P. (2020). The image processing algorithms for biometric identification by fingerprints. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, 1*(439), 14-22.

Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security, 1*(1), 4-17.

Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security, 1*(1), 18-25.

Mueller, R.S. (2019). Report on the investigation into Russian interference in the 2016 presidential election. Retrieved from https://www.justice.gov/storage/report_volume2.pdf

Nakashima, E., & Harris, S. (2018). How the Russians hacked the DNC and passed its emails to WikiLeaks. Retrieved from https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

Nwankwo, W., & Njoku, C.C. (2020). Adoption of i-voting platform in Nigeria: Dealing with network-level cybersecurity concerns. *Technology Reports of Kansai University*, 62(3), 185-198.

Okrój, S., & Jatkiewicz, P. (2023). Differences in performance, scalability, and cost of using microservice and monolithic architecture. In: *Proceedings of the ACM Symposium on Applied Computing* (pp. 1038–1041). Tallinn: Association for Computing Machinery.

Omurzakova, A., Shalbolova, U., & Mukhanova, G. (2022). Risk assessment of social public-private partnership projects. *Public Policy and Administration, 21*(2), 140-150.

Ottoboni, K., & Stark, P.B. (2019). Election integrity and electronic voting machines in 2018 Georgia, USA. *Springer International Publishing*, 166-182.

Riadi, I., & Raharja, P.A. (2019). Vulnerability analysis of E-voting application using open web application security project (OWASP) framework. *International Journal of Advanced Computer Science and Applications*, 10(11), 135-143.

Roh, C.H., & Lee, I.Y. (2020). A study on electronic voting system using private blockchain. *Journal of Information Processing Systems*, 16(2), 421-434.

Sanger, D.E., & Edmondson, C. (2019). Russia targeted election systems in all 50 states, report finds. Retrieved from https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

Savchenko, O. (2022). Innovative aspects of development of digitalization of public governance in the USA. *Democatic Governance, 2*(30), 120-130.

Shariy, V.I. (2019). The effectiveness of local municipal authorities of Ukraine in the exercise of powers delegated by the government. *Asia Life Sciences, 1*, 159–167.

Shrivastava, G., Gupta, D., & Sharma, K. (2021). *Cyber crime and forensic computing: Modern principles, practices, and algorithms*. London: Walter de Gruyter.

Sopilko, I., & Rapatska, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs, 28*(1), 44-54.

Srokosz, M., Rusinek, D., & Ksiezopolski, B. (2018). A new WAF-based architecture for protecting web applications against CSRF attacks in malicious environment. In *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 391-395). Poznan: IEEE.

Stedmon, N. (2020). *The impact of cyber security threats on the 2020 US elections*. Poole: United Kingdom.

Sϕhoel, H., Jaatun, M.G., & Boyd, C. (2018). OWASP top 10-do startups care? In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). Glasgow: IEEE.

Tatsyi, V., Getman, A., Ivanov, S., Karasiuk, V., Lugoviy, O., & Sokolov, O. (2010). Semantic network of knowledge in science of law. In: *Proceedings of the IASTED International Conference on Automation, Control, and Information*

Technology - Information and Communication Technology, ACIT-ICT 2010, (pp. 218-222). https://www.actapress.com/PaperInfo.aspx?paperId=41146

Teplytskyi, B. (2021). Modern possibilities of forensic examination in the process of investigation of crimes in the field of computer systems and telecommunication networks. *Law Journal of the National Academy of Internal Affairs*, *11*(2), 30-37.

Van der Staak, S., & Wolf, P. (2019). *Cybersecurity in elections: Models of interagency collaboration*. Stockholm: International Institute for Democracy and Electoral Assistance.

Vilks, A., & Bergmanis, D. (2018). Global organized crime in Latvia and the Baltics. In: *Global Organized Crime and International Security* (pp. 63–70). Abingdon: Taylor and Francis Ltd.

Vilks, A., Kipane, A., Kudeikina, I., Palkova, K., & Grasis, J. (2022). Criminological Aspects of Current Cyber Security. *Revista de Direito, Estado e Telecomunicacoes, 14*(2), 94-108.

Wang, R., Xu, G., Zeng, X., Li, X., & Feng, Z. (2018). TT-XSS: A novel taint tracking based dynamic detection framework for DOM Cross-Site Scripting. *Journal of Parallel and Distributed Computing,* 118, 100-106.

Zetter, K. (2018). Was Georgia’s Election System Hacked in 2016? Retrieved from https://www.politico.com/magazine/story/2018/07/18/mueller-indictments-georgia-voting-infrastructure-219018/