e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

CONCEPT IN INFORMATION SECURITY TECHNOLOGIES DEVELOPMENT IN E-VOTING SYSTEMS

Nameer Hashim Qasim[*1], Volodymyr Vyshniakov[*2], Yurii Khlaponin[*3], Vadym Poltorak[*4]

[*1]AL Qalam University College Kirkuk, Iraq.

[*2,3]Cybersecurity and Computer Engineering Department, Kyiv National University ofConstruction and Architecture, Kyiv, Ukraine.

[*4]Department of Automatics and Control in Technical Systems, NTUU "Igor Sikorsky KyivPolytechnic Institute", Kyiv, Ukraine.

ABSTRACT

Standard information protection technologies assume the presence of the owner of information. It is the owner who chooses the means of protection, asit is an interested person. In secret ballot systems, the information belongs to society and organizers must create conditions for voters to make sure that the secrecy of votes and the accuracy of their counting is preserved. In developed democracies, problem is addressed through random voter's audit of all procedures where information threats are suspected. It completely eliminates the reasons for distrust in the voting system. The concern of citizens is that in the case of introduction of e-voting it is impossible to provide audit. There are no other ways to ensure the trust of voters than to give them a full audit opportunity. The only surefire way to gain trust is to create truly open system for audit, in which voters would be able to verify anything that might cause mistrust. This work is devoted to designing of such protected system for e-voting. The paper describes principles of secret e- voting system building, in which voters or their proxies have opportunity to audit the system hardware and software, which allows them to ensure that there is no violation of confidentiality and integrity of information. The principles of eliminating illegal influence on voters by bribery or other methods of moral or forceful pressure are also considered. The results of the e-voting system implementation are described and links are provided for conducting of experimental voting over the Internet.

Keywords: E-Voting, Voter Information Protection, Trust Ensuring In E-Voting, Transparency In E-Voting Systems, Elimination Of Illegal Influence On Voters.

I. INTRODUCTION

Computerization covers all processes of human activity incessantly and inevitably, including the most important decisions, which use the procedure of mass secret expression of human will. This is a fact that cannot be denied, but people's concern about innovation in the most developed democracies, such as Italy, where, as described in [1], election fraud is never suspected, should also be acknowledged. They do not want to lose democracy through the introduction of new technologies. Their experience is exemplary for countries where elections end in scandals and protests. At the same time, unquestionable trust is achieved through openness to the audit of all processes that may cause mistrust. Any random voter can per-form an Audit. Thus the recipe for absolute trust is not complicated, but it requires activity on the part of the public and political will from the organizers of the election process. It is difficult to imagine a society in which fair democratic elections are possible without these two com- ponents. Each year the problem becomes more acute to en suring trust in voting systems. This was largely felt in the US presidential election in 2020, where the issue of no confidence reached the level of the president of the state [2]. It is in this country that there is an impressive variety of technologies for accounting for the will of citizens.Modern society is becoming increasingly demanding of the democratic principles of state formation. An exampleof this is the mass protests in countries where there are attempts to monopolize the power. All this indicates that the trust of citizens is one of the most important requirements for the improvement or development of voting systems. Distrust can lead to suspicions of fraud, which is a destructive factor for the sustainable development of countries.

The rights of voters are declared in Article 25 of the UN International Covenant of December 16, 1966, which

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

states that elections must be genuine, periodic, free, secret and equal [3]. Therefore, the developers of innovative methods have focused on these requirements, and the confidence in the processes has been forgotten for a long time. Such a requirement is not explicitly present in the International Covenant. But it is obvious that a democratic society will not accept innovation without its implementation, because it does not want to exchange democratic values for amore convenient way of expressing will. People cannot trust tools that are not open to full scrutiny. We should not count on real successes in the development of e- democracy until the developers find really convincing methods of disclosing everything that can cause mistrust for the audit. This is stated in paragraph 39 of the EU Council Recommendations on e-voting standards: "The e- voting system is subject to audit. The audit system must beopen and comprehensive" [4].

It is known that not enough attention has been paid to ensuring trust in the vast majority of electronic voting systems, which have allegedly been successfully implement- ed. At the same time, one cannot rely on the fact that the system was created and maintained exclusively by honest people. Nor can it be argued that traditional systems also have opportunities for fraud and therefore should not re- quire full transparency from innovative methods. These arguments cannot convince the true defenders of democracy. There are no other ways to ensure the trust of voters than to give them the opportunity to audit. Therefore, creating truly open audit systems is the only way to gain trust.

In such systems, voters have the opportunity to check any- thing that may cause mistrust. This work is devoted to the principles of creating such systems and the first results of their implementation.

II. WHAT IS LACKING IN MODERN PROTECTION TECHNOLOGIES FOR E-DEMOCRACY SYSTEMS

Existing standards for protecting computer information from a variety of threats assume that there is an information owner, and he or she, as an interested person (or group of people), makes demands to build a security sys- tem. In the case of computer networks, the information to be protected is located on a server running a network operating system, which always has an administrator with the rights to view and modify all user information files. The owner has the opportunity to hire administrators who en- joy his trust, and if necessary, dismiss them and replace them. In this case, in case of damage to information due to breakage of means of protection, the loss is borne exclusively by the owner of the information.

In an e-democracy system, information can belong to a large community of citizens, such as the results of a secret ballot. No trust in any administrators in this case is unacceptable. Here, all actions of the administrator that may damage the information must be continuously monitored by the community, and in case of violations of security rules, urgent precautions must be taken. The first step to building such a security system is to create a user- controller with rights that allow you to check the contents of all files, including operating system files, as well as run server-safe commands to check all processes that are potentially dangerous to critical information. including administrator actions. It is necessary that the rights of the us- er-controller should be available to any representative of the community of citizens or his proxies. Confidential in- formation that may be placed in files must be encrypted in a way that prevents it from being disclosed. It is desirable that the possibilities for creating a user-controller be embedded in all those operating systems that are designed for e-democracy. Also, it would be desirable to keep the history of administrator commands in a file open for control, which cannot be corrected or deleted in system. The purpose of this proposal is to simplify the integrity checking of the operating system, because the administrator can modify files at the request of attackers. If you check all of the administrator's actions, it's easy to detect such abuses and make sure that no freelance actions have been taken by the administrator, which means that the operating sys- tem can be trusted. You should not suspect abuse of operating system developers, because all their codes are open, and the functions are declared and carefully checked not only by developers but also by numerous users from around the world.

III. PRINCIPLES OF TRUSTWORTHY SYSTEMS BUILDING

Issues are primarily related to the secrecy of votes and the fairness of the results of their counting that cause distrust of citizens during e-voting. Disclosure of the secrecy ofthe vote makes it possible to force voters to

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

vote not at their own discretion by bribery or other method, but on the instructions of another person. Therefore, it is necessary that the voter does not have the opportunity to demonstrate his real choice to anyone and even to himself, because otherwise it will contribute to the influence of his choice by outsiders.

Only those procedures can give rise to distrust in the e- voting system, which is related to the secrecy and countingof votes. Therefore, we propose to allocate a separate voting server for their implementation, on which all processes and files are monitored by the community of citizens through the audit server. To ensure continuous monitoring,the audit server and the voting server communicate directly through the switch, which minimizes the delay of signals during the exchange of data between them. The rest ofthe connections between the blocks of the voting system are established by means of secure communication proto- cols via Internet channels. All these connections are shownin Figure 1.

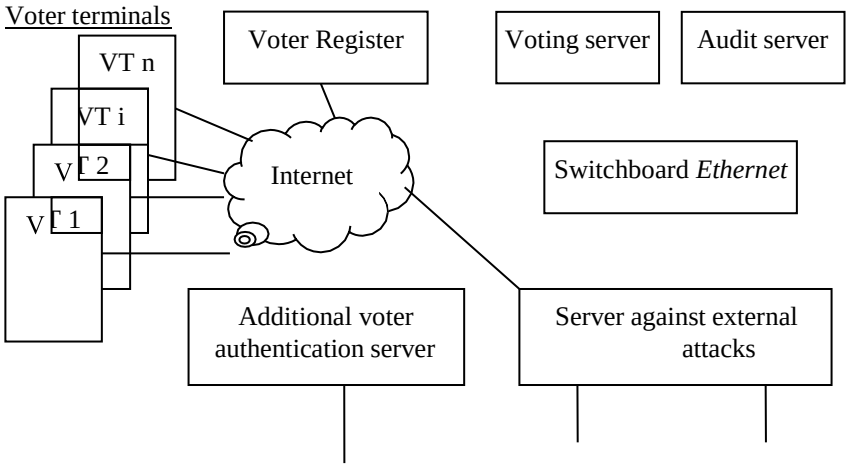

Fig 1: Block diagram of the e-voting system

Citizens' mistrust may also be due to suspicion of falsifying the voter register by adding extra people to be re- placed by hired people. The fight against this method of falsification requires only the political will of the organizers to publish information on the number of voters on each street within the polling station, on each house within the street and on each apartment within the house. Then voterswill be able to find extra voters in their apartments, extra apartments in their homes and extra houses on their streets.It is impossible to detect such falsifications by the efforts of programmers only. From now on, we will assume that our principles are suitable only for a democratically- minded society, in order to distance ourselves from problems that cannot be solved by technical means. Such a society aims to detect and prevent abuses when making joint decisions by remote secret ballot. This allows citizens to exercise their right to vote via the Internet when they are unwilling or unable to vote at a polling station.

The main principle of our system is to deprive the votingserver of those functions that do not affect the secrecy of votes and their counting, in order to facilitate the audit, which allows detecting the presence or absence of harmful effects on the server. Not every voter is able to conduct such an audit on their own today, but the necessary knowledge is provided at school in computer science les- sons, so the audit of such a system becomes possible forthe growing number of voters every year. Our task is to give voters the opportunity to see the fair work of this sys- tem. If they lack the knowledge to audit, they can get help from observers and more educated voters or experts.

The initial stage in the conduct of voting is preparation of the voter register. Identifiers and passwords are required for voters in the on-line mode in addition to passport data in the register. It is convenient to choose passport numbersas identifiers, because they are always unique and cannot be forgotten. Passwords should be stored as a cipher that cannot be decrypted by third parties. To do this, we use thepower function of the prime element of the Galois field, where the power is formed as a concatenation of the identifier and password with the addition of a given maximum length. The Galois field is chosen for one for which the problem of discrete logarithm has not yet been solved. Therefore, these data cannot be decrypted in a reasonable amount of time.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

During registration, the voter is provided with a temporary password and a link to the website of the register, where it is possible to check and change your password. Before each vote, the registers are printed in paper form for polling stations operating by traditional technology. And a file with encrypted IDs and passwords (74 bytes of cipher per each voter) is created and sent to the voting server for voters who will vote remotely. No personal voter information can be obtained from this file.

The voting server is audited immediately after the start- up and creation of the user-controller. The audit begins at a time when there is no critical information on this server. Therefore, no restrictions on the full inspection of all soft- ware and hardware by voters or their proxies are required. Controllers may require that the installation of the voting server be performed under the supervision of community experts. The voting server was implemented on a standard Raspberry Pi 3 Model B minicomputer, which is widely known and commercially available. It hardware is open to the public inspection. All this can be easily replaced at the request of controllers in case of problems with trust in the hardware or the SD memory cards with which it works. The view of voting server on the Raspberry Pi 3 Model B minicomputer is shown in Figure 2.

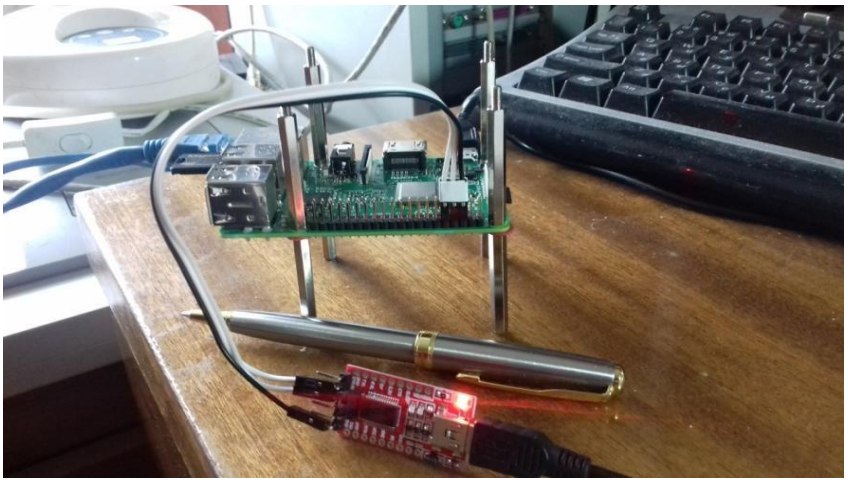

Fig 2: Server on a Raspberry Pi 3 Model B minicomputer

The purpose of the presence of citizens during the installation is to eliminate the suspicion that the hardware or operating system (OS) is falsified. The OpenBSD operating system is downloaded from open servers on the Internet,so its authenticity can be verified by downloading this sys-tem to another similar computer and then comparing the system files on these two computers, as described in [5]. An important feature of OpenBSD is that it has a monopoly control over the server until the power outage and does not allow any external interference in the operation of ap- plications. In addition, the audit server automatically detects all processes that could be potentially harmful. After citizens and their proxies check the software and hardware of the voting server and connect the audit servers, voters can continue the audit remotely without losing information about the identified violations.

The principle of the audit server operation is as follows. This server periodically accesses the voting server every few seconds as a user-controller (SSH) for information about currently active processes (ps -aux command). The audit server does not respond to the processes started by the controllers and the operating system, and in case of any other process its parameters are logged and an alarm issent to the devices specified by the controllers. This identifies processes that can be potentially dangerous.

The server for protection against external attacks be- longs to the Internet service provider. This server should be transparent to voters, but it can host the tools to create a proxy attack Man in the Middle if the provider agrees with the attackers. This attack is a very dangerous threat that al- lows the disclosure and substitution of votes. The difficulty of combating such a threat is that it can be implemented at any time on any intermediate server between the voter and the voting server. Such an attack can only be carried out on the equipment of providers who are responsible for such actions and can be punished. The purpose of protecting against this threat is to ensure that each voter has easy- to-use means to detect this threat when connecting to the voting server. Detection of intermediary attacks does not cause any complications due to the audit server.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

The server of additional authentication of voters allows to carry out specification of the person on biological or other signs and provides protection against illegal influence on voters by bribery or other methods for forcing them to vote against own discretion. In case of voting at meetings or meetings on-line the stage of additional authentication should be canceled, as such authentication complicates the procedure of expression of will. At the same time, everything remains in full that ensures the trust of voters, namely protection against violations of the secrecy of votes and against falsification of their counting.

The list of requirements for the voting server that must be met to ensure the unquestionable trust of voters is given in Table 1.

Table 1: Requirements for the voting server to ensure the trust of voters

#	Requirement	Fulfillment of the requirement
1	Availability of hardware auditingwithout personal restrictions.	Selection of well-known hardware with open installa-tion for inspection and with the possibility of their re-placement in case of suspicion of forgery
2	Availability of OS auditing duringits installation, as well as during the entire period of operation	Select an open OS that allows you to create a user- controller who is prohibited from executing com- mands that may interfere with the server, but can readall files and execute secure commands
3	Impossibility of imperceptible re-placement of hardware and OS during the entire period of opera-tion after the implementation of paragraphs 1-2	Providing remote access to the audit server to all vot-ers and their proxies, as well as permission to install additional auditing servers that continuously demon- strate the safe state of the server's software and hard-ware or send an alarm
4	Control staff actions on server management, including download-ing software packages	Adoption of rules according to which the staff must execute the command history> haabbccdd.txtbefore the end of the managementsession, where instead of aabbccdd enter the date and time: aa - month, bb – day number, cc - hours, dd - minutes. This allows you to control all the actions of staff.
5	Availability of application verifi-cation	A choice of well-known computer languages (HTMLand JavaScript) and a simple programming style, as well as the openness of the software and the ability to test it
6	Quick notification in case of vio-lations	Establish rules for the acceptance of reports of viola-tions and for appropriate response

Consider the meaning of each of these requirements and features of their implementation.

The first requirement is ignored by most developers,who believe that the inspection of hardware by citizens or their proxies is not required. In this case, the voting server will be a "black box", even for voters who are well versed in computer technology. At the same time, it is impossible to eliminate the suspicion that in this "black box" an imitator is hidden who shows voters a supposedly fair vote, but in fact reveals and substitutes their votes. It is not possible to gain the trust of voters because of such suspicion with- out opening the hardware to

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

the audit.

Choosing a well-known open-air mini-computer completely dispels the suspicion of a "black box" with a hidden simulator. It is not possible to create a simulator on the single board of this computer due to lack of resources. In addition, all these resources will be captured by the OpenBSD operating system, the installation and launch of which is allowed to control of any member of the public. This control requires the direct presence of controllers in the room where the server equipment is located only in the preparatory period, when there is still a lot of time before the start of voting and there is nothing secret in the memory. The controllers only need to check the accuracy of instructions for installing and starting the operating sys- tem, as well as the correctness of the connection of the audit server according to the diagram shown in the Fig. 1. Highly qualified specialists are not required for such an inspection, because the instructions are simple and open. This ends the need for the presence of controllers in the server room. Further control is performed remotely based on the command ps -aux, which displays the parameters of all active processes at the current time. An example of the result of this command is shown in the Figure 3.The ps -aux command allows you to detect any attempt to interfere with the server, because each intervention is accompanied by the appearance of a new active process.

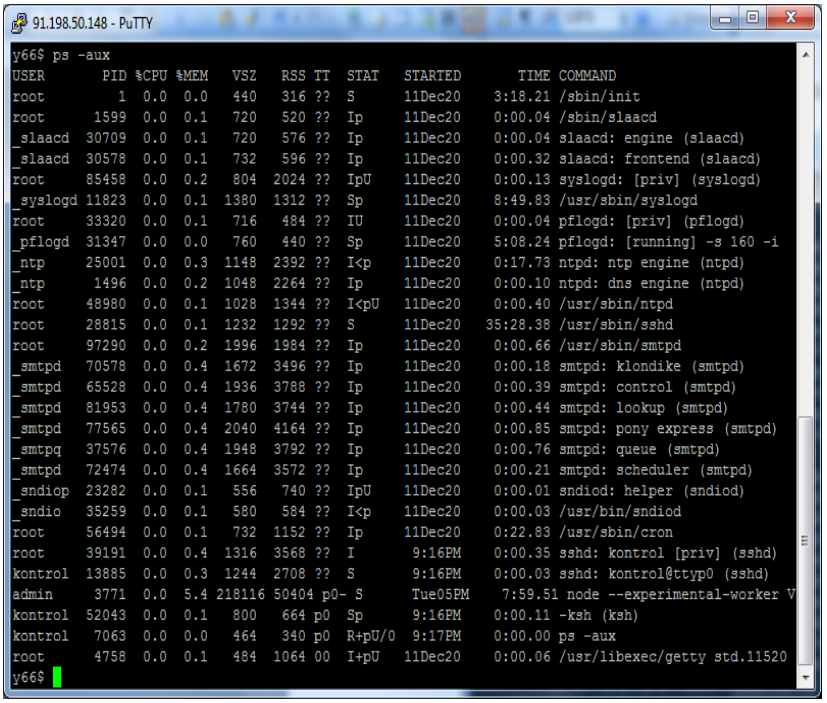

Fig 3: View of the result of the ps -aux command

Of the many attributes of active processes, only the first two and one last attribute are sufficient to analyze these interventions. The first column (USER attribute) displays the name of the user who started the process, the second (PID attribute) - a random identifier that is provided to the process at startup and remains unchanged until its completion,and the last (COMMAND attribute) - the command which initiated this process. At the time of OS startup, more than 20 active processes of the OS itself occur, the first of which is provided with PID = 1, and the other is provided with unpredictable random PID values. Therefore, it is not possible to secretly restart the OS, because this will change all the PID values, except the first, which is easy to detect by remembering the initial result of the psaux com- mand. It is clear that it is absolutely impossible to replace hardware without restarting the OS. The instructions for the administrator stipulate that after starting the OS, you should create two users named admin and control. The admin user is given administrator rights to work with files, but only within the / home / admin / directory, and the control user is given controller rights. In addition to these us- ers, the system necessarily creates a primary root user, who is granted full rights and without which it is impossi- ble to configure the system, but after performing actions that require full rights, the file / etc / ssh / sshd_config pa- rameter PermitRootLogin yes to PermitRootLogin no means denying access to the server with root privileges, after which the server can be managed only by the admin user, with limited

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

rights, which simplifies the monitoring of his actions. The names of all OS users are stored in the / etc / group file, which al- lows you to verify the correctness of the adduser com- mand, which the administrator uses to create users. We see23 processes in the Figure 3, that implement the functions of the OS, which was launched on December 11, 2020 (as evidenced by the value of the attribute STARTED), 4 pro- cesses that are associated with the command ps -aux, entered by the user kontrol, and one process started by admin.

Here's an explanation of the four active processes in- volved in running the ps-aux command. The first process with PID = 39191 is a call to the sshd service, which accepts all requests from clients. The task of this service is client authentication and message encryption. Thanks to this service, the control client was given the right to create a second process of the same service (PID = 13885), be- cause it is a valid user of the OS. The third process (PID = 52043) was created by the user control to send their com- mands. This process controls the availability of rights to execute commands and allowed to create a fourth process (PID = 7063), which implements the execution of the command ps -aux. The admin process (PID = 3771) is a program that decrypts and counts the votes of voters.

The task of the audit is to check whether the administrator has actually run the regular program, which is located on the voting server in the directory / home / admin /. This program is also presented in advance on a site accessible to voters. Both files with the program are open for copying on the Internet. They should be compared by any availablemethod. There can be no difficulty, because the program isa text file in JavaScript in a few hundred lines. The pro- cess of starting the program is controlled through a file with a history of commands, which should be created by the administrator according to the instructions after each session of server management. In this way, voters or their proxies can be sure of the validity of the current applica- tion.

The audit server automatically detects dangerous active processes on the voting server as follows. After receiving the next result of the ps –aux command, each line is checked using three lists of security features. The first list shows the PID values of permanent OS processes. The PID of the application is also added to this list after the above validation. The second list shows the values of the USER attribute namely the control and some user names that are assigned by the OS itself to support the system in automatic mode. The third list shows the values of the

COMMAND attribute, which includes the commands sshd, ksh and several other commands that the OS executes automatically to support its work. The process is considered safe if at least one of these three lists is detected. Thus, any cases of interference in the work of the OS, including the regular actions of the administrator, are automatically detected, logged and initiate the sending of danger messages to the means provided by voters.

The openness and simplicity of the applications make it easy to analyze all the transformations associated with encryption and counting. This makes it possible to eliminate suspicions about the incorrect operation of programs or thepresence of any malicious bookmarks.

The implementation of the last requirement to respond incase of violations depends only on the political will of the voting organizers, because no matter how impeccable the technical means are, the information obtained through them can simply be ignored.

IV. DATA PROTECTION DURING TRANSMISSION VIA THEINTERNET

In addition to automatically detecting dangerous processes on the voting server, each voter can remotely check the status of the server and detect possible information threats using the audit key, which allows you to go to the appropriate web page when communicating with the voting server. The appearance of the web page for the audit ofthe polling station server is shown in Figure 4. Using the "OS Command" key on the audit website, voters can initiate an additional inspection of the hardware of the serverof their polling station at any time, as shown in Fig. 5.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

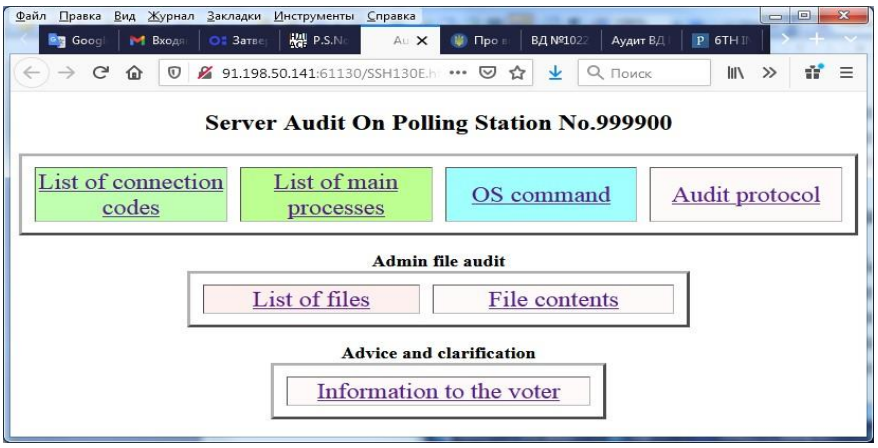

Fig 4: Web page for the audit of the polling station server

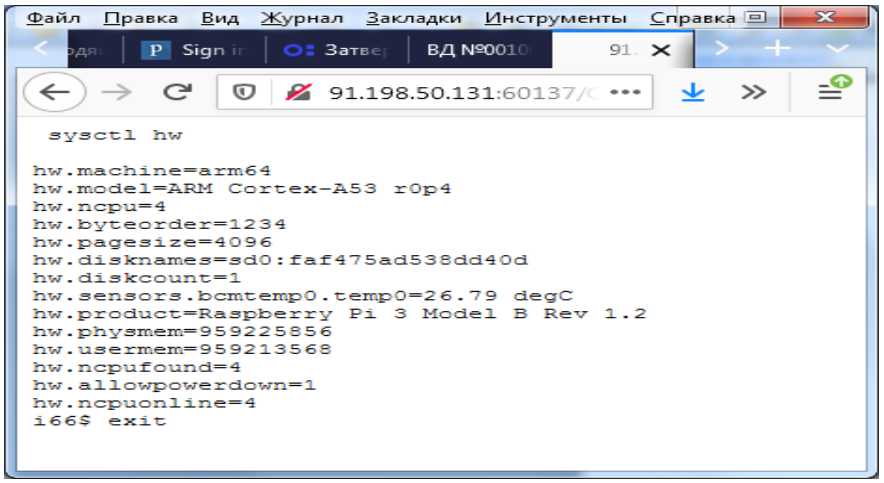

Fig 5: The result of the sysctl hw command

The sysctl hwcommand displays the basic specifications of the voting server, including the type of computer (Raspberry Pi 3 Model B Rev 1.2), the amount of RAM,the number of cores, and the type of processor, and so on. All important characteristics of the server's software and hardware can be checked remotely. But most importantly, each voter can be sure that there is no attack by an intermediary when exchanging confidential data with the voting server. To do this, he must use the "Connection Log" key (see Figure 5) to highlight the characteristics of the connections, among which you should find the code of his connection, which he receives in each message from the server during the voting. The appearance of such a message from the server and the connection log page is shown in Figure 6 and Figure 7 respectively.

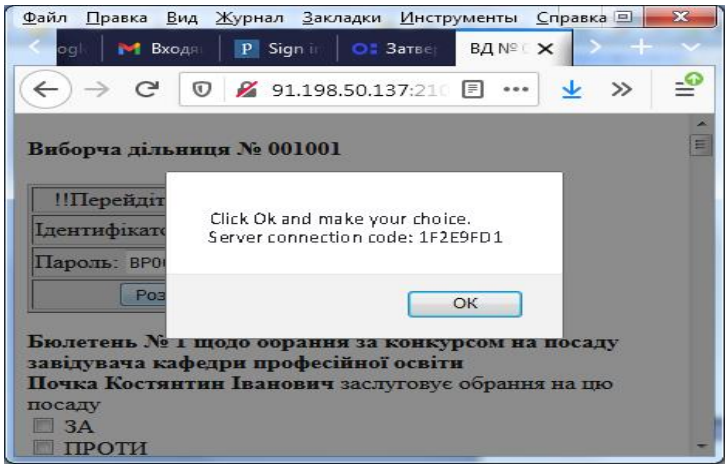

Fig 6: The appearance of the connection code message

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

Intermediary attacks are unlikely due to of their com- plexity and the possibility of penalizing ISPs who are responsible for network access services quality.

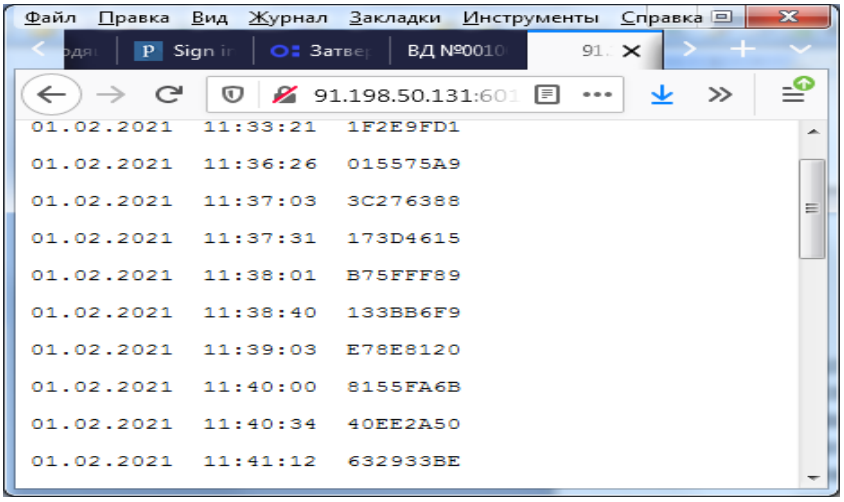

Fig 7: View the connection log page

However, they cannot be ignored, believing that these attacks are a dangerous threat if the Diffie-Gellman algorithm which is used.

The mediator's attack is detecting as follows. On the Diffie-Gellman algorithm [6], the initial part of the sequence that the server sends to the client is registered in the log, where the date and time are indicated at the beginning of the line (see Figure 7). On the client side, after receiving this numerical sequence, its initial part is added in messages called "Server connection code" (see Figure 6). In the case of an intermediary attack on the attacker's serv- er, its random number is generated, from which the Diffie- Gellman algorithm forms its numerical sequence for sending to the client, which will be different from the one formed by the regular server. The attacker will be detected because the fictitious code will be absent when message received by the voter from the log on the server. The voter receives data from the voting server through the audit server and through a channel protected from attacks by the mediator.

To protect data during the exchange of information be- tween the voter and the voting server, the Vernam cipher was chosen, which provides very high protection against disclosure, which is mathematically proven in [7]. The use of this cipher requires special conditions, but the ad- vantage is that data leakage during channel transmission becomes almost impossible. This is an important component in ensuring voter confidence. Table 2 lists the conditions for robust data protection during transmission.

Table 2: Conditions for ensuring absolute data protection during transmission

Condition	Description of the condition
Generation of random bit sequences(not pseudo-random)	A method is implemented of generating random (non-pseudo-random) bits, which allows to gener- ate random sequences on any computer, the methodis described in [8]
Each random bit sequence can beused for encryption only once	Random bit sequences are generated independentlyof each other for each communication session
To exchange random bit sequences,you should use a completely secure communication channel	Follow the Diffie-Gellman algorithm to exchange of random bit sequences, with such parameters forwhich in modern conditions there is no possibility of data disclosure

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

In [9] the Diffie-Gellman algorithm parameters choice was substantiated for the problem of e-voting, and in [10] the counteraction to mediator attacks is offered which are important threat in case of this algorithm is using. It is this method of detecting mediator attacks that is chosen in our system, as described above.

The parameters of the multiplicative algebraic group for the implementation of the Diffie-Gellman algorithm are selected from the following conditions. First, you need to make it impossible to disclose data for a certain amount of time. Second, it is necessary that the time of cryptographic transformations does not exceed the value set by the election regulations. In Ukraine, state elections provide 12hours for each polling station where the number of voters cannot exceed 2,500. The narrowest point in the data processing chain is the voting server, which means that it should not spend more than 17 seconds processing voter data. Obviously, the number of voters who vote remotely cannot reach 100%, but it is desirable to reduce the time of voter data processing to 3-5 seconds due to the uneven flow of voter requests and the possibility of pauses. For elections during a meeting where the number of voters does not exceed 500, the voting process should not take more than one hour. This means that the average data processing time of one voter by the server should not exceed 7 seconds in normal meeting condition.

In order to prevent data disclosure, a Galois field with characteristic 2 and exponent, which is a safe prime number belonging to the series 503, 563, 587, 719, was chosen.The solution of the discrete logarithm problem for such fields is currently unknown, so this protection for modern voting systems is quite acceptable. The time spent calculating the power of an element over a Galois field characterizes the longest of the data processing, which requires more than 6 seconds of Raspberry Pi 3 CPU time. There- fore, the uplink operation is divided into threads that are processed on different cores of a 4-core processor for minimizing the average time spent. Due to this, the average data processing time of one voter is reduced to 2 secondsin the case of the degree of field 503. This result fully satisfies the requirements of existing voting systems.

V. ELIMINATION OF ILLEGAL INFLUENCE ON VOTERS

According to Article 25 of the UN International Covenant, voters must have the right to freedom of expression, but there are cases of bribery and other illegal influence, when voters are forced to vote not at their own discretion, but on someone's instructions. At the same time, criminals need information about how the voter voted, because otherwise they will not be able to achieve their goal of con- trolling the actions of voters. In the case of remote voting, voters are not protected from possible observation of their actions by criminals. This means that the e-voting system must provide the conditions to be of coercion-resistance and receipt-freeness. Therefore, it is necessary to create such conditions that the voter has the opportunity to hide his choice from the malefactor, and for this it is impossibleto do without complicating the voting procedure. The only place a voter can truly hide his or her choice is his or her own memory. At the same time, the system should not provide the voter with information that his vote has been counted, because it is possible that the voting takes place under the supervision of an intruder. From the other hand, there can be no secret actions in the system, because the software is open to everyone, including attackers. Thisproblem is solved by introducing another procedure, whichwas proposed in [9], and which coincides in time with the period of updating the voter lists. This clarification takes place within two weeks before the start of voting. Voters who choose to vote remotely also need to get their final decision on the type of voting they want, as in each case they have the right to refuse remote voting and must be listed to receive a paper ballot. Thus, voters for remote voting should apply twice to the server, which will workaccording to the schedule shown in Figure8.

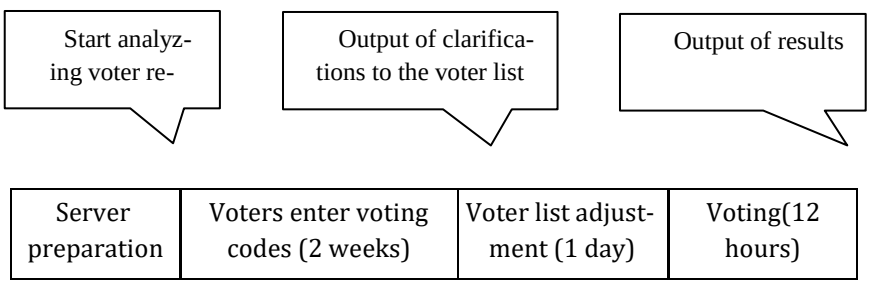

Fig 8: Schedule of the polling station voting server

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

The first access of voters to the voting server takes place during the period of updating the lists, which has duration of 2 weeks according to the election legislation of Ukraine. The form of dialogue of the voter with the server in this period is presented in Figure 9.

With the help of this dialogue the following three tasks are solved:

- entering a code that will replace the password during voting;
- confirmation by the voter of the fact of his personal voting (by means of the server of additional authentication, see Figure 1);
- receiving a final decision from the voter regarding re- mote participation in this voting.

No one but the voter himself should know the voting code. Therefore, it is necessary for the voter to invent this code and not forget it until the moment of voting. It is this knowledge that protects the voter's voice from any outside influence.

Additional authentication is required to eliminate the transfer of voting rights to another person, as this is prohibited by election law. Any incontrovertible personality traits, such as biological ones, can be used on the authentication server. This server is not auditable by voters be- cause it does not contain information related to the issue of distrust. Therefore, proprietary software can be used here. The task of this server is to provide answers to requests from the voting server. The inquiries contain only the vot- er ID, and the answers contain permission or prohibition. In the simplest case, you can use traditional authentication technology in the form of face-to-face verification with the presentation of a passport at a special point, where you should create conditions similar to voting booths. At the same time, voters will be able to be authenticated at any time convenient for them for two weeks, and on election day they will not need to arrive at the polling station. It should be noted that there is a time limit for entering the voting code within 15 minutes after authentication. The number of attempts to enter the code is not limited, and the last code received by the server is considered valid.

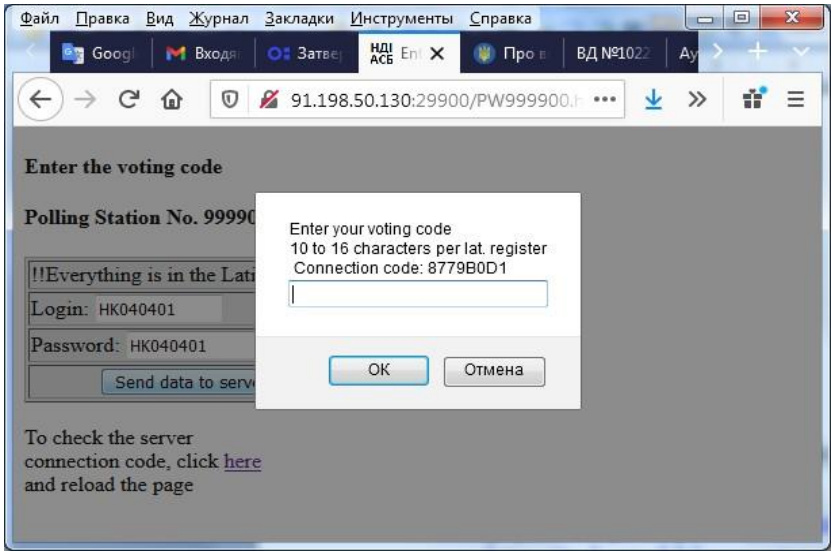

Fig 9: Form of the voter dialogue with the voting server during the code entry

After the voter entry period ends, the server provides access to the data about the voters who entered the codes. These data are used at the polling station to prohibit the issuance of paper ballots to these voters. Voting codes are stored exclusively in the server's RAM, to which only the application has access. The form of the voter's dialogue with the server during the voting is shown in Figure 10.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

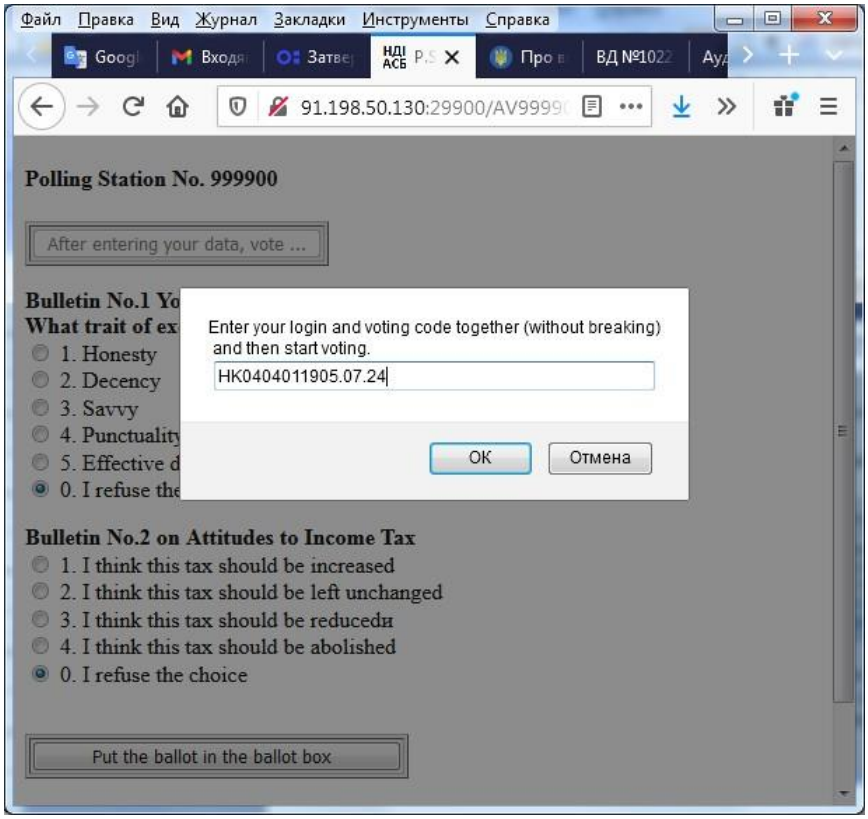

Fig 10: Form of dialogue of the voter with the server during voting

The server counts the voter's vote only if the code is correct, but returns a message about receiving the vote even if only the first two characters of the code are correct and hasthe form shown in Figure 11.

Thus, except for the voter himself, no one can get information about whether his vote was counted or whether it was a fictitious voter's vote, because only the voter knows the correct code and the code he actually entered into the system. The number of attempts to vote is unlimited, but only the first vote with the correct code is counted.

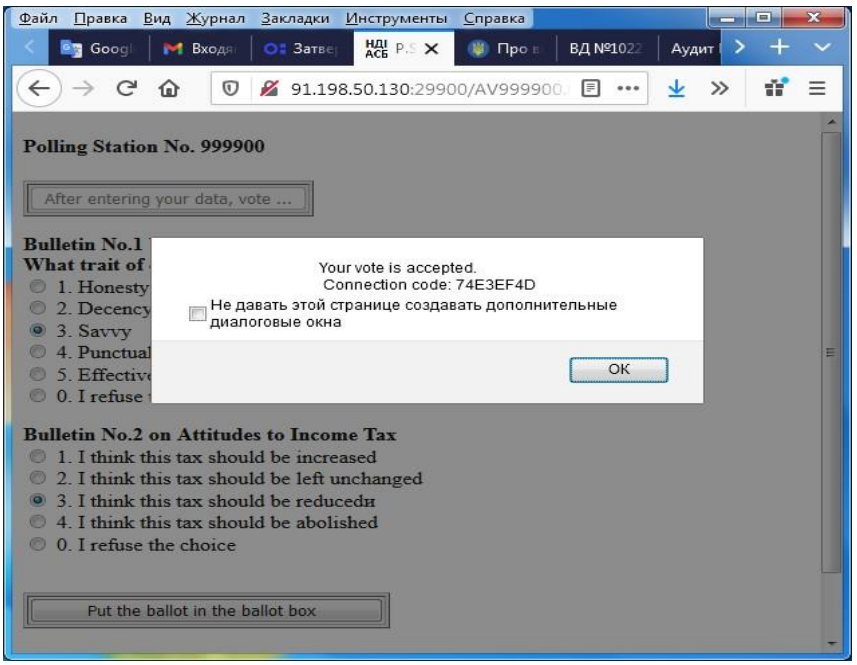

Fig 11: Notification of the voter about the server receiving his vote

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:09/September-2021 Impact Factor- 6.752 www.irjmets.com

If there is an error in the first two characters of the code, a message about the error code the server provides, which allows you to check the correctness of the server's reactions.

VI. EXPERIENCE OF IMPLEMENTATION AND WIDELYAVAILABLE TESTING OF THE VOTING SYSTEM

According to the plan of the Government of Ukraine,which was approved by the Cabinet of Ministers on June 12, 2019 №450-r [11], the introduction of e-voting is en-trusted primarily to higher education institutions. This approach differs significantly from that which has existed fora long time in other countries, where they relied entirely on professional developers and received a stream of criticism for failing to ensure public confidence, as describedin many works by researchers [1,12,13]. Thanks to thisapproach, the idea of the famous American scientist BruceSchneier was implemented, who in [14] gave the followingadvice on future developments: "If we're going to spend money on new voting technology, it makes sense to spend it on technology that makes the problem easier instead ofharder." In fact, in this work B. Schneier laid the idea of creating simple and open to audit e-voting systems, but this idea was not supported by professional developers. It is clear that the idea of simplification is not attractive for professionals, because it can negatively affect their fund- ing. As the analysis of modern e-voting systems shows, they continue to be complicated [12]. But the idea of Bruce Schneier was supported in the student work "Opensystem of secret ballot", which was published in 2014 in the collection of e-voting KNUBA (Kyiv National University of Construction and Architecture) [15]. In the firstplace in this work, the trust in the e-voting system due to its openness was put forward. The problem of trust is thatpeople can get rid of distrust only if a public audit is possible from the beginning of voting to the end of the votecount. Since the audit of e-voting systems requires special knowledge, it is necessary to acquire knowledge in the field of IT to achieve trust. Therefore, the Plan of the Government of Ukraine on the priority implementation of e- voting in higher education institutions can be considered appropriate, because this knowledge is acquired in higher and secondary education institutions. In addition, if students activate and create developments themselves, thesoftware and hardware solutions will be simpler and clear- er, and this benefits trust. It is for these reasons that the decision was made to choose the means of secret remote voting at the meetings of the Academic Councils on-line during the Covid-19 epidemic in Kyiv universities. The results of this implementation are described in [16]. For the last three years, KNUBA students have been using the e- voting system of their own design to elect their representatives to student self-government bodies [17]. At the same time, they get acquainted with the software and hardware of the system itself and make suggestions for their improvement. Access to all procedures required for e-voting is provided through the website http://vybir.knuba.edu.ua/, where e-voting is also possible at experimental polling stations in Ukrainian, English and Russian. The initiative wasalso taken by students of the Faculty of Informatics and Computer Science of the National Technical University of Ukraine, who in 2020 began holding elections of their representatives to self-government bodies using this e-voting system. Experts of the National Aviation University of Ukraine proposed to use this system to hold elections tothe governing bodies of the Red Cross of Ukraine. These elections were successfully held on December 4, 2020, where voters voted from different regions of Ukraine without leaving their place of residence during the quarantine period. Thus, the efficiency of this e-voting systemcan be considered practically proven.

VII. CONCLUSION

It is shown that in contrast to the known technologies of information protection, which assumes the presence of the owner to whom this information belongs, in secret ballot systems the information belongs to the society as a whole. This requires a special approach to building an informationprotection system due to the impossibility of identifying a person who would enjoy the absolute trust of all citizens. Therefore, it should be possible to conduct a widely avail- able audit of all software and hardware of the voting sys- tem, which may lead to distrust, as well as an audit of the actions of staff that may affect the operation of the voting system. The right to an audit should have any voter or his /her proxy throughout the operation of the voting system. Without such an audit, it is impossible to imagine the un- questioning trust of citizens in the media, and the presence of distrust is a destructive factor for democracy. In order toensure a full-fledged audit, which is able to detect any at- tempts to violate the secure state of voter information, the following set of measures is proposed. First, the

installation and start-up of voting servers is carried out under the supervision of voters or their proxies at a time when there is no critical information on the servers yet. Second, after launching the servers, voters continue to audit remotely using their dedicated servers without losing information about the presence or absence of interference with the voting servers. These specialized servers are able to detect and record any attempts to violate the secure state of information on the voting servers. Third, all software and hardware solutions are simple and open, which minimizes the time to conduct a full test. Implementing a voting serv-er on a well-known open-ended mini-computer eliminates suspicions of a "black box" that shows voters a fair vote, but in fact reveals and substitutes their votes, because it is impossible due to lack of technical resources. When sending confidential data over the Internet, absolute protection is provided through the use of known methods of advanced encryption. The average processing time of re-quests by the voting server is about two seconds. This means that in case of simultaneous access to the server of 30 voters, the waiting time in the queue will not exceedtwo minutes, and the server is able to serve more than 1,500 voters per hour during the voting. This means that the use of this system on Raspberry Pi 3B mini-computers fully meets the requirements for service speed. In order to prevent the transfer of voting rights to another person, the use of a separate server is provided, on which licensed means of authentication based on biological or other characteristics of a person can be installed. This server does not require a widely available audit by voters, as it doesnot contain information related to the issue of trust, namely the votes and their counting. To eliminate illegal influence on voters by bribery or other methods of moral or coercive pressure, voting technology was used, which allows voters to conduct a fictitious vote to mislead criminals. This technology does not allow anyone but the voter to know the true result of his vote. In recent years, this e- voting system has elected university students to self- governing bodies. In 2020, this system was introduced for secret ballot at meetings of scientific councils on-line inthe face of an epidemiological threat. On December 4, 2020, elections of the governing bodies of the Red Cross Society of Ukraine were held, where voters voted from different regions of Ukraine without leaving their place of residence during the quarantine period. The described sys- tem is open for review and experimental voting over the Internet.

VIII. REFERENCES

[1] Lombardi E. Electronic Vote & Democracy. URL: http://www.electronic-vote.org (access date: 02.01.2021).

[2] Conspiracy theories, a staple of US elections

[3] http://e-lected.blogspot.com/search/label/Elections%20in%20the%20United%20States

[4] International Covenant on Civil and Political Rights

[5] https://zakon.rada.gov.ua/laws/show/995_043#Text (access date: 04.01.2021).

[6] Recommendation CM / Rec (2017) 5(1) of the Committee of Ministers to member States on standards for e-voting https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

[7] Vyshnyakov VM, Komarnitsky OA Transparent e-democracy systems. Accent Graphics Communications & Publishing, Ottawa, Canada. 2019. - 96 p.

[8] W. Diffie, M. E. Hellman. New Direction in Cryptography. IEEE Transactions on Information Theory. 1976. v.IT-22, n.6. pp. 644-654

[9] Shannon C. Communication Theory of Secrecy Systems. Bell System Technical Journal. 1949. 28 (4). pp. 656–715.

[10] Chuprin VM Generation of random numbers by regular means of Internet hosts./V.M. Chuprin, VM Vishnyakov, MP Prygara // Information protection. - 2016. - Vol. 18, №4. - pp. 323-335.

[11] Chuprin VM, Vishnyakov VM, Prigara MP Method of counteracting illegal influence on vot- ers in the Internet voting system. Information security. - 2017. - Volume 23, №1. - pp. 7–14.

[12] Chuprin VM, Vyshnyakov VM, Komarnytsky OO, Method of counteracting attacks of a mediator in a transparent system of Internet voting, Information protection, Ukrainian Infor- mation Security Research Journal. - Kyiv.: NAU, 2019. - T.20. - №2. - pp.172-182.

[13] Pro zatverdzhennya planu zakhodiv shchodo realizatsiyi Kontseptsiyi rozvytku elektronnoyi

demokratiyi v Ukrayini na 2019-2020 roky. (2019). Available at: https://zakon.rada.gov.ua/laws/show/405-2019-%D1%80/sp:max10#Text. (Accessed:23 November 2020).

[14] Schneier, B. (2020) Voatz Internet Voting App Is Insecure. March 15, 2020. Available at: https://www.schneier.com/crypto-gram/archives/2020/0315.html (Accessed: 23 November 2020).

[15] Golubitskiy, S. (2019). Mutnaya tekhnologiya. Uroki moskovskikh vyborov na blokcheyne. Available at: https://новаяgazeta.ru/articles/2019/09/30/82175-mutnaya-tehn o logiya. (Accessed: 23 November 2020).

[16] Schneier, B. (2004) What's Wrong With Electronic Voting Machines? Available at: https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html. (Accessed: 23 November 2020).

[17] Vyshniakov, V.M., Prygara, M.P. and Voronin O.V. (2014)," Vidkryta systema tayemnoho holosuvannya" [The system of secret ballot is open], Upravlinnya rozvytkom skladnykh sys- tem. Zbirnyk naukovyh prac', No. 20, pp. 110 – 115.

[18] Chernyshev, D.O., Khlaponin, Y.I. and Vyshniakov, V.M. (2020), "Dosvid vprovadjennya elektronnoho holosuvannya v zakladi vyshchoi osvity" [Experience of introduction of elec- tronic voting in higher education institutions], Zbirnyk naukovyh prac Viiskovogo instytutu Kyjivskogo nacionalnogo universytetu imeni Tarasa Shevchenka. VIKNU, 2020. № 68. c. No. 68, pp. 90 – 99.

[19] Khlaponin Y.I., Vyshniakov V.M., Prygara, M.P. and Poltorak, V.P. (2021) The New Con- cept of Guaranteeing Confidence in the E-voting System.