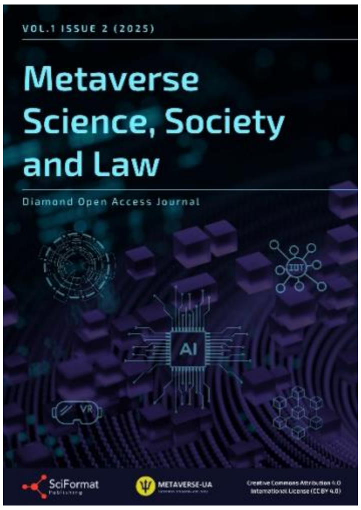

VOL.1 ISSUE 2 (2025)
Metaverse Science, Society and Law
Diamond Open Access Journal
AI
VR
SciFormat
METAVERSE-UA
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Metaverse Science, Society and Law

Vol. 1, Issue 2 (2025)

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

☎ +15878858911
✉ editorial-office@sciformat.ca

ARTICLE TITLE	AUTOMATED COMPLEX "ELECTRONIC SIGNATURE OF THE VOTER (EPO)" AS AN ELEMENT OF THE CRITICAL INFRASTRUCTURE OF THE ELECTION PROCESS
DOI	https://doi.org/10.69635/mssl.2025.1.2.26
RECEIVED	23 August 2025
ACCEPTED	25 November 2025
PUBLISHED	05 December 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

AUTOMATED COMPLEX "ELECTRONIC SIGNATURE OF THE VOTER (EPO)" AS AN ELEMENT OF THE CRITICAL INFRASTRUCTURE OF THE ELECTION PROCESS

Dmytro V. Zhuravlov
D.Sc. (Law), Professor, Honored Lawyer of Ukraine Office of the President of Ukraine, Ukraine
ORCID ID: 0000-0002-2205-6828

Dmytro D. Zhuravlov
Graduate Student Private Joint Stock Company "Higher educational institution "Interregional Academy of Personnel Management", Ukraine
ORCID ID: 0000-0003-0353-0544

ABSTRACT

The article studies the automated complex "Electronic Voter Signature" (EPO) as an element of the critical information infrastructure of the election process. It is shown that modern electoral systems can no longer rely solely on paper procedures and traditional identification mechanisms, as the intensity of cyber threats aimed at undermining trust in voting results is increasing. A system model of the EPO complex is proposed, in which key modules are allocated: biometric verification of voters, cryptographic protection and signature, management of voting sessions, logging and auditing, integration with the electronic voting system, as well as security monitoring subsystems based on Zero Trust, IDS (intrusion detection systems) and SIEM (centralized event correlation) approaches. To assess the reliability and stability of the complex, probabilistic models of reliability theory, indicators of average uptime (MTBF) and mean recovery time (MTTR), availability factor and generalized stability function were used. Special attention is paid to modeling cascade failures in the network of district nodes interacting through secure channels, using graph models and simulation scenarios. To increase the effectiveness of cyber defense, the use of machine learning methods, in particular, deep architectures CNN+LSTM, AE+LSTM and Byte2Image transformations for analyzing network traffic and event logs is proposed. It has been demonstrated that the combination of redundant architectural solutions, the Zero Trust concept and intelligent anomaly detection systems allows achieving a significantly higher level of availability and resilience of the EPO complex compared to the basic configurations. A method for protecting the biometric identification and authentication unit by human face from spoofing attacks is proposed using algorithms for converting color image spaces into YCrCb and CIE L*u*v* and analyzing attack signs using the ETC classifier. The normative aspects of the regulation of electoral information systems in Ukraine were discussed, the need for formal recognition of electoral systems as a component of the national critical infrastructure was emphasized. Recommendations were formulated for the integration of cyber resilience requirements into national electoral and cybersecurity regulations, as well as directions for further research on risk modeling and evaluation of the effectiveness of hybrid ML/AI solutions in the electoral process.

KEYWORDS

Voter Electronic Signature, Critical Information Infrastructure, Reliability, Resilience, MTBF, MTTR, Zero Trust, IDS, SIEM, Machine Learning, E-Voting

CITATION

Dmytro V. Zhuravlov, Dmytro D. Zhuravlov. (2025) Automated Complex "Electronic Signature of The Voter (EPO)" as an Element of The Critical Infrastructure of The Election Process. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.26

Introduction

Electronic information systems of the electoral process are gradually acquiring the characteristics of a critical infrastructure, the continuous functioning and security of which determine the legitimacy of the formation of public authorities, public confidence in the results of voting and the political stability of the state. In these conditions, the issues of reliable identification and authentication of voters, fixation of the fact of expression of will and ensuring the integrity and irrefutable nature of voting data are of particular importance. One of the promising areas for the development of electoral technologies is the introduction of automated electronic voter signature (EPO) complexes, which combine biometric, cryptographic, network and software components into a single system architecture [1,2,3].

Unlike classic electronic signatures, which are mainly aimed at business entities and authorities, the EPO complex must function in conditions of mass use, heterogeneous technical environment of polling stations, variable quality of communication channels and an increased level of threats of targeted interference. This necessitates the consideration of the EPO not only as a cryptographic mechanism, but as an element of critical infrastructure with its inherent requirements for fault tolerance, redundancy, recoverability and cyber resilience [4,5,6].

The regulatory framework of Ukraine in the field of elections, electronic trust services and cybersecurity already contains several provisions relevant for the development and operation of such systems [7,8,9]. In particular, we are talking about the Law of Ukraine "On Elections of People's Deputies of Ukraine"[10], the Law of Ukraine "On the State Register of Voters"[11], the Law of Ukraine "On Electronic Trust Services"[12], the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [13] and by-laws that regulate the categorization of critical infrastructure facilities, etc. [14,15,16].

Comparative analysis shows that individual states, in regulations on information security and critical infrastructure facilities, already apply a risk-oriented approach, which provides for a detailed classification of information systems, establishing requirements for their fault tolerance, redundancy and incident response procedures [17,18]. The logic of such acts can be used as a model for building regulatory requirements for EPO complexes in Ukraine, considering the national characteristics of the electoral process and the standards of the Council of Europe and the OSCE for democratic elections [19,20,21].

The article is aimed at forming a system model of the automated complex "Electronic Signature of the Voter" as an element of critical information infrastructure, developing a mathematical apparatus for assessing reliability and stability, as well as substantiating architectural solutions that combine redundancy, modern cyber defense components (IDS, SIEM, Zero Trust) and machine learning methods for detecting anomalies. The scientific novelty of the work lies in the integration of approaches to the theory of reliability, simulation modeling of cascading failures and in-depth analysis of security events to a single framework for assessing the stability of electoral information systems [22,23].

Research methods

1. System model of the EPO complex

The automated complex of the EPO is considered as a distributed multi-level system, which includes: a module for biometric verification of voters, a cryptographic module for generating and verifying an EPO, a module for managing a voting session, a subsystem for logging and auditing, a module for integration with the electronic voting system, a subsystem for monitoring and responding to incidents (IDS, SIEM, Zero Trust), as well as a storage and backup infrastructure. At the level of logical description, the system is presented in the form of an oriented graph of dependencies, in which the vertices are modules and infrastructure nodes, and the edges are data channels and functional dependency relations. This allows the graph theory apparatus to be used to analyze cascading failures and localize critical nodes

The automated complex of EPOs, presented as an oriented graph of dependencies, allows you to efficiently analyze cascade failures and localize critical nodes using modern methods of graph theory. This approach is relevant for complex systems with many interdependent modules, such as biometric verification, cryptographic module, auditing, integration, monitoring, and redundancy.

Modeling a system as an oriented graph

Each module or infrastructure node is represented as a vertex of the graph, and functional and information dependencies are represented as oriented edges [24,25].

Absolute dependency between modules allows for the formalization of failure scenarios: if a critical module fails, it can cause cascading failure of dependent components [26,27].

This structure makes it possible to automate the construction of fault tree analysis (FTA) and Failure Modes and Effects Criticality Analysis (FMECA) for complex systems [28].

Detection and localization of critical nodes

To identify critical nodes, centrality metrics are used: degree (degree), mediation (betweenness), eigenvector centrality (eigenvector centrality) [29].

Nodes with high values of these metrics have the greatest impact on system resilience: their failure can cause large-scale cascading failures [30]

Graph algorithms allow you to determine a minimum set of nodes, the protection of which maximizes the system's resilience to failures [31].

2. Probabilistic reliability model and availability factor

For each module of the EPO complex, it is assumed that the failure rate is constant within the selected observation interval.

Basic formulas and approaches

−Uptime function: R_i(t) = e^ {-λ_i t}, де λ_i — Module failure rate [32].
−MTBF та MTTR : MTBF_i = 1/λ_i, MTTR_i = 1/μ_i, де μ_i — Recovery intensity [33].
−Availability Factor: A_i = MTBF_i / (MTBF_i + MTTR_i)[34].
−Serial connection: A_sys = ∏ A_i — System availability without redundancy [35].
−Parallel redundancy (1 з m): A_res = 1 - ∏ (1 - A_j) — for redundant subsystems [36].

Then the failover function of a single module can be described by the exponential law: R_i(t) = e^ {-λ_i t}, where λ_i is the failure rate of the i-th module. Mean Uptime (MTBF) and Mean Recovery Time (MTTR) are defined as MTBF_i = 1/λ_i, MTTR_i = 1/μ_i, where μ_i is the recovery rate. The availability factor of an individual module takes the form A_i = MTBF_i / (MTBF_i + MTTR_i). In the case of serial connection of modules, the availability factor of the system without redundancy is calculated as A_sys = ∏ A_i. If parallel redundancy of the type "1 of m" is implemented for individual critical subsystems, the availability factor of the corresponding subsystem is determined as A_res = 1 - ∏ (1 - A_j). Thus, it is possible to assess the impact of different redundancy strategies on the overall level of availability and resilience of the EPO complex.

3. Generalized stability function

To take into account not only purely reliable characteristics, but also cyber resilience, it is proposed to introduce a generalized resilience function F_res(t), which aggregates several indicators: availability of A_sys(t), probability of timely detection of an attack D(t), service stability indicator S(t) and the degree of preservation of data integrity C(t). In the simplest approximation, we can consider the linear convolution F_res(t) = w1 A_sys(t) + w2 D(t) + w3 S(t) + w4 C(t), where w_i are the weight coefficients determined by the expert. The value of F_res(t) ∈ [0; 1] can be interpreted as an integral index of the stability of the EPO complex in each scenario of operation.

4. Modeling cascading failures

The network of nodes of the EPO complex (district servers, regional nodes, central computing resources, cryptographic gateways) is considered as a graph G = (V, E), where V is a set of nodes, E is a set of edges (communication channels). To analyze cascade failures, simulation modeling is used, in which the failure of one node can with a certain probability cause overloading of adjacent nodes and their failure. This approach makes it possible to investigate scenarios of mass failures, for example, in the event of a large-scale DDoS attack or failure of backbone communication channels.

5. Integration of ML/AI components

The security monitoring system of the EPO complex includes a network IDS, a SIEM platform and the Zero Trust concept. To increase sensitivity and reduce the number of false positives, deep machine learning architectures AE+LSTM, CNN+LSTM, and Byte2Image transformations are used. AE+LSTM is used to analyze time series of log data, CNN+LSTM is used to classify network traffic patterns, and Byte2Image allows you to display raw network packets in the form of pseudo-images, over which CNN effectively isolates patterns inherent in different types of attacks [37,38,39].

6. Biometrics System Protection

A component of the security system provides a module for protecting the process of biometric identification and authentication by a person's face based on the ETC classifier and counteracts the most common methods of spoofing attacks: printed attack, using device displays (replay attack) and mask attack [40,41]. The algorithm for countering spoofing attacks is based on the transformations of the color space of the image into the spaces YCrCb and CIE L*u*v* for better allocation of ETC by the classifier of features of falsified images [31]. This approach focuses on the problem of detecting print attacks and display attacks but is also suitable for detecting mask attacks. The method is based on the use of color spaces YCrCb and CIE L*u*v*, provides the ability to analyze both individual images and video streams, and is also characterized by resistance to changes in background and face lighting conditions [[42],[43]]. To determine the effectiveness of the biometric protection system, the metric is used: HTER = (FAR + FRR)/2, where FAR is the coefficient of erroneously allowed identifications, FRR is the coefficient of erroneously prohibited identifications. The established value of the efficiency of the biometric protection system is HTER < 1%.

Research results

1. Assessment of the availability of the EPO complex under different redundancy strategies

To demonstrate the capabilities of the proposed methodology, let's consider a simplified example, in which three key modules are distinguished: the biometric verification module (M1), the cryptographic transaction server (M2) and the voting system integration module (M3). Assume the conditional values of MTBF and MTTR given below (the information is conditional in nature, used only to illustrate the application of the technique). Conditional simulation results are shown in Table 1.

Basic approaches to assessing accessibility

Unit Analysis: Highlighting key components (e.g., biometric verification, cryptographic server, integration with the voting system) allows you to separately assess their reliability and impact on the overall availability of the system.

Using MTBF and MTTR metrics: Mean Uptime (MTBF) and Mean Recovery Time (MTTR) are the baseline parameters for calculating the probability of system uptime during an election period.

- Redundancy strategies: Choosing between "1+1" (hot standby), "N+1" (cold standby), or distributed clusters has a significant impact on availability. For example, hot redundancy allows instant switching to a redundant module, while cold redundancy takes time to start [[44],[45],[46]].

Table 1. Reliability parameters of the modules of the EPO complex (conditional example)

Module	MTBF, год	MTTR, год	Availability Factor A_i
M1	30000	2	0,99993
M2	25000	3	0,99988
M3	40000	2	0,99995

In the absence of redundancy, the total system availability factor (serial connection) is approximately A_sys ≈ 0.99976. If we implement redundancy of the "1 out of 2" type for the cryptographic operation server with the same parameters for the main and backup nodes, we will get A_M2^res ≈ 0.999999, which increases the overall availability of the complex to A_sys^res ≈ 0.99988.

2. The effectiveness of ML/AI components in incident detection

To evaluate the effectiveness of various approaches to detecting anomalies in traffic and log data, three configurations are considered: K1 – signature IDS without ML; K2 – AE+LSTM for log analysis; K3 – CNN+LSTM with Byte2Image for traffic and AE+LSTM for logs. Conditional simulation results are shown in Table 2.

Table 2. Comparison of Security Monitoring System Configurations (Conditional Data)

Configuration	Completeness of detection (TPR), %	Fraction of false positives (FPR), %	Cumulative F1-індекс
К1	78	9	0,81
К2	89	7	0,87
К3	94	5	0,91

3. Example of modeling cascading failures (code snippet)

Rice. 1 – Python code snippet for modeling cascading failures in the network of EPO nodes.

```
import networkx as nx
import random
def simulate_cascade(G, p_fail_initial=0.05, p_overload=0.3, steps=10):
    """
    Simulates cascade failures in the graph G.
    p_fail_initial – Baseline probability of initial node failure;
    p_overload – the likelihood of the node losing its performance in case of overload;
    steps – Number of Modeling Steps.
    """
    failed = set()
    # Initial set of bounces
    for node in G.nodes():
        if random.random() < p_fail_initial:
            failed.add(node)
    history = [set(failed)]
    for _ in range(steps):
        new_failed = set()
        for node in G.nodes():
            if node in failed:
                continue
            failed_neighbors = len([n for n in G.neighbors(node) if n in failed])
            if failed_neighbors == 0:
                continue
            p = 1 - (1 - p_overload) ** failed_neighbors
            if random.random() < p:
                new_failed.add(node)
        if not new_failed:
            break
        failed |= new_failed
        history.append(set(failed))
    return history
G = nx.erdos_renyi_graph(n=50, p=0.05, seed=42)
 cascade_history = simulate_cascade(G)
 print("Number of steps of the cascade:", len(cascade_history))
 print("Total Node Failure Rate:", len(cascade_history[-1]) / G.number_of_nodes())
```

4. The effectiveness of the protection system in detecting spoofing attacks

To determine the effectiveness of the anti-spoofing module, two publicly available image datasets were used, namely: CASIA FASD and Idiap REPLAY-ATTACK. In total, both datasets contain up to 2000 entries [32] with real access and attack attempts. Testing was carried out using the Python language and the OpenCV library, Scikit-learn. The results of testing the module are shown in Table 3.

Table 3. Comparison of Security Monitoring System Configurations (Conditional Data)

Method	Dataset	EER(%)	HTER(%)
Proposed solution: YC_rC_b+Luv+ETC	CASIA FASD	0.074	0.7
	Idiap REPLAY-ATTACK	0.074	0.58

From the data in Table 3, it can be concluded that the proposed module fulfills the requirement set for it and the HTER indicator < 1%.

The results of the simulation indicate that the automated EPO complex should be designed according to the principles characteristic of critical infrastructure facilities, and not as a "conventional" information system. This is consistent with the conclusions of international studies in the field of electoral infrastructure protection, which emphasize that attacks on electronic voting systems can be systemic in nature and combine technical, organizational, informational and psychological vectors of influence.

The Biometric Voter Identification Verification Complex (Electronic Voter Signature (EPO)) is a high-tech, multifunctional solution designed to guarantee the security, authenticity and efficiency of the electoral process in the context of the digital transformation of public administration. Its key function is to provide guaranteed, legally significant identification of the person participating in the vote through the integrated processing of several biometric parameters — the capillary pattern of the palms and the morphometric characteristics of the face. Conceptually, the complex was developed as a means of not only technical, but also legal trust in the expression of the will of citizens.

Structure and functional modules of the complex

1. Video analytics block for face recognition

The composition includes a high-precision digital video camera with a built-in real-time image analysis module. After scanning, an instant comparison of the morphological features of the user's face with the data stored in the encrypted voter database is performed. Deep learning algorithms allow you to consider age-related changes, minimal facial deviations and lighting conditions, as well as recognize attempts to disguise yourself as another person during biometric analysis of a person's face. The initial scan is entered into the database.

2. Palm capillary pattern scanning module

Built-in ultrasonic or optoelectronic capacitive sensors of the new generation read the unique microprofile of the capillary network of each palm. Two-factor scanning of both hands allows you to achieve an accuracy of more than 99.99%, which is superior to standard fingerprint-based identification methods. Thanks to the non-contact method, the risk of transmission of infections or mechanical damage to the sensor is eliminated. The initial scan is entered into the database.

3. User Touch Panel

The high-resolution touchscreen provides an intuitive interface. The voter receives step-by-step instructions, confirmation of identification and, if necessary, informative feedback on further actions. The screen can adapt to the needs of people with visual or hearing impairments (multilingual mode, voice prompts, contrast interface).

4. Thermal printer of verification results

After the identification is completed, the system automatically prints a receipt certifying the completion of the procedure. The receipt indicates the voter's unique number, confirmation of successful authentication, a QR code to access the ballot (in the case of digital voting) or the number by which the voter will receive a paper ballot.

5. Digital Security and Data Protection Infrastructure

The system complies with the requirements of GDPR, ISO/IEC 27001 and DSTU ISO/IEC 27018. All biometric data is stored in encrypted form using blockchain identifiers and Confidential Cloud Vault technologies. Encryption unit for data transmission over data transmission channels. The possibility of multi-level authentication of system administrators and supervisory authorities is provided.

Scientific social and legal justification

In the context of a global demand for transparency of electoral processes, the introduction of biometric voter identification systems is not just a technical innovation, but a tool for strengthening trust in the electoral system as a key element of the democratic system [47,48]. Biometrics, in particular facial recognition technologies and analysis of the venous structure of the palm, minimizes the risks of double voting, document fraud or manipulation of the voter register.

The use of such a complex brings electoral processes closer to the principles of digital legitimacy, i.e. electronic action, which has legal force due to the reliability of the technical environment. In addition, the system ensures inclusivity by lowering barriers for voters with disabilities and the elderly thanks to an adaptive interface.

Here is a detailed and at the same time accessible description of the algorithm of action for a voter who uses a biometric verification complex when voting in elections. This algorithm takes into account the need for initial registration, identity verification and protected access to the expression of will:

1. Arrival of a voter at the polling station

When a person comes to the polling station, he turns to the members of the election commission and presents one of the official identity documents - for example, a passport of a citizen of Ukraine, an ID card or another document provided for by law.

2. Checking in the voter list and issuing a coupon

Members of the commission check the presence of a voter in **the state register of voters**. If everything is in order, the voter receives **a special ballot card** with a unique number. This number is not a vote or a ballot, but a technical identifier that serves as the key to the biometric verification procedure.

3. Approach to the verification complex

The voter approaches **the biometric verification complex**, which consists of:

– touch screen;

– video cameras for face recognition;

– sensors for scanning palms (left and right);

– thermal printer for printing a receipt.

4. Scanning procedure

– Instructions appear on the screen. The voter attaches:

– first, **both palms to the sensors** (the system fixes the unique capillary pattern of the veins);

– Then **it looks at the camera** (the system recognizes the face and compares it with the existing database).

– This procedure only takes a few seconds and does not require any special knowledge or skills.

5. Printing a receipt (confirmation of verification)

After a successful scan, the system:

– confirms that the person is a valid voter and has already been verified;

– **prints a receipt** with a registration number, QR code or unique code;

This receipt is legal proof that the person has the right to vote.

6. Receiving a ballot or voting through an electronic system

The voter has two options:

a) Paper voting:

The voter presents the receipt to the commission member and receives **a paper ballot**, with which he then votes in the classic way – he fills it out in the booth and puts it in the ballot box.

b) Electronic voting:

If an electronic system is implemented at the polling station, the voter can immediately vote **through the same complex**, choosing a candidate on the touch screen (the vote is recorded in a secure digital register).

7. Completion of the voting procedure

Upon completion, the voter can leave the polling station, making sure that his right has been exercised and his data is protected. A second vote or fraud attempt will be automatically blocked because the biometric profile has already been used.

This algorithm provides **a high level of security, eliminates duplication of votes,** and significantly increases **trust in the election process**, while remaining understandable and simple for the general public. If necessary, I can visualize this process in the form of a diagram or infographic.

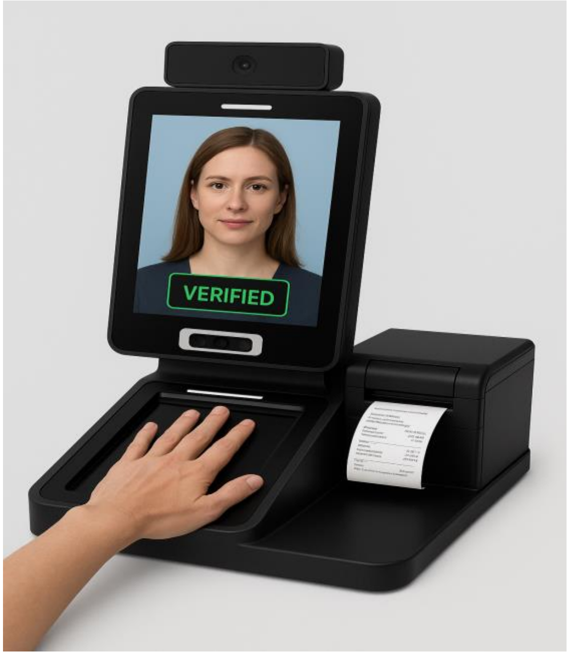
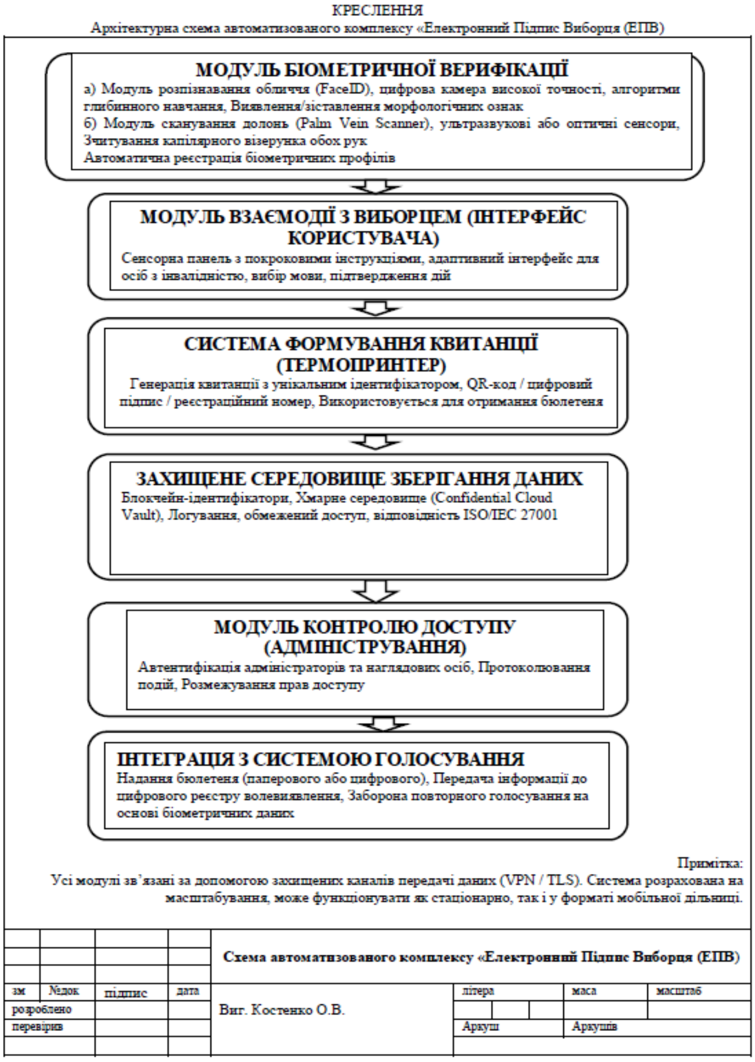


Fig.1. *Voter identification complex*

Comparison with the practice of other countries shows that an effective approach to ensuring the resilience of the CVO is the comprehensive application of categorization of objects by criticality levels, the establishment of minimum availability and redundancy indicators, requirements for the implementation of IDS/SIEM, vulnerability management procedures, and regulated incident response and audit procedures. The logic of these regulations can be adapted to Ukrainian realities, considering already adopted laws and by-laws in the field of cybersecurity and critical infrastructure protection.



КРЕСЛЕННЯ
Архітектурна схема автоматизованого комплексу «Електронний Підпис Виборця (ЕПВ)

МОДУЛЬ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ
а) Модуль розпізнавання обличчя (FaceID), цифрова камера високої точності, алгоритми глибинного навчання, Виявлення/зіставлення морфологічних ознак
б) Модуль сканування долонь (Palm Vein Scanner), ультразвукові або оптичні сенсори, Зчитування капілярного візерунка обох рук
Автоматична реєстрація біометричних профілів

МОДУЛЬ ВЗАЄМОДІЇ З ВИБОРЦЕМ (ІНТЕРФЕЙС КОРИСТУВАЧА)
Сенсорна панель з покроковими інструкціями, адаптивний інтерфейс для осіб з інвалідністю, вибір мови, підтвердження дій

СИСТЕМА ФОРМУВАННЯ КВИТАНЦІЇ (ТЕРМОПРИНТЕР)
Генерація квитанції з унікальним ідентифікатором, QR-код / цифровий підпис / реєстраційний номер, Використовується для отримання бюлетеня

ЗАХИЩЕНЕ СЕРЕДОВИЩЕ ЗБЕРІГАННЯ ДАНИХ
Блокчейн-ідентифікатори, Хмарне середовище (Confidential Cloud Vault), Логування, обмежений доступ, відповідність ISO/IEC 27001

МОДУЛЬ КОНТРОЛЮ ДОСТУПУ (АДМІНІСТРУВАННЯ)
Автентифікація адміністраторів та наглядових осіб, Протоколювання подій, Розмежування прав доступу

ІНТЕГРАЦІЯ З СИСТЕМОЮ ГОЛОСУВАННЯ
Надання бюлетеня (паперового або цифрового), Передача інформації до цифрового реєстру волевиявлення, Заборона повторного голосування на основі біометричних даних

Примітка:
Усі модулі зв'язані за допомогою захищених каналів передачі даних (VPN / TLS). Система розрахована на масштабування, може функціонувати як стаціонарно, так і у форматі мобільної дільниці.

Схема автоматизованого комплексу «Електронний Підпис Виборця (ЕПВ)

зм | №док | підпис | дата
розроблено
перевірив
Виг. Костенко О.В.
літера | маса | масштаб
Аркуш | Аркушів

Fig 2. *Architecture of the voter identification complex*

The introduction of ML/AI components (CNN+LSTM, AE+LSTM, Byte2Image) into the electoral infrastructure raises a new range of challenges related to the transparency and explainability of model decisions, the risk of data bias, dependence on the quality of training samples, and the possibility of targeted attacks on models. This requires a combination of a technical approach with legal and ethical regulation, including requirements for algorithm validation, certification of software and hardware complexes, and ensuring the possibility of external audit.

A separate area for discussion is the balance between increasing security through biometric identification and protecting voters' personal data. The use of biometrics in the context of an EPO can significantly reduce the risks of voting for another person, but at the same time creates sensitive data sets that, in case of compromise, cannot be "reissued" as a traditional password or token. Therefore, the architecture of the system should provide for strict requirements for the storage of biometric character patterns, their pseudonymization or storage only in the form of cryptographic fingerprints, which do not allow reconstructing the original images.

Conclusions

The paper proposes a system model of the automated complex "Electronic Signature of the Voter" (EPO) as an element of the critical information infrastructure of the election process. On the basis of the apparatus of reliability theory, probabilistic failure models and simulation modeling of cascade failures, an approach to assessing the availability and stability of the complex using MTBF, MTTR, availability factor and generalized stability function is formed. It is shown that even partial redundancy of individual critical modules (in particular, cryptographic operation servers and integration nodes) leads to a significant increase in the integral availability index.

The integration of Zero Trust approaches, IDS/SIEM systems, and deep machine learning models (AE+LSTM, CNN+LSTM, Byte2Image) increases the likelihood of timely detection of incidents and reduces the proportion of false positives, which has a positive effect on the D(t) component of the generalized resiliency function. For the biometric verification complex, the ETC classifier model was used to detect spoofing attacks with an HTER efficiency of < 1%, which allows you to effectively detect falsification of biometric data. At the same time, ML/AI solutions require additional regulatory regulation in terms of transparency, validation, certification, and protection against targeted attacks.

Because of a comparative analysis of approaches to the regulation of critical facilities in Kazakhstan and other countries, the expediency of formal recognition of electoral information systems, in particular EPO complexes, as elements of the national critical infrastructure of Ukraine has been substantiated. This should be accompanied by the inclusion in electoral and cybersecurity legislation of requirements for minimum availability indicators, redundancy, audit procedures and incident response.

Promising areas for further research are the development of more detailed risk assessment models considering sociotechnical factors, the construction of multi-level digital twins of electoral infrastructure for testing in a virtual environment, as well as the formation of a regulatory framework that would integrate the EPO complex into the broader ecosystem of digital governance and e-democracy.

REFERENCES

[1] Faruk, M., Alam, F., Islam, M., & Rahman, A. (2024). Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Clust. Comput.*, 27, 4015-4034. https://doi.org/10.1007/s10586-023-04261-x.

[2] Shaikh, A., Adhikari, N., Nazir, A., Shah, A., Baig, S., & Shihi, H. (2025). Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman. *F1000Research*. https://doi.org/10.12688/f1000research.160087.1.

[3] Potluri, P., Jayakarthik, R., Agarwal, S., S, S., S, V., & R, A. (2024). A Comprehensive Evaluation of Secured Electronic Voting System Design based on Face Biometric Authentication Policy. *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 446-453. https://doi.org/10.1109/i-smac61858.2024.10714856.

[4] Alown, M., Kiraz, M., & Bingol, M. (2025). Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems. *IEEE Access*, 13, 20512-20545. https://doi.org/10.1109/access.2025.3531349.

[5] Prajapat, S., Gautam, U., Gautam, D., Kumar, P., & Vasilakos, A. (2024). Designing a Robust Quantum Signature Protocol Based on Quantum Key Distribution for E-Voting Applications. *Mathematics*. https://doi.org/10.3390/math12162558.

[6] Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS. *Journal of Security and Sustainability Issues*, 9, 977-992. https://doi.org/10.9770/jssi.2020.9.3(22).

[7] Terlyuk, O., & Terlyuk, I. (2025). Electronic Voting in Ukraine: Legal Aspects in the Context of Technological Innovations and Prospects. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. https://doi.org/10.23939/law2025.46.343.

[8] Gavrik, R. (2022). On the prospects of introduction of electronic voting in Ukraine in the context of implementation of the concept of development of electronic democracy and digitalization. *Uzhhorod National University Herald. Series: Law*. https://doi.org/10.24144/2307-3322.2022.70.45.

[9] Pavshuk, K., Mokhonchuk, B., Romaniuk, P., Liubchenko, O., & Murtishcheva, A. (2025). Possibilities of Implementing E-Voting System in Ukraine. *Politics in Central Europe*. https://doi.org/10.2478/pce-2025-0009.

[10] Verkhovna Rada Ukrainy. (2012). Pro vybory narodnykh deputativ Ukrainy [On the elections of people's deputies of Ukraine], Vidomosti Verkhovnoi Rady Ukrainy (VVR), 10-11, Art. 73. https://zakon.rada.gov.ua/laws/show/4632-

17#Text (vtratyv chynnistʹ, okrim polozhenʹ shchodo orhanizatsiyi ta provedennya promizhnykh vyboriv ta zamishchennya narodnykh deputativ Ukrainy, obranykh u zahalʹnoderzhavnomu vyborchomu okruzi, povnovazhenʹ yakykh dostrokovo prypyneni, shcho diyutʹ do nastepnykh cherhovykh abo pozacherhovykh vyboriv narodnykh deputativ Ukrainy, na pidstavi Kodeksu № 396-IX vid 19.12.2019, VVR, 2020, № 7, № 8, № 9, st.48).

[11] Verkhovna Rada Ukrainy. (2007). Pro Derzhavnyi reiestr vybortsiv [On the State Register of Voters], Vidomosti Verkhovnoi Rady Ukrainy (VVR), 20, Art. 282. https://zakon.rada.gov.ua/laws/show/1024-16#Text

[12] Verkhovna Rada Ukrainy. (2022). *Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy* [Law of Ukraine on electronic identification and trust services] (Law No. 2155-VIII, 2017, as amended by Law No. 2801-IX, 2022). *Vidomosti Verkhovnoi Rady Ukrainy*, *45*, 400. Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19

[13] Verkhovna Rada Ukrainy. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* [On the basic principles of ensuring the cybersecurity of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, *45*, 403. https://zakon.rada.gov.ua/laws/show/2163-19

[14] Polotnianko, O., Madryha, T., Pyrohovska, V., Pozniakov, S., & Berezovska-Chmil, O. (2024). Regulatory frameworks for securing electoral processes in Ukraine: managing information security challenges. *Multidisciplinary Science Journal*. https://doi.org/10.31893/multiscience.2024ss0702.

[15] Gudz, L. (2024). ENSURING HUMAN RIGHTS IN THE CONTEXT OF IMPLEMENTATION OF ELECTRONIC VOTING IN UKRAINE: PERSPECTIVES AND RISKS. *The Journal of V. N. Karazin Kharkiv National University, Series "Law"*. https://doi.org/10.26565/2075-1834-2024-37-07.

[16] Havrik, R. (2023). Estonian experience of electronic voting: prospects of implementation in Ukraine. *Economics. Finances. Law*. https://doi.org/10.37634/efp.2023.6.13.

[17] Khade., S. (2025). Enhancing Electoral Integrity: Implementation of a Secure E-Voting Platform. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. https://doi.org/10.55041/ijsrem41520.

[18] Jafar, U., Aziz, M., Shukur, Z., & Hussain, H. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors (Basel, Switzerland)*, 22. https://doi.org/10.3390/s22197585.

[19] Pavshuk, K. (2024). Trust in electronic voting: the Estonian case. *Problems of legality*. https://doi.org/10.21564/2414-990x.166.310197.

[20] Polotnianko, O. (2025). The use of modern information technologies during elections in developed countries. *Visegrad Journal on Human Rights*. https://doi.org/10.61345/1339-7915.2024.6.13.

[21] Son, S. (2021). Legal regulation of the universal European election process. *ScienceRise: Juridical Science*. https://doi.org/10.15587/2523-4153.2021.234520.

[22] Haripriya, T., G, V., Babu, M., Aswini, G., & S, R. (2024). Biometric System Based Electronic Voting Machine. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/cseit2410315.

[23] Abdullah, A., & Ali, N. (2025). Secure E-Voting System Utilizing Fingerprint Authentication, AES-GCM Encryption and Hybrid Blind Watermarking. *Journal of Applied Engineering and Technological Science (JAETS)*. https://doi.org/10.37385/jaets.v6i2.6223.

[24] Chen, C., Tan, D., Meng, X., & Gao, J. (2022). An influential node identification method considering multi-attribute decision fusion and dependency. *Scientific Reports*, 12. https://doi.org/10.1038/s41598-022-23430-3.

[25] Singh, K., Chandrasekar, V., Zou, W., Kurths, J., & Senthilkumar, D. (2025). Graph coloring framework to mitigate cascading failure in complex networks. *Communications Physics*. https://doi.org/10.1038/s42005-025-02089-y.

[26] Tigrek, R. (2019). Fault Management Based on Systems Description as Directed Graph With Absolute Dependence Relations. *IEEE Systems Journal*, 13, 3687-3696. https://doi.org/10.1109/jsyst.2019.2927404.

[27] Wang, R., Li, Y., Xu, J., Wang, Z., & Gao, J. (2022). F2G: A hybrid fault-function graphical model for reliability analysis of complex equipment with coupled faults. *Reliab. Eng. Syst. Saf.*, 226, 108662. https://doi.org/10.1016/j.ress.2022.108662.

[28] Xu, W., Liu, X., Wang, T., & Liu, X. (2025). Fault-tolerant adaptive synchronization for discrete high-order multi-agent systems with stochastic noise. *IEEE Transactions on Automation Science and Engineering,* 22, 14833-14842. https://doi.org/10.1109/tase.2025.3562514.

[29] Rivas-Dávalos, F., Toledo-Adame, D., & Martinez-Ceseña, E. (2025). Identifying core nodes in interaction graphs for critical component analysis in cascading failures of power grids. *Archives of Electrical Engineering*. https://doi.org/10.24425/aee.2025.153022.

[30] Kabir, S. (2017). An overview of fault tree analysis and its application in model-based dependability analysis. *Expert Syst. Appl.*, 77, 114-135. https://doi.org/10.1016/j.eswa.2017.01.058.

[31] Duan, D., Duan, D., Lv, C., Si, S., Wang, Z., Li, D., Gao, J., Havlin, S., Stanley, H., & Boccaletti, S. (2019). Universal behavior of cascading failures in interdependent networks. *Proceedings of the National Academy of Sciences*, 116, 22452 - 22457. https://doi.org/10.1073/pnas.1904421116.

[32] Issa, L., & Hassan, Z. (2021). Use of a modified Markov models for parallel reliability systems that are subject to maintenance. *Journal of Physics: Conference Series*, 1999. https://doi.org/10.1088/1742-6596/1999/1/012087.

[33] Çekyay, B., & Özekici, S. (2015). Reliability, MTTF and steady-state availability analysis of systems with exponential lifetimes. *Applied Mathematical Modelling*, 39, 284-296. https://doi.org/10.1016/j.apm.2014.05.029.

[34] Signoré, J. and Leroy, A. (2021). Markov modeling. *Springer Reliability Engineering Series*. https://doi.org/10.1007/978-3-030-64708-7_31 .

[35] Çekyay, B., & Özekici, S. (2015). Reliability, MTTF and steady-state availability analysis of systems with exponential lifetimes. *Applied Mathematical Modelling*, 39, 284-296. https://doi.org/10.1016/j.apm.2014.05.029.

[36] Torrado, N., Arriaza, A., & Navarro, J. (2021). A study on multi-level redundancy allocation in coherent systems formed by modules. *Reliab. Eng. Syst. Saf.*, 213, 107694. https://doi.org/10.1016/j.ress.2021.107694.

[37] Ain, N., Sardaraz, M., Tahir, M., Elsoud, M., & Alourani, A. (2025). Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach. *Sensors (Basel, Switzerland)*, 25. https://doi.org/10.3390/s25051346.

[38] Susilo, B., Muis, A., & Sari, R. (2025). Intelligent Intrusion Detection System Against Various Attacks Based on a Hybrid Deep Learning Algorithm. *Sensors (Basel, Switzerland)*, 25. https://doi.org/10.3390/s25020580.

[39] Susilo, B., Muis, A., & Sari, R. (2025). Intelligent Intrusion Detection System Against Various Attacks Based on a Hybrid Deep Learning Algorithm. *Sensors (Basel, Switzerland)*, 25. https://doi.org/10.3390/s25020580.

[40] Balamurali, K., Chandru, S., Razvi, M., & Kumar, S. (2021). Face Spoof Detection Using VGG-Face Architecture. *Journal of Physics: Conference Series*, 1917. https://doi.org/10.1088/1742-6596/1917/1/012010.

[41] Moon, Y., Ryoo, I., & Kim, S. (2021). Face Antispoofing Method Using Color Texture Segmentation on FPGA. *Secur. Commun. Networks*, 2021, 9939232:1-9939232:11. https://doi.org/10.1155/2021/9939232.

[42] Sharma, D., & Selwal, A. (2023). A survey on face presentation attack detection mechanisms: hitherto and future perspectives. *Multimedia Systems*, 29, 1527 - 1577. https://doi.org/10.1007/s00530-023-01070-5.

[43] Turhal, U., Yilmaz, A., & Nabiyev, V. (2023). A new face presentation attack detection method based on face-weighted multi-color multi-level texture features. *Vis. Comput.*, 40, 1537-1552. https://doi.org/10.1007/s00371-023-02866-2.

[44] Alown, M., Kiraz, M., & Bingol, M. (2025). Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems. *IEEE Access*, 13, 20512-20545. https://doi.org/10.1109/access.2025.3531349.

[45] Jafar, U., Aziz, M., Shukur, Z., & Hussain, H. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors (Basel, Switzerland)*, 22. https://doi.org/10.3390/s22197585.

[46] Juybari, M., Hamadani, A., & Ardakan, M. (2023). Availability analysis and cost optimization of a repairable system with a mix of active and warm-standby components in a shock environment. *Reliab. Eng. Syst. Saf.*, 237, 109375. https://doi.org/10.1016/j.ress.2023.109375.

[47] Kostenko O. V. Compromise of a personal electronic signature key. Legal scientific electronic journal. 2019. № 6. C. 266-269. DOI: https://doi.org/10.32782/2524-0374/2019-6/63

[48] Kostenko O. V., Prokopovich-Tkachenko D. I., Florov S. V. Legal risks of compromising a qualified electronic signature. Legal Scientific Electronic Journal. 2023. No. 11. Pp. 373-379. DOI: https://doi.org/10.32782/2524-0374/2023-11/91