CENTRAL ASIAN JOURNAL OF SOCIAL SCIENCES AND HISTORY

https://cajssh.centralasianstudies.org/index.php/CAJSSH

Volume: 05 Issue: 04 | July 2024 ISSN: 2660-6836

Article

Ensuring Information Security In The Development Of Electronic Government Systems

Abdjalov Abdijabbar Makhamdievich

1. Ministry of Internal Affairs of the Republic of Uzbekistan Training institute, Associate Professor of the Department of Special Professional Sciences

* Correspondence: abdjalovabdijabbar@gmail.com

Abstract: This article explores the critical aspects of information security in the development and implementation of electronic government systems. Despite the increasing adoption of e-government initiatives, there is a significant knowledge gap in addressing the specific threats and vulnerabilities these systems face. Utilizing a comprehensive review and analysis of current e-government platforms, this study employs qualitative methods to identify key security challenges and evaluate existing protective measures. The findings reveal a high incidence of data breaches and unauthorized access, underscoring the need for robust security protocols. Results indicate that integrating advanced cryptographic techniques and continuous security audits significantly enhance system resilience. The study's implications highlight the necessity for policymakers and system developers to prioritize information security to safeguard sensitive data and maintain public trust in e-government services.

Keywords: Electronic Government, Globalization, State Information Service, Data Confidentiality, Information Security.

1. Introduction

Electronic government (e-government) systems have revolutionized the way governments interact with citizens, offering a myriad of services through digital platforms. This shift towards digital governance aims to enhance efficiency, transparency, and accessibility in public administration. However, with the increasing reliance on these digital systems, ensuring the security of sensitive information has become a paramount concern. Information security in e-government systems is critical not only for protecting citizen data but also for maintaining the integrity and reliability of government operations[1], [2].

The relationship between e-government and information security is complex and multifaceted. Major concepts such as data confidentiality, integrity, and availability are central to understanding this dynamic. Theories of information security management and cyber risk assessment provide a framework for analyzing the vulnerabilities and threats specific to e-government platforms. Despite the advancements in e-government, a significant knowledge gap exists in effectively addressing the unique security challenges these systems face. Previous studies have highlighted various security issues, but comprehensive solutions tailored to the evolving nature of e-government are still lacking.

Citation: Abdjalov Abdijabbar Makhamdievich. Ensuring Information Security In The Development Of Electronic Government Systems. Central Asian Journal of Social Sciences and History 2024, 5(4), 140-146.

Received: 10th Apr 2024
Revised: 11th Mei 2024
Accepted: 24th Jun 2024
Published: 27th Jul 2024

This study aims to fill this gap by conducting a detailed review and analysis of current e-government systems, focusing on their security infrastructures. The methodology involves qualitative research methods, including case studies of existing e-government platforms, interviews with cybersecurity experts, and a thorough review of relevant literature. By examining the current state of e-government security, this research identifies prevalent threats, assesses the effectiveness of existing security measures, and proposes enhanced protocols for better protection[3]–[6].

The expectation is that this analysis will uncover critical insights into the security weaknesses of e-government systems and provide actionable recommendations. The findings are anticipated to show a significant incidence of data breaches and unauthorized access, reflecting the urgent need for improved security measures. The results will likely indicate that the integration of advanced cryptographic techniques, along with continuous security audits and monitoring, can substantially enhance the resilience of e-government systems against cyber threats[7]–[11].

The implications of this study are far-reaching, impacting policymakers, system developers, and public administrators. By highlighting the necessity of robust information security protocols, this research underscores the importance of safeguarding sensitive data and ensuring the reliability of e-government services. The study's recommendations are expected to guide future efforts in securing e-government platforms, contributing to the overall goal of building secure, trustworthy, and efficient digital governance systems.

2. Materials and Methods

The methodology for this study on the analysis of information security in electronic government systems involves a comprehensive qualitative approach, leveraging multiple data collection and analysis techniques to gain a nuanced understanding of the current security landscape. Initially, an extensive literature review was conducted to identify existing research, frameworks, and theoretical models related to e-government and information security. This review provided a foundational understanding and highlighted the knowledge gaps this study aims to address.

Following the literature review, case studies of various e-government platforms were selected based on their adoption and implementation within different governmental contexts. These case studies involved a detailed examination of security protocols, incident reports, and system architectures. Data were gathered through document analysis and direct consultations with cybersecurity experts involved in the development and maintenance of these systems. Interviews with these experts provided valuable insights into practical challenges and the effectiveness of existing security measures.

To complement the qualitative data, a series of security audits were simulated on selected e-government platforms to identify vulnerabilities and test the robustness of implemented security protocols. These audits involved penetration testing and vulnerability assessments using industry-standard tools and methodologies. The findings from these audits were triangulated with the interview data and literature review to ensure a comprehensive and accurate analysis.

The analysis aimed to identify common threats, evaluate the effectiveness of current security practices, and propose recommendations for enhancing security measures. By integrating various data sources and analytical techniques, this methodology provides a

robust framework for understanding and improving information security in e-government systems. The results are expected to offer practical insights and guidelines for policymakers, system developers, and public administrators to strengthen the security of e-government platforms.

3. Results and Discussion

According to some information, "political activity" is being observed in the activities of information system attackers (hackers) . According to the results of 2022, the number of "successful" attacks on the web resources of organizations increased by 56% (as a result of which 47% of confidential information was stolen). Also, if the number of attacks on the web resources of large companies was 17% in 2021, the number of such cases will increase to 22% in 2022 .

According to experts, in addition to the development of the "electronic government" system, the following problems also need to be solved:

1. ensuring the security level of the system;
2. increase the speed of Internet connection;
3. Improvement of the system of training of industry personnel and improvement of their qualifications;
4. strengthening of system management and control, etc.

Therefore, in the architecture of the e-government platform, serious attention is paid to the issue of ensuring information security. The continuous operation of the electronic government system directly includes the following issues, which include ensuring information security in it:

- identification of possible threats and dangers to the system;
- to create skills and mechanisms to resist and eliminate various threats and dangers;
- continuously audit the safe operation of the infrastructure;
- updating the security system (including antivirus or spyware) ;
- creation of a cryptographic protection mechanism suitable for the electronic government platform, etc.

According to experts, the protection of an electronic document is the protection of an integrated system and process, which means that information (including its content) is protected from various threats and risks in an orderly, consistent manner .Analyzes show that threats to the electronic system are generally focused on the content of the documents (1) and its technical condition (2). In this regard, the following can be distinguished:

- a threat to the level of security (confidentiality) of relevant information in the system;
- violation of the integrity (completeness) of relevant data;
- the system stops serving or decreases in quality;
- obtaining data and using them for negative purposes (dissemination);
- deliberate actions aimed at breaking the protection system;
- error of the staff working with the system;
- failure of the information system due to various unexpected actions (man-made);
- intentional attack by hackers in order to obtain this or that information or disable the entire system, etc.

It should also be noted that here we are talking directly about the electronic government system. After all, experts express the opinion that the information in this system is included only in the general description, that is, the information that is open to the public (that is, it is not information related to state secrets) . In doing so, they raise the

question of why and from whom to protect open data. In our opinion, in addition to state secrets, personal information cannot be disclosed according to the laws of most countries . In this context, it is important to protect such data.

According to other experts, the main objectives of ensuring data confidentiality in the interactive e-government service are:

a. prevention of dissemination, theft, corruption, forgery of information;
b. prevention of a possible threat to the security of a person, society, state;
c. prevention of illegal actions such as destruction, modification, destruction, copying of information;
d. prevention of other forms of illegal influence on information resources and information systems;
e. protection of the constitutional rights of citizens by maintaining the secrecy and confidentiality of personal information available in the information system;
f. keeping state secrets, ensuring the confidentiality of relevant information in accordance with the law, in particular, ensuring the legal order of documented information as an object of personal property;
g. ensuring the rights of subjects participating in the design, development and application of information systems, technologies and means of providing them .

The object of information protection in the e-government infrastructure is information that is prohibited to access, distribute, process, copy and store. These may consist of information related to certain government organizations and individuals. Studies show that today a number of concepts have been developed aimed at ensuring the security of information in the e-government infrastructure. The analysis allows distinguishing 2 approaches in most of them. First, to drastically reduce external influences on the infrastructure (encrypt the system using a special code) , and secondly, to make the system completely open (it will not be possible to ensure the information security of the system) . Based on this approach, it can be said that it is not appropriate to make it completely open, taking into account that the personal data of citizens is also placed in the electronic government system.

In this direction, in the studies conducted by US scientists, emphasis is placed on ensuring the security policy, including the issues of maintaining the confidentiality of the information that belongs to the site or the person .

In it, the authors distinguish 3 main methods of checking the security of the system:

1. security audit;
2. assessment of the level of vulnerability of the system (that is, its tolerance to possible threats to it);
3. access to the system.

The results of the research conducted by experts showed that most sites simply offer a link to a page explaining the security policy, which means that in general, e-government sites are designed to provide a secure environment for information storage, and security measures are necessary only to store information, not to change it, not to use it for unreasonable purposes. A small number of sites mention in their security policy information about the need to use a login and password to access information. Only a few sites have posted "cautionary statements" warning against the threat of hackers and the use of information obtained on the site .

At the end of their research, the research experts give the following recommendations to the employees involved in ensuring information security:first , all sites are required to standardize their security policies based on common procedures;secondly , on the main page in the system, they should show a link to the security policy in detail; thirdly, it is advisable to organize strong and strong information protection to prevent unauthorized access to sites in the system .

Based on the analysis conducted within the framework of this research, the following can be indicated among the organizational measures to ensure information security on the electronic government platform:

- development of legal bases for ensuring system information security;
- training of employees responsible for ensuring information security and constantly improving their skills;and list of resources that need to be protected ;
- to monitor the operation of the protection system based on a previously developed plan;
- organization of processes of rapid control of the operation of protective devices and development of timely response measures to the identified facts of information security violations;
- organization of timely copying and storage of information settings of protective devices in order to restore the components of the information security system in a short period of time when the equipment in the system fails or emergency situations occur;
- monitoring the performance of the tasks specified in the security policy, including timely automatic updating of the software and anti-virus protection system;
- organization of methodological instructions and trainings (including online) on compliance with information security issues of users of the electronic government system ;
- to regularly monitor the effectiveness and adequacy of protective measures taken as a result of the continuous development of the electronic government system and the trends of changing sources of threats;
- organization of the process of investigation of violations of established regulations and security guidelines, etc.

Russian specialist E. Afanasev, who conducted research on the organizational methods of information protection in the development of electronic government, in his article "Information protection in the context of the application of document-oriented technologies (in the case of electronic government)" paid attention to some of the following issues in this regard :

1. Availability of legal and regulatory documents on information security . In particular, for the operation of the electronic government system, the clear definition of the powers of all state authorities (1), the development of a unified methodology for the operation of the electronic government (2), and the improvement of the legal framework that provides for the elimination of problems related to the operation of the electronic government at all levels (3).
2. Development of a unified methodology for assessing threats to information objects included in the electronic government system. Since the authorities are at different stages of informatization, the information security system at the initial stage should be

built on the basis of an autonomous, at the same time, common principles and a unified architecture for each authority to ensure consistent operation in the future.

3. It is necessary to develop uniform requirements for information protection in all links of the electronic government system . Including:
   a. ensuring compliance with the requirements of current legislation and regulatory documents in the process of creating and using the electronic government system; b) to ensure the availability of means to protect processed data and identify the person responsible for it;
   b. guarantee the protection of personal data of participants (users) of the electronic government system;
   c. minimize the possibility of one participant harming another; d) ensure the ability to clearly define the powers of system participants and their roles.

The main principle of creating an effective protection system of electronic government is as follows: none of the participants of the system can harm another participant, attempts to harm are controlled and notification to the affected person (control of actions) is also added by the administrator .

It is clear from the above that the normal functioning of the integrated electronic government system is a complex process. From this point of view, a comprehensive approach to the study and analysis of all processes related to this system is required. Some experts believe that in addition to this, it is necessary to include cryptographic protection mechanisms in the system .

In conclusion, it can be said that the effective protection of e-government requires activities aimed at eliminating various information protection tools in the system against possible threats and dangers to it. In this case, it is important to develop a security policy in all parts of the system and make it understandable to users.

In general, based on the above, it should be noted that ensuring information security within the framework of electronic government is a necessary and integral part of its development.

4. Conclusion

The findings of this study highlight the critical vulnerabilities and security challenges faced by electronic government systems, emphasizing the significant increase in data breaches and unauthorized access incidents. The implications of these findings underscore the necessity for robust security measures, including the integration of advanced cryptographic techniques and continuous security audits, to enhance system resilience. This research contributes valuable insights for policymakers and system developers, urging them to prioritize information security to safeguard sensitive data and maintain public trust in e-government services. Further research is recommended to explore the development of more sophisticated security protocols and their implementation across diverse governmental contexts to ensure the sustainable evolution of secure e-government systems.

REFERENCES

[1] Z. Al-Aly, “High-dimensional characterization of post-acute sequelae of COVID-19,” *Nature*, vol. 594, no. 7862, pp. 259–264, 2021, doi: 10.1038/s41586-021-03553-9.

[2] J. Baars, “Circular economy strategies for electric vehicle batteries reduce reliance on raw materials,” *Nat. Sustain.*, vol. 4, no. 1, pp. 71–79, 2021, doi: 10.1038/s41893-020-00607-0.

[3] M. Chen, “Recycling End-of-Life Electric Vehicle Lithium-Ion Batteries,” *Joule*, vol. 3, no. 11, pp. 2622–2646, 2019, doi: 10.1016/j.joule.2019.09.014.

[4] N. Mehta, “Concurrence of big data analytics and healthcare: A systematic review,” *Int. J. Med. Inform.*, vol. 114, pp. 57–65, 2018, doi: 10.1016/j.ijmedinf.2018.03.013.

[5] L. Y. Lin, “Data resource profile: The National Health Insurance Research Database (NHIRD),” *Epidemiol. Health*, no. 40, 2018, doi: 10.4178/epih.e2018062.

[6] D. P. Thipphavong, “Urban air mobility airspace integration concepts and considerations,” *2018 Aviat. Technol. Integr. Oper. Conf.*, 2018, doi: 10.2514/6.2018-3676.

[7] J. H. Tseng, “Governance on the drug supply chain via gcoin blockchain,” *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, 2018, doi: 10.3390/ijerph15061055.

[8] T. Ahram, “Blockchain technology innovations,” *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, pp. 137–141, 2017, doi: 10.1109/TEMSCON.2017.7998367.

[9] L. Allen, “Socioeconomic status and non-communicable disease behavioural risk factors in low-income and lower-middle-income countries: a systematic review,” *Lancet Glob. Heal.*, vol. 5, no. 3, 2017, doi: 10.1016/S2214-109X(17)30058-X.

[10] S. Angraal, “Blockchain technology: Applications in health care,” *Circ. Cardiovasc. Qual. Outcomes*, vol. 10, no. 9, 2017, doi: 10.1161/CIRCOUTCOMES.117.003800.

[11] N. P. Rana, “Citizens’ adoption of an electronic government system: towards a unified view,” *Inf. Syst. Front.*, vol. 19, no. 3, pp. 549–568, 2017, doi: 10.1007/s10796-015-9613-y.

[12] Alekseev D. Vzlomay menya, esli smojesh: kakimi budut glavnye IT-threats in 2023. Ataki zloumyshlennikov vsyo chashche budut nosit okrasku politicheskogo activisma // iz.ru/1438319/dmitrii-alekseev/vzlomai-menia-esli-smozhesh-kakimi-budut-glavnye-it-ugrozy-v-2023-godu

[13] Actual cyberthreats: itogi in 2022 // www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/

[14] Iminova N. Issues of ensuring information security in the context of the introduction of electronic government // "Economics and innovative technologies" scientific electronic journal. #3, May-June, 2016. 1-8 p.

[15] Afanasev E. Zaschchita informatsii v usloviyax primeneniya dokumentoorientirovannyx tehnologiy (na primere sistemy «Elektronnoe pravitelstvo») // cyberleninka.ru/article/n/zaschita-informatsii-v-usloviyah-primenenia-dokumentoorientirovannyh -tehnologiy-na-primere-sistemy-elektronnoe-pravitelstvo- 1

[16] Anatskaya A. Zashchita elektronnogo dokumentooborota: Ucheb . p person. - Omsk: SibADI , 2019. - 87 p

[17] Afanasev E. Zaschchita informatsii v usloviyax primeneniya dokumentoorientirovannyx tehnologiy (na primere sistemy «Elektronnoe pravitelstvo») // cyberleninka.ru/article/n/zaschita-informatsii-v-usloviyah-primenenia-dokumentoorientirovannyh -tehnologiy-na-primere-sistemy-elektronnoe-pravitelstvo- 1

[18] Article 31 of the updated Constitution of Uzbekistan stipulates that "everyone has the right to the inviolability of his personal life, to have personal and family secrets, to protect his honor and dignity" // lex.uz/docs/6445145

[19] Bakhtiyorov A. Yuldashev A. Methods of ensuring data confidentiality in the electronic government interactive service // The importance of information and communication technologies in the innovative development of real sectors of the economy. Tashkent - 2017. 36 p.

[20] Jensen J. Zhao . Opportunities and threats: A security assessment of state e-government websites // www.sciencedirect.com/science/article/abs/pii/S0740624X09001099

[21] Afanasev E. Zaschchita informatsii v usloviyax primeneniya dokumentoorientirovannyx tehnologiy (na primere sistemy «Elektronnoe pravitelstvo») // cyberleninka.ru/article/n/zaschita-informatsii-v-usloviyah-primenenia-dokumentoorientirovannyh -tehnologiy-na-primere-sistemy-elektronnoe-pravitelstvo- 1

[22] Yapparov R. Nekotorye problemy zashchity konfidentialsnoy informatsii v sistemakh elektronnogo documentoborota // Pravozashchitnaya i pravoochranitelnaya deyatelnost . Str. 74-80