INFORMATION PROTECTION MECHANISM IN THE ".UZ" DOMAIN

Gafurov Sh. A.
Independent researcher of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract:
In this article, the conceptual model of the national segment of the Internet network in the e-government platform is researched. a mechanism for protecting information from attacks in domains located in the national segment of the Internet network is proposed.

Keywords: website, electronic government, eGov system, cyber-attacks, web resources, efficiency, integration.

Convenience, transparency and reliability of socio-economic interactive services provided by specialists of all state and non-state organizations in society to citizens (with registration to all Internet users) are directly related to the usability of the ".uz" domain platform of the national segment of the Internet network. is a related issue. In addition, the ".uz" domain of the Internet network, in turn, determines the following:

- of the ".uz" domain in the technological processes of state administration ;
- in the ".uz" domain of the Internet network ;
- the presence of possible threats and protection mechanisms directed to the ".uz" domain of the Internet network .

in the ".uz" domain and ways to protect them can be suggested as follows. It includes networks of interconnected state organizations, a complex security system, a cloud platform of the ".uz" domain that provides data exchange and application support, and the interconnection of offices for state agencies and administrative services. can be expressed in the form of a conceptual model of the ".uz" domain in the e-government platform, which includes the centralization and unification of the communication platform and network operation, system maintenance and service management .

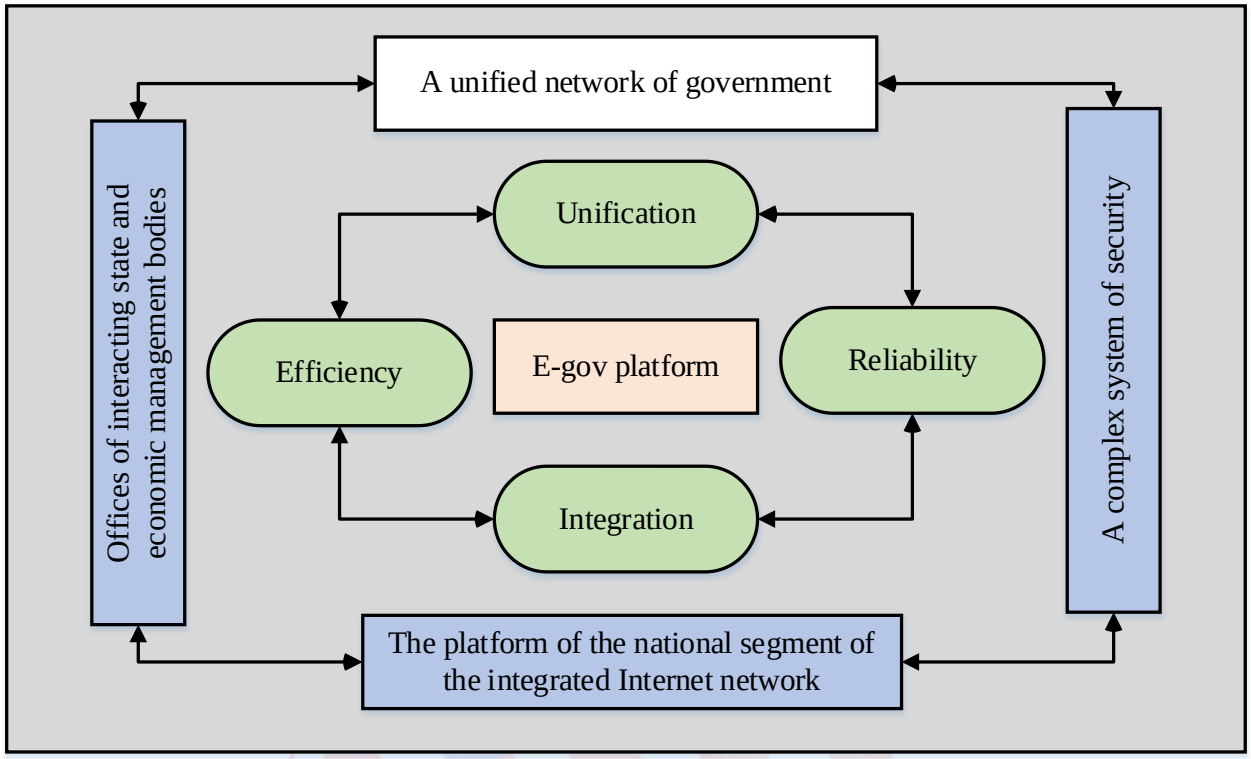

Figure 1. Conceptual model of the national segment of the Internet network in the e-government platform

In turn, a cloud platform is offered as a solution to ensure security in the infrastructure of the ".uz" domain, and the main task is to build a complex system of network security for protection against unauthorized access and cyber attacks, along with the data reception, processing and transmission module. . Generally, ".uz" domain security is required to be protected with a level 3 information protection system based on the world standard and national standards. In addition, ".uz" domain security information using systems that support visual network monitoring and protect users from internal and external threats with the help of comprehensive security protection.

In this case, comprehensive protection - meeting the requirements of the ".uz" domain and secure integration into electronic government systems created the following advantages:

- simplified management of access to the Internet, that is, the possibility of minimizing information security risks;
- a single security platform, i.e. the ability to visually monitor traffic and effectively manage risks;
- providing level 3 protection in network isolation and access control;
- collects information about various security incidents and activates protection mechanisms to identify threats in the ".uz" domain .

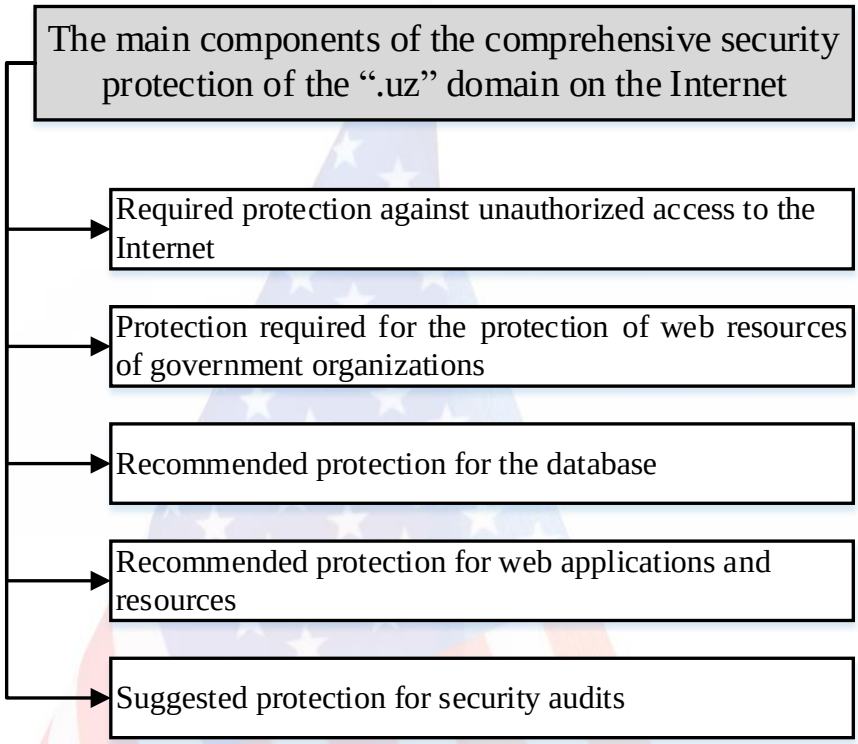

Figure 2. The main components of the comprehensive protection of information security in the ".uz" domain

Based on these advantages, it is possible to protect against potential threats to web applications and resources located in the ".uz" domain. As a result, the following opportunities are created:

- the website and web resources ;
- ensure the security of files on the web server;
- organization of a simplified security audit;
- m ensuring the security of data processing centers;
- organizing work online;
- securing network boundaries.

The information gathering function of a multi-layered security system causes the system to send alerts and reports when security threats are detected.

In the principles of information security for the security of web applications and resources located in the ".uz" domain, presented in international standards, it is recommended to use a multi-level approach to information security in order to protect their systems from all sources of threats. But this does not always mean that it is appropriate. Such situations are appropriate only in the local or corporate network of the organization, otherwise, it is not recommended in the global network.

Based on this, the infrastructure of web applications and resources located in the ".uz"domain serves as a system of information security. Protection in this way allows to fight and prevent information security incidents caused by internal or external threats to web applications and

resources located in the ".uz" domain in several formats . The proposed method consists of two separate solutions for estimating information security in web applications and resources located in the ".uz" domain, that is, a solution for incidents caused by external threats and a solution for security incidents caused by internal threats. In this, structured and unstructured threats are considered as internal and external threats. When implementing the proposed method, it is necessary to ensure a high level of filtering of data in the ".uz" domain, blocking external attacks .

References

1 I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in: ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secure. Priv., 2018, pp. 108–116.

2 R. P atil, H. Dudeja, C. Modi, Designing an efficient security framework for detecting intrusions in virtual network of cloud computing, Comput. Secure. 85 (2019) 402–422.

3 SD Cakmakci, H. Hutschenreuter, C. Maeder, and T. Kemmerich, "A Framework for Intelligent DDoS Attack Detection and Response Using SIEM and Ontology," 2021 IEEE Int. Conf. Commun. Work. ICC Work. 2021 - Proc., pp. 7–12 .

4 CM Ahmed, MR Gauthama Raman, and A. P. Mathur, "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems," CPSS 2020 - Proc. 6th ACM Cyber-Physical Syst. Secure. Work. Co-located with AsiaCCS 2020, pp. 23–29 .

5 M. Arafat, A. Jain, and Y. Wu, "Analysis of intrusion detection dataset NSL-KDD using KNIME analytics," Proc. 13th Int. Conf. Cyber Warf. Secure. ICCWS 2018, vol. 2018-March, pp. 573–583, 2018.