DOI: 10.33498/louu-2020-04-225-244

Rzayeva Gulnaz Aydin

PhD in Law, Lecturer at the UNESCO Department of "Human Rights and Information Law" of Baku State University, Lecturer at Law faculty of Academy of State Customs Committee of the Republic of Azerbaijan
(Baku, Azerbaijan)
ORCHID ID: https://orcid.org/0000-0001-5305-7113
gulnazaydin@yahoo.com

Ibrahimova Aytakin Nazim

PhD in Law, Deputy Dean of Law Faculty of Baku State University, Professor at the Department of "Constitutional Law" of Baku State University
(Baku, Azerbaijan)
ORCHID ID: https://orcid.org/0000-0002-3134-8486
aytakin_ibrahimli@yahoo.com

УДК 342

ORGANIZATION OF INFORMATION SECURITY IN E-GOVERNMENT AS MEANS OF INFORMATION RIGHTS PROTECTION

Abstract. As a concept, electronic government is directed to improving the efficiency of the activity of the state institutions and improving the living standards of citizens. Formation of the electronic state determines the pace of development of human rights and freedoms in accordance with the requirements of the time, among which the rights of information are of particular importance. However, in a situation where the completeness, accessibility and confidentiality of information is not fully ensured, there are obstacles to the realization of information rights. Therefore, the organization of information security is one of the means of guaranteeing information rights. In this regard, information security should be analyzed not only from technical aspect but also from human rights law. These highlights confirm the relevance of the topic of the article.

The article's objective is to analyze the notions "e-government", "e-parliament" and "e-court", to list priorities of e-state from aspect of human rights and freedoms provision, to determine the legal, theoretical and technical approaches to the information security

in various models of e-government, to define difference between electronic security or information security, to research the importance of e-governance from the human rights aspect and to put forward suggestions about protection of information rights violated in cyberspace.

The authors conclude that, full access to information, in new society ensures information and other rights and freedoms. Therefore, the lack of information security or low level of information security prevents the e-government from benefiting its citizens. One such barrier is considered an electronic divide or digital divide. Due to the global nature of cyberspace and information society, these problems should be solved not only at national level but also internationally. Above all, security should not be taken from the technical aspect. This prevents problems from being solved. Information security should also be analyzed as a legal institution, and the distinction between the terms "information protection" and "information defence" should be clarified. The legal aspect of the matter should be expressed.

Thus, the authors conclude with an optimistic approach that elimination the problems arising during the formation of e-government will serve both to promote basic human rights and freedoms, and to make every citizen an active member of the digital society.

Keywords: information rights; information security; e-parliament; e-government; e-court; security tendencies; e-security.

The changes and innovations that are launched in the information society also affected economic, social, political and cultural life. A new state concept – *e-state model* came to the forefront as a result of changes in governance. Public administration backed by defining characteristics such as open, transparent, participatory, convenient, expedient and effective characteristics as a result of the formation of e-state replaced traditional public administration. "E-state" is a considerably elaborated topic in terms of both conception and application and it is studied in many scientific researches and literature for a short while as a consequence of attention paid to e-governance on both international and national level.

The formation of the e-state led to a radical change in many traditional approaches. So, virtual "twins" of real creatures emerged in the world with the influence of Internet: traditional education is replaced by e-learning, traditional science- with e-science, citizen-by e-citizen, (digital), traditional state with e-state and traditional commercial with e-commerce, etc. Thus, the world will be consolidated by the unity of these "twins" and incompleteness (problems), inherited from the past will be eradicated. Therefore, the rights and freedoms already existed in the traditional world are taking new form and content. Given that ICT plays a key role in e-governance, inadequacy of information security and electronic security can ultimately increase the number of human rights violations. It is essential to pay special attention from this point of view to such aspects of e-state activity.

Priorities of e-state from aspect of human rights and freedoms provision

Electronic state development, which is a topical issue of our time is not a fashionable project and should be interpreted as a new form of securing human rights and freedoms. The e-state is understood as the state that provides individuals and legal entities with information and ensures one's total development via own security. The e-state aims to ensure transparency in public administration. The idea of e-state is realized with the development of websites of the state, where the state fulfils citizen's rights to free access to information, bears responsibility for the information contained within electronic systems and fulfils the function of communication mean.

There are many definitions of e-state in the literature. R. Heeks explained e-state as the application of information and communication technologies to enhance the activities of government agencies[1].

D. L. McClure, the Deputy Chief of General Accountant Office of the United States, expressed his views on e-state in this way: The e-state has the potential to create a better relationship between the state and the public, providing more convenient and effective interaction with the citizen[2].

The Turkish author M. Yıldız described the e-state in his article as the ability of state's organizational bodies to use ITC technologies in order to provide information and secure democratic governance[3].

According to other interpretation, e-state is state system where all public services are provided electronically. Citizens will be able to access public services in an easy and cost efficient way avoiding bureaucratical impediments in the system. The e-state should not be understood only as an electronization of state's all programs[4].

The e-state together with its activities brings about a significant improvement in transparency and quality of public administration by accelerating the process, but first simplifying these relationships and reducing financial costs. Government agencies cannot fulfill their commitments because of the high level of red tape.

Paper-based work required for the provision of commitments and services extends the duration of work, consequently, increases the expenses and therefore the overall expenditure of the state budget. E-state activities can bear an impact of introducing positive changes on improving the opportunities and

[1] Richard Heeks, 'Understanding e-Governance for Development' (2001) 11 iGovernment Working Paper <https://ssrn.com/abstract=3540058> (accessed: 22.03.2020).

[2] United States. General Accounting Office. *Electronic Government: Federal Initiatives Are Evolving Rapidly but They Face Significant Challenges* (May 22, 2000) <https://digital.library.unt.edu/ark:/67531/metadc290097> (accessed: 22.03.2020).

[3] M Yıldız, 'Uluslararası Kuruluşların Türkiye nin E-devlet Siyasalarına Etkisi' [2007] 40 Amme *İdaresi* Dergisi 39.

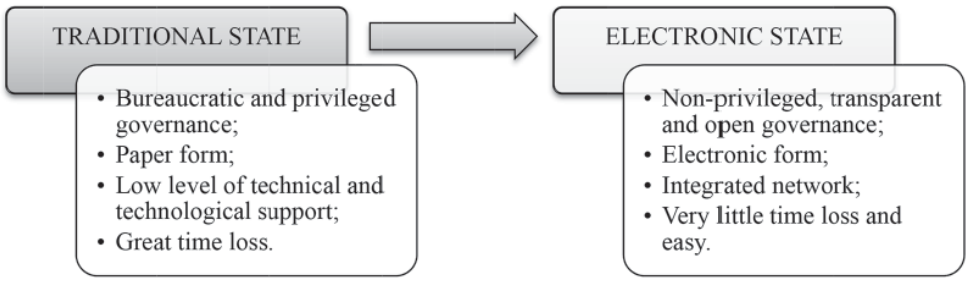
[4] Asma Al-Hashmi and Abdul Basit Darem, 'Understanding Phases of E-government Project' in Sahu G P (ed), *Emerging Technologies in E-Government* (Gift Publishing 2009) 152.

ПРАВО УКРАЇНИ • 2020 • № 4 • 225-244

quality by reducing these financial costs and shortening the deadlines. Citizens' access to any kind of public services causes their satisfaction with the state. Bureaucracy will be greatly reduced with e-state and users will be able to get service indirectly and also standardization of public services will be ensured. *Benefits of e-state for citizens and the state* can be grouped as follows[5]:

FOR CITIZEN	FOR STATE
Ability to access information without assistance;	Reduce dependence on external means;
Easy access and use of information;	Decrease in access information using classical means;
Progress in building mutual relations with the state;	Easier and faster access to information;
Rapid resolution of problems;	Prevention of delays in public services
Increasing citizens' trust in the state;	Increasing citizen satisfaction for better service;
Active participation of citizens in governance;	Establishing fast relations within the state and abroad;
Ability to access information at any time and place.	Increase in activity of state bodies.

Thus, e-state by these advantages offers a number of easier and more convenient forms of implementation than traditional form of governance



Society operates not for the state, but the state functions for the society in e-state. Therefore, if the state implements information policy without regard to

[5] Demokan Demirel, 'E-Devlet ve Dünya Örnekleri' (2006) 61 Sayıştay Dergisi 94.

the interests of citizens, such a policy can be considered as failure. In this regard, it would be appropriate to mention cybercopying and cyber-pessimistic approach division of the Ronald Meinardus, Regional Director for East Asia and North Africa regions of Friedrich Naumann Foundation. According to R. Meinardus, cyberoptimists believe that, ICT development has a positive impact on civic society. Accessibility to information and knowledge will ultimately enable civil society members to participate equally in all sectors of society. The use of ICT will also facilitate the development of democratic elements.

However, cyberpessimists on the contrary, claim that Internet has opposite effect. Internet will lead to the gap between the rich and the poor, those who are actively and passively involved in political life, in their opinion. Proponents of this position try to prove their interpretations based on statistic indicators: According to statistics data of Organization for Economic Co-operation and Development, 54,3 % of Americans used Internet every day in the early 21st century, while this figure was 0,4 % in Africa. The fact of the hegemony of the developed countries suggests that English language is used in cyberbullying[6]. The interpretation of cyberpessimistic position cannot be rejected. Indeed, digital inequality prevails in the modern world. However, this inequality is not the result of the development and implementation of ICT. The reasons for digital inequality are the differences existing in traditional society and harsh and one-sided laws and legal procedures of traditional societies.

On the contrary, the development of e-society and the elimination of this inequality was set as a target. It is no coincidence that, the idea of creating knowledge societies in UNESCO reports, as well as the issues related to the preservation of cultural heritage and linguistic diversity is aimed at ensuring equal participation of all people in ICT applications. At the same time, the principle of the joint participation of public administration bodies and stakeholders in the application of ICT for development envisaged by the Declaration of Principles also recognizes the civil society. On the other hand, it would be wrong to deny the positive impact of ICT on the development of society in modern times. In most cases, the informatization process results in increased citizen engagement. For example, it is possible to increase voter turnout with the help of electronic voting, etc.

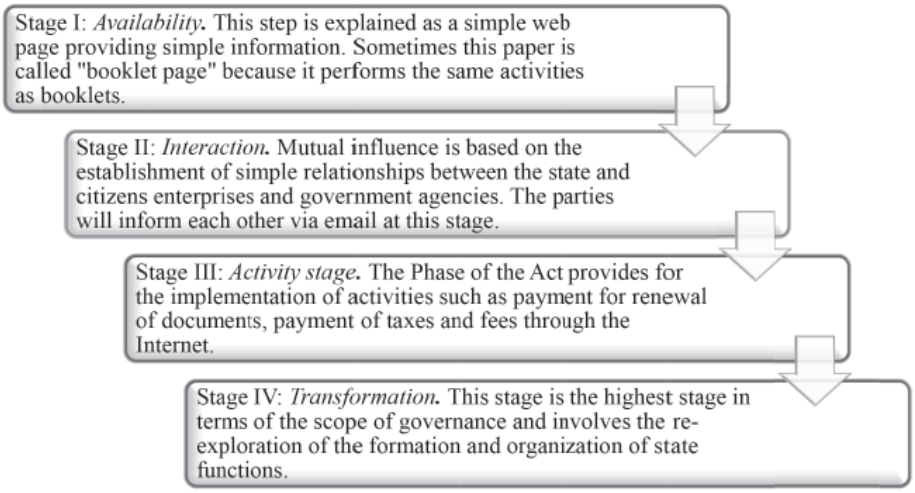
E-state models and overall citizen satisfaction

E-state cannot be applied as a single-stage simple project. E-state is a secular activity that involves several stages and periods of development. Different models of development can be encountered in literature. Let's explore three

[6] Ronald Meinardus, 'The Political Impact of the Internet' Business World Internet Edition (March 26, 2003, and March 27, 2003).

of the best-known models amidst these models: *Gartner model, Layne and Lee development model, UN e-government approach and the World Bank model:*

Gartner's 4-stage e-state development model. According to the research conducted by Gartner's team, it was determined that from the point of view of identifying the stages of e-state development and developing a roadmap to ensure customer services' qualitative level, e-state development stage consists of four phases[7]:

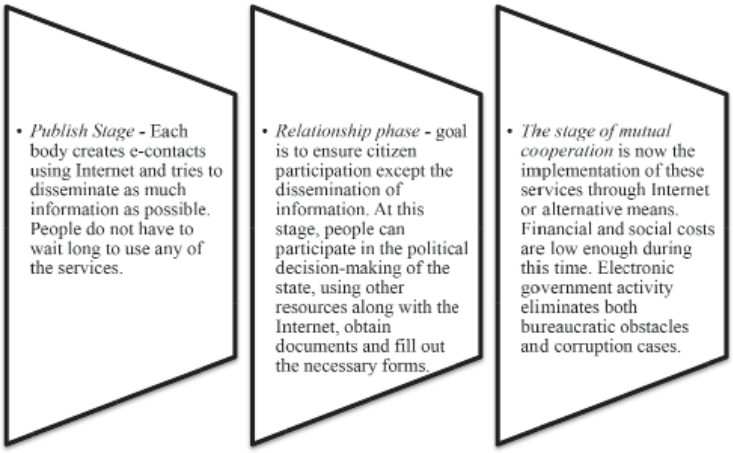


Development model developed by the World Bank. This model was published in "E-Government Handbook for Developing Countries" in 2002. The World Bank stated the stages of the project developed by the World Bank are not interconnected, and that it is not necessary to complete the previous phase to start the next stage. Stating that three phases of the model presented are also a way to reach the goals of the e-government, the World Bank explains the stages and the characteristics of these stages as followings[8]:

According to the World Bank's approach, in order to provide proper means of communication for public services, states create web pages where users can operate online in the final stage of e-government development. The reason for setting a obligatory requirement of ICT application is connected with states' will to regulate hard and difficult work conditions. The main reason is that the long-term thrift can be achieved and productivity can be increased in this way. Citizens had to face bureaucracy and corruption in the past as they had to wait

[7] M Alshehri and S Drew, 'Implementation of e-Government: Advantages and Challenges' in *International association for scientific knowledge (IASK) E-ALT Conference proceedings* (2010) 79–86.

[8] 'E-Government Handbook for Developing Countries' *(A Project of InfoDev and The Center for Democracy & Technology)* <http://www.infodev.org/infodev-files/resource/InfodevDocuments_16.pdf> (accessed: 22.03.2020).

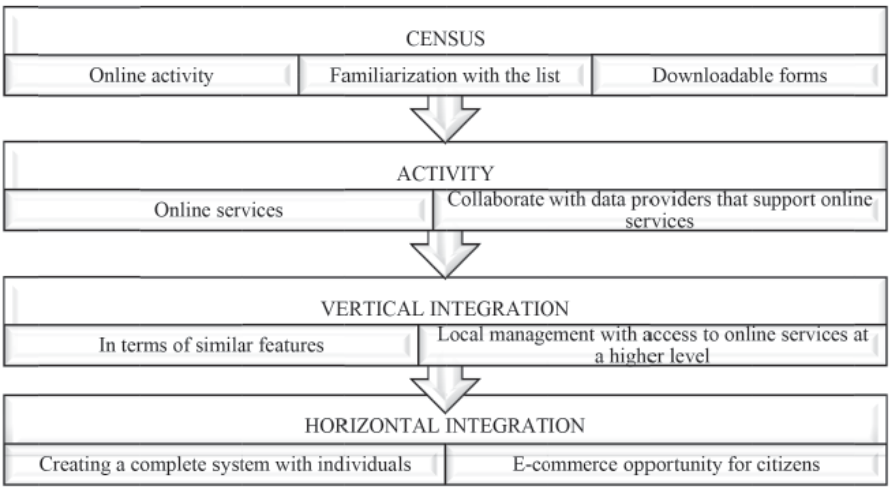


for hours in a queue for public service to be delivered in order to change their identity cards. The state's use of ICT at this stage eliminates misuse of power, bureaucracy and corruption, therefor it increases citizens' trust in the state.

Civilian stands in shopping centers in Brazil, mobile public computers carried by a plougher in pocket in India and ASAN services in Azerbaijan can be shown as an example of the World Bank's e-development activities.

Layne and Lee development model. Layne and Lee introduced e-state as a phenomenon of evolution and presented a four-stage development model: Census, Activity, Vertical Integration and Horizontal Integration. These four stages and key features of each of them are explained briefly as follows:

Individuals and legal entities want to use public services in the same way they access the services of the private sector through Internet during census



ПРАВО УКРАЇНИ • 2020 • № 4 • 225-244

stage. Therefore, all citizens will do search of state information via Internet rather than by phone call or other means that requires spending money.

They will feel depressed if they fail to use these services. Thus, the state will create a state information system that will be applicable to the pressures of workers who have the ability to use media technology and citizens' income groups. States prefer to minimize the risks by implementing small-scale projects at this stage, since they are not professional enough in this sphere. As civil servants spend most of their time answering basic questions about the service to citizens, existence of the web page is also useful from the point of view of government agencies' activity. Citizens have the opportunity to become familiar with policies and laws and know in advance which government agency they must apply for support through existence of the state's web pages. But, unfortunately citizens still use available services, such as waiting in queue in some cases.

Citizens prefer to carry out these activities over the Internet instead of going to governmental bodies to complete required *documentation during activity stage*. E-activity contributes to increased productivity both for customers and organizations. It also offers great opportunities to both sides such as time saving. The second stage is the beginning of the transition to e-government, mainly through fulfilled activities.

The services provided in *vertical integration stage* focus on the provision of public services elsewhere (online) rather than the automatization and personalization of deadlines. Electronization of state is not just about the provision of available public services over the Internet. World development also raises citizens' expectations from state and local self-governments. Main issue here is the organization of e-services in all government agencies in a vertical direction and ensuring continuity in this service.

There are wide opportunities for citizens to benefit from full potential of ICT in the *horizontal integration stage*. A citizen needs more than one public service in many cases. For example, a citizen in search of asylum needs government support in education, medical care and food. Government agencies need to work together to cope with this problem.

Thus, it is possible to determine whether a person really needs help only based on a certificate issued by relevant government agencies. Owners of information from different backgrounds in e-state communicate with each other, share information on citizens in the best possible way. This interaction is a perfect example of horizontal integration. For example, when a citizen moves to another city or region, his/her personal information will be electronically transferred to social services centers in the new place of residence and he/she will no longer have to re-apply for services in the new residence area.

UN approach on e-state. E-state is described in five steps in one of the UN reports on governance[9].

Appearance: Creating web pages, sites that provide information and services in various forms
Expanded participation (development): Dynamic development of e-filing of information through the creation of web pages on public and private sectors
Interactivity: Unlimited access to online services by both parties in public-private relations and provision of maximizing access to information
Interaction: Users can easily use the services provided for them by paying fee.
Information Network: State is providing e-services to both citizens and the private sector in the same way at this stage due to their wish.

As seen from the aforementioned models, the ultimate goal in any development model of e-state is to increase civic satisfaction. It is also considered a major advantage of the e-state.

Implementation of e-Governance for the branches of government and for main securing mechanisms of fundamental rights and freedoms

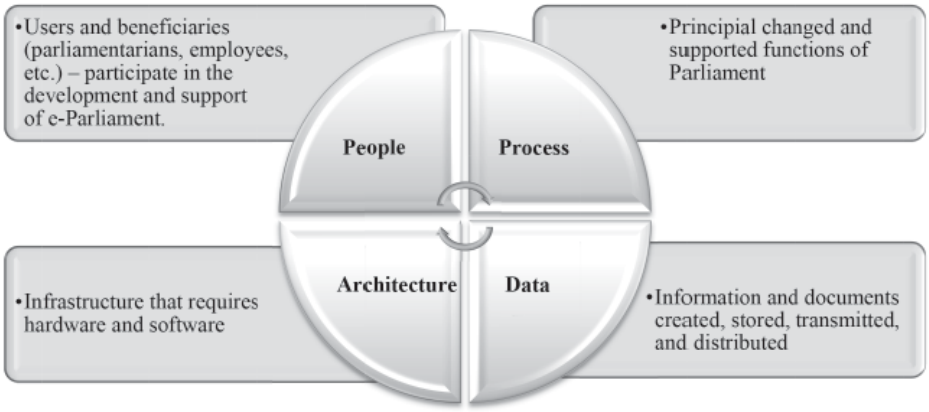
Digitization of the state involves digitization of its legislative, executive and judicial power in general. The digitization of the legislative body's activity led to emergence of the concept of *"electronic parliament"*. E-Parliament envisages the application of information and communication technologies in the activity of the Parliament, with the need to ensure citizens' participation in governance, taking into account the needs and offers of the parliament.

World e-Parliament Report 2018 provides a similar concept to e-Parliament. According to the report, taking into account various approaches, it can be considered that e-parliament provided by the application of ICT becomes the legislative body, which is more open, transparent and more efficient in the public and political life of the country[10]. It worth mentioning that in many international documents, "e" within the concept of "e-parliament" is problematic: it could be understood either as "effective" or "electronic"? – Actually, the activity of parliament within the framework of e-government is definitely electronic. But at the same time, electronicized parliament must also be effective to provide services to the citizen. In this regard, we believe that e-parliament should function as an electronic legislative body.

There are four main components of the e-parliament concept:

[9] U*nited Nations Global E-Government Survey* (2003) <https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/UN%20E-Government%20Survey%20series/UN%20E-Government%20Survey%202003.pdf> (accessed: 22.03.2020).

[10] *World e-Parliament Report 2018* <https://www.ipu.org/file/5920/download> (accessed: 22.03.2020).



Electronic elections should be mentioned as a clear example of e-parliament development. The state is able to increase its citizens' activity degree and participation in the political life of the state in this way. Electronic voting is a system that allows you to quickly count votes as a result of electronically registering of voters.

Advantages of the electronic electoral system: High voting activity; removal of errors during voting and counting; increasing confidence in the electoral system; Voting by only one candidate; Decrease in the number of invalid votes; Voting ability of voters with limited physical abilities; Ensuring confidentiality in the election process; Reduction of election irregularities; Determining results within a shorter timeframe; The use of less human labor than the existing election process; Save on financial expenses. Each of the listed advantages proves that citizens' rights are highly secured within e-governance.

Main purpose of forming the second branch of state power, "e-government" is the simplification and transparency of relations between state bodies and citizens with the use of ICT. Currently, electronization of e-government is implemented through "one window" principle in most countries. A similar rule exists in the Republic of Azerbaijan. Thus, website "e-gov.az" introduces a list of services provided to sub-groups created by different executive bodies, as well as detailed information about the service. The positive side is that the portal provides not only one direction, but also the terms of use in different directions. For example, it is possible to make search for services of executive authorities, by entering "Organizations" section. Section "Fields" was created to facilitate the search for a citizen. Services in the fields including social security, education and other services are available there[11].

The most valuable feature of e-state development in the Republic of Azerbaijan is the improvement of the conditions for the securing citizens'

[11] E-governrnent portal <https://www.e-gov.az> (accessed: 22.03.2020).

rights and freedoms. It covers guaranteeing the rights and freedoms in all areas. In case she/he consider to address the issue, this citizen is able now to obtain detailed information through various electronic portals about the state bodies and the forms of application. In the meanwhile all of this also indirectly secures the information rights.

For example, in accordance with the Decree No. 262 of the President of the Republic of Azerbaijan "Measures for the Establishment of an Electronic Registry of the State Service" dated September 11, 2014, the State Agency for the Public Service and Social Innovations under the President of the Republic of Azerbaijan was established. The Agency introduces a single news portal for public services, which includes a centralized search database for government services. A citizen who enters this search database will be able to find answers to any questions that may arise during the realization of his/her rights, and will also receive information on whether this form should be submitted electronically[12].

E-court created within the e-state is considered a new form of human rights protection, the development of which starts with the creation of a single Internet portal. This portal provides citizens with the opportunity to obtain detailed information on Supreme court, the first instance courts, the court of appeals, their jurisdiction, processed cases and decisions made, documents that need to be added to the application, admission dates, etc., the ways to acquire the samples of lawsuits and other court documents, as well as online application and responding. It is also possible for citizens to apply to the employees of justice system through the "e-services" mentioned above, along with online applications that citizens have already applied. E-court system opens up wide opportunities for citizens to receive court information promptly and to file lawsuits electronically in many countries. For example, every citizen in Azerbaijan can create an "Electronic Cabinet" by registering within "Electronic Court" information system. Submission of electronic lawsuits and other documents, certified by electronic signature through electronic cabinet, detailed study of court materials, notification of assigned process via SMS, e-mail and other methods, familiarization with the course of execution, acquisition of electronic decision of court by judge's e-signature and online payment of court fees are possible through e-cabinet.

Information security provision as important e-governance direction: E-security or information security?

Information security is aimed at preventing threats from legal aspect of infringement of accessibility, integrity and confidentiality of information. According to the sources, the first computer virus, which destroyed for the

[12] Portal of public services <http://dxr.az> (accessed: 22.03.2020).

first-time the thousands of ARPANET links, including universities, scientific-research institutes and military departments in early November 1988 was created and led to massive loss. The damage caused by this worm, known as "Morris worm" named in honor to its creator Robert Morris was estimated at about $ 100 million. The damage by Morris worm once again proved that information security is not a superficial problem and thus the issue of information security was brought up around the world. Due to this fact, November 30 was declared as "International Information Security Day". This day is already celebrated in almost all countries.

If to consider global nature of Internet, information security should be at the forefront of discussion on the international rather than national level. That is why mainly a number of programs, projects and mechanisms have been developed to ensure global information security on international level. International documents including "Creating a Global Cybersecurity Culture" approved by UN General Assembly Resolution No. 57/239 dated December 20, 2002, and appendix to it "Elements for the Creation of a Global Cyber Security Culture"[13], Declaration on the "Misuse of Information Technology for Criminal" approved by Resolution No. 55/63 dated 22 January 2001; "Budapest Convention on Cybercrime" dated 23 November, 2001 and others can be shown as an example.

Electronic security means unintentional and unauthorized access to computers, networks, programs, data and protecting them from change and destruction. Concept of electronic security can also be expressed as information technology security. As you can see, electronic security covers mainly technical aspects. Information security is of a wider nature. It is true that, the majority of activities aimed at ensuring information security are technical and organizational measures. However, information security is ensured not only by the implementation of this kind of activities, but also through other activities. At the same time, we must be aware that overall information threats are also a grave problem for the use of e-services by e-citizens. Therefore, information security must be provided on the level of e-governance, which includes e-security. So, e-security in e-government refers to purely technical and organizational problems. The question arises: But why should e-security be interpreted as a technical-organizational problem considering from legal perspective? – The reply can be the following – due to low level of security there is a breach of accessibility, completeness and confidentiality of information and it, in its turn, creates problems with the implementation of human rights and freedoms. It is no coincidence that e-security was mentioned as an important

[13] Creation of a global culture of cybersecurity: resolution, United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003 <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf> (accessed: 22.03.2020).

issue since the early stages of the e-government establishment till nowadays. For example, the United Nations classified the problems which states face during e-government building as following:

Problems with organizational management	7/24 hours lack of resources for updating information; lack of e-culture; insufficient organizational support; technological problems
Problems with governance	failure to use high-volume ICT; lack of confidence in ICT in management; dissenting attitude of professionals; misinformation management; a strong belief in the old system of governance in both government and the private sector
Problems in the formation of the political plan	lack of strategic planning and coordination; the absence of political leaders; problems with the transition of local government to the background

As it is seen, most of the above problems are due to feeble electronic security. Interactivity is fixed as the fourth phase also in UN e-Government Staging and it maximizes access to online services without hindrance and information accessibility by both parties with state-citizen relationships.

Computer Emergency Response Teams (CERT) plays a special role in ensuring international information security. This teams were first established at the University of Carnegie-Mellon in the United States in 1988 and later the similar programs were expanded worldwide. Nowadays, there are functions such as these teams in many countries and their main purpose is to provide direct information security. All of these teams are united in the International Union of National Centers for Struggle against Computer Incidents[14]. The Republic of Azerbaijan is also a full member of the Union and International Union of National Centers for Struggle against Computer Incidents and the Special Communication and Information Security was established in our country.

Electronic Security Center plays a great role in ensuring information security in our republic. The Center, which is a coordinating body under the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan was established on the basis of the Decree of the President of the Republic of Azerbaijan "On measures to improve activities in the field of information security" dated September 26, 2012. One of the advantages of the Center is that the preventive activities are not limited to one direction. The Electronic Security Center, which presents users the portal https://www.cert.az/, is also investigating cyber-attacks, as well as providing information

[14] The CERT Division <https://www.sei.cmu.edu/about/divisions/cert/index.cfm> (accessed: 22.03.2020).

on existing and potential electronic threats at national level, educating users in the field of cyber security; developing guidance on programs and technical tools that can be used against users to prevent electronic threats; giving them recommendations and providing methodical support to users. Thus, methodical recommendations are given in various directions in "Education" section of the Center's website and warning information is posted in section "Warning" for all subjects[15]. However, unfortunately, such useful information is not always available to the public. It would be appropriate to mention the "Statistics of 2017 on the use of Internet information resources of government agencies" of the Center for Computer Incidents of the State Agency for Private Communication and Information Security as a confirmation of the above-mentioned statement. According to the statistics, none of the websites created for information security protection exists among the most frequently used domains from the official internet resources of government agencies by 2017[16]. Therefore, it is expedient to share such information on websites or social networks that are commonly used as links or under "more attractive" news headlines. It should be noted that, it raises the issue of information security protection during the electronic document exchange since the electronic document circulation is dominating in our country in recent years. The Law of the Republic of Azerbaijan "On Electronic Signatures and Electronic Document" dated March 9, 2004 defines specific rules regarding electronic documents, which are of great importance in terms of the provision of information security. For example, the law defines imperative rules for the preservation and protection of electronic documents, as well as implies the certification of electronic signatures and prevents in essence, the "leakage" of information in electronic document circulation, destruction and misrepresentation of information for different purposes. However, it should also be noted that, it is possible to legally destroy or utilize information carriers due to the fact that the information loses its relevance after a certain period of time. It is no coincidence that, inclusion of information utilization attitudes was proposed while defining the subject of information rights in previous chapters. This kind of relationship is even more significant from aspect of information security. In most cases, improper disposal of electronic waste can lead to information leaks. Therefore, activities in this area should be further strengthened. The issue is that, there are many impediments regarding the destruction of electronic data, since the regulations concerning the destruction of information in the current legislation mainly relate to the information provided on paper. In case official registration of "Personal Data Information

[15] Official website of the Cyber Security Center <https://www.cert.az> (accessed: 22.03.2020).
[16] Official website of the Computer Emergency Response Center <https://cert.gov.az> (accessed: 22.03.2020).

System" approved by the Order of the Cabinet of Ministers of the Republic of Azerbaijan dated December 17, 2010 is abolished, the methods of destroying electronic personal information contained in the information system is implied in the "Rule for Data Destruction in the Information System": destruction of electronic information carrier by mechanical means; making it impossible to restore; the creation of a situation where electronic media cannot be restored; Formatting electronic information carriers in the way impossible to restore; deletion of data in electronic information carrier through special software which is not possible to restore. Several types of methods can be used during liquidation of information.

The issues dealing with electronic documents generally are not covered in "Instructions for Conducting Documentation in Public Authorities, Entities, Organizations and Enterprises " dated January 19, 2005 approved by the President of the Republic of Azerbaijan, but only paper-based separation acts are mentioned. It is true, that provisions on the abolition of documents are generally provided in statutory legal acts concerning limited information (e.g. state secrets legislation). However, it is more rational to incorporate relevant provisions into Article. 30 of the Law of the Republic of Azerbaijan "On Electronic Signatures and Electronic Document" (electronic document protection) due to different methods of electronic documents' abolition.

One of the measures taken in recent years to ensure information security is the creation of a "Safe Internet" service in accordance with the instructions of the Ministry of Transport, Communications and High Technologies. Users of all age category can protect themselves from harmful content via this filtering service. Via provided wide range of services, parents can control resources that include games and movies promoting crime, violence, racism, discrimination and extremism that can physically inflict harm to minors. It is possible to restrict access to content that is considered to be unsafe from the submitted list by including them to "black list" after joining the service. You can also deactivate the filter at any time and activate resource in the "black list". The list of web pages restricted for this type of service should be updated regularly. Because there is an active development in the direction of committing various illegal activities by "abusive" people using ICTs. In our opinion, there might appear problems with operation mechanism of secure Internet services. First, web pages are growing in Internet. Quick detection of those web pages can be a little bit tricky. Secondly, viruses and other harmful software can be transmitted not only through these web pages, but also via simple online chatting. The services, which restrict access of minors to negative websites are simply aimed at moving them away from the "dangerous" areas. However, given that the "forbidden behavior becomes more attractive", as well as psychological characteristics of

minors and teenagers, it is impossible to exclude them from access to banned webpages from other computers connected to the Internet. We believe that it is more expedient to strengthen the work of authorities dealing with computer incidents in this regard.

Biometric information technologies have great potential in ensuring information security both at national and international levels. According to the experience, one of main reasons of crimes and unethical behavior in information and communication systems, especially in Internet environment, is the lack of user identification mechanisms when it is needed. Following the terrorist attacks committed in the United States on September 11, 2001, the UN Security Council adopted a resolution on the identification of people based on biometric data and the use of new generation documents. Production and application of electronic passports implied biometric technologies and their use is organized in border control systems over biometric identification systems, in the conduct of operational search activities and protection of public order in accordance with the new standards adopted by the International Civil Aviation Organization, International Maritime Organization, International Labor Organization, International Organization for Standardization and other agencies in some countries and recommendations of the International Organization for Migration. Interdepartmental and interstate information systems were established, certain experience was collected and specialization and competition between producers of relevant software and hardware tools were strengthened. The implementation of specific projects, the production of appropriate forms, and software and hardware tool were launched in this area. The application of biometric technologies will enhance the protection of passport and visa and other identity documents, the control over person's access to documentation via another individual data, the improvement of critical infrastructure and the protection regime of other facilities, accuracy of identification and comprehensive personalization of individual data of a person in various information resources.

The application of online biometric services will provide wide opportunities to ensure a high level of public safety in the near future.

Elimination of electronic (digital) inequality contributes to the protection of information security

One of the objects of current research is "digital divide" in the period of global information society establishment and in the period when information's becoming a leading force of society. Various sources use concepts like "information inequality", "digital inequality", "digital divide", "digital decomposition", "electronic divide" and so on. These concepts have essentially

the same meaning. The terms "information divide" and "information inequality" are more commonly used in early days, while the terms "digital divide" or "digital inequality" were applied lately. What is digital inequality and what factors stipulate it? – Referring to Geneva Declaration of Principles, this concept can be interpreted in a broad (global) and narrow (local) sense. Article. 10 of the Declaration states that, participatory states fully recognize benefits of the information revolution are not shared equally among developed and developing countries, as well as in the field of information technology and within the states themselves. Such inequal distribution stipulates digital inequality in information society. Thus, famous saying "the person who has information, possesses the world" is still valid. Because the search, acquisition, dissemination and transmission of information in states with high ICT development rates is easily and fastly implemented so that problem is not occurred upon access to relevant information in such a case. A similar situation exists among members of society, as well. People with information culture are more likely to take advantage of ICT opportunities more widely than others and thus actively participate in society in this way. However, it should be taken into consideration that, main task in building a global information society is to protect and guarantee human rights and freedoms. Such a task can be considered fulfilled if everyone is closely involved in the creation, acquisition, production, transfer and dissemination of information and knowledge. On the other hand, main development direction of the information society opens to all ensuring access to information, ideas and knowledge and possession of everyone to contribute in that area. Both sides of the problem reaffirm digital inequality is a major obstacle to the development of a global information society and urgency of the issues to be resolved.

Thus, digital inequality is difference in access to information, as well as using ICT irrespective of different criteria (factors) among different layers of society and the world countries. Internet, main means of access to information, is the most important attribute and the driving force of global information society. In this regard, limited access to the Internet is an important criterion for digital inequality. Highest growth of digital divide can be observed in the latest Statistical Data for March 25, 2018, which reflects the number and proportion of global Internet users by region[17]. Europe (16,8 %) and North America (8,2 %) are characterized by high development rates (Europe – 85,2 % and North America – 95 %), although they cover a very small part of the world population. Asian and African countries, on the contrary, are inferior to the number of Internet users. It reaffirms existence of digital inequality around the world.

[17] Internet World Stats <http://www.internetworldstats.com/stats.htm> (accessed: 22.03.2020).

Summarizing the abovementioned, we can conclude that existing digital inequality in the world stipulates the formation of e-threats in e-governance. It also requires the development of new trends in line with existing demands. Thus, today different approaches to "information security" were formed, since purpose of "information attacks" changed (acquisition of different confidential information) . Therefore, currently protection of transmitted information must be ensured in addition to the security of computer networks and systems. All of these contribute to the creation of new security tendencies[18]. It is important to note that, each development tendency forms a different development tendency within itself, that ultimately creates appropriate security tendency. Setting up of portable and personal mobile devices increased application and usage trends as infrastructure development trend. Each mobile device also creates new opportunities for cyberattacks. That is why new programs and other security measures that can prevent cyber-attacks on mobile devices are planned and implemented to hinder that.

Conclusion. The state's digitization includes the digitization of its legislative (e-parliament), executive (e-government) and judicial (e-judicial) authorities. It is noteworthy, in the notion "e-parliament" the letter "e" and its definition: Does this sign mean "effective" or "electronic"? – In our opinion, the activity of the parliament within the framework of electronic state is definitely electronization. Therefore, e-parliament should be used in the meaning of an electronic legislative body.

The most evolving aspect of e-state is displayed in the digitization of executive body. Electronic services provided to the citizen through various websites open wide opportunities for free and easy realization of his/her rights and freedoms. However, this system has some problems along with advantages. For example, having a mobile number on the person's name and documents proving his/her identification are key terms to register on e-Government Portal. Three main documents at least are required for registration. In our opinion, it is more expedient to reduce the number of these requirements. Because most citizens do not have a valid passport, SSPF (state social protection fund) card, or driving license. Therefore, just registering mobile number and ID card may be enough to proceed with registration in the system. E-service application provided in this way will be easier and more affordable.

Any gaps or deficiencies in electronic information systems can eventually lead to the destruction of all data. Therefore, e-state information security should be at the forefront on both international and national levels as one of the main areas of government information policy. Since information security is wider

[18] Under the term "security tendency", the emergence of new changes as a result of development of computer networks infrastructure, application and usage of ICT should be understood.

concept than electronic security, protection of the latter in e-governance serves ensuring of the completeness, accessibility and confidentiality of information. Therefore, an ordinary citizen, benefitting of e-state facilities should be made sure that, his/her rights and freedoms are protected and that he/she will not be exposed to criminal conspiracy. Struggle against cybercrime should be strengthened for this reason and the issues over spams and cyber security should be studied on international and local level. Internal (inside the system) and external (external interference with the system) factors that create electronic problems existent in the operation of e-state should be prevented, and integrity, accessibility and confidentiality of information should be observed.

Referring to the mentioned, we can conclude that the elimination of the problems that arise during the formation of e-state will guarantee the protection of fundamental human rights and freedoms within bilateral development and will provide that every citizen will be an active member of the society, which is, in its turn, is a prerequisite of the information society.

REFERENCES

Bibliography

Edited books

1. Al-Hashmi Asma and Darem Abdul Basit, 'Understanding Phases of E-government Project' in Sahu G P (ed), *Emerging Technologies in E-Government* (Gift Publishing 2009) (in English).
2. Alshehri and Drew S, 'Implementation of e-Government: Advantages and Challenges' in *International association for scientific knowledge (IASK) E-ALT Conference proceedings* (2010) (in English).

Journal articles

3. Demirel D, 'E-Devlet ve Dünya Örnekleri' (2006) 61 Sayıştay Dergisi 94 (in Turkish).
4. Yıldız M, 'Uluslararası Kuruluşların Türkiye nin E-devlet Siyasalarına Etkisi' [2007] 40 Amme İdaresi Dergisi 39 (in Turkish).

Newspaper articles

5. Heeks R, 'Understanding e-Governance for Development' (2001) 11 iGovernment Working Paper <https://ssrn.com/abstract=3540058> (accessed: 22.03.2020) (in English).
6. Meinardus R, 'The Political Impact of the Internet' Business World Internet Edition (March 26, 2003, and March 27, 2003) (in English).

Websites

7. 'E-Government Handbook for Developing Countries' *(A Project of InfoDev and The Center for Democracy & Technology)* <http://www.infodev.org/infodev-files/resource/InfodevDocuments_16.pdf> (accessed: 22.03.2020) (in English).
8. Creation of a global culture of cybersecurity: resolution, United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003 <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf> (accessed: 22.03.2020) (in English).

9. 'United Nations Global E-Government Survey' (2003) <https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/UN%20E-Government%20Survey%20series/UN%20E-Government%20Survey%202003.pdf> (accessed: 22.03.2020) (in English).
10. United States. General Accounting Office (*Electronic Government: Federal Initiatives Are Evolving Rapidly but They Face Significant Challenges*, 22.05.2000) <https://digital.library.unt.edu/ark:/67531/metadc290097> (accessed: 22.03.2020) (in English).
11. 'World e-Parliament Report 2018' <https://www.ipu.org/file/5920/download> (accessed: 22.03.2020) (in English).

Рзаєва Гюльназ Айдин
Ібрагімова Айтакін Назім

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕЛЕКТРОННОМУ УРЯДУВАННІ ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ

Анотація. Мета електронного урядування як концепції полягає у покращенні ефективності діяльності державних інститутів та підвищенні рівня життя громадян. Формування електронної держави визначає темпи розвитку прав і свобод людини відповідно до вимог сьогодення, серед яких особливе значення мають інформаційні права. Однак у ситуації, коли повнота, доступність і конфіденційність інформації не забезпечується повною мірою, виникають перешкоди для реалізації інформаційних прав. Тому організація інформаційної безпеки є одним із засобів гарантування інформаційних прав. У зв'язку з цим, інформаційну безпеку слід аналізувати не тільки з технічної точки зору, але й в аспекті права в галузі прав людини. Ці основні моменти обґрунтовують актуальність теми статті.

Мета статті – проаналізувати такі поняття, як "електронний уряд", "електронний парламент" і "електронний суд», показати пріоритети електронної держави з точки зору забезпечення прав і свобод людини, визначити правові, теоретичні та технічні підходи до інформаційної безпеки в різних моделях електронного урядування, виявити різницю між електронною безпекою та інформаційною безпекою, дослідити значення електронного урядування в аспекті прав людини і представити пропозиції щодо захисту інформаційних прав, порушених у кіберпросторі.

Автори доходять висновку, що повний доступ до інформації в новому суспільстві є гарантією інформаційних та інших прав і свобод. Таким чином, через відсутність інформаційної безпеки або низький рівень інформаційної безпеки електронний уряд не може приносити користь своїм громадянам. Одним з таких бар'єрів вважається електронний розрив або цифровий розрив. З огляду на глобальний характер кіберпростору та інформаційного суспільства, ці проблеми необхідно вирішувати не тільки на національному рівні, а й на міжнародному. Перш за все, безпеку не слід сприймати з технічної точки зору. Це перешкоджає вирішенню проблем. Слід також проаналізувати інформаційну безпеку як правовий інститут і уточнити різницю між термінами "інформаційний захист" і "інформаційна оборона". Необхідно розкрити юридичний аспект цього питання.

Таким чином, автори з оптимізмом доходять висновку, що усунення проблем, які виникають при формуванні електронного урядування, сприятиме кращій реалізації основних прав і свобод людини та допоможе кожному громадянинові стати активним членом цифрового суспільства.

Ключові слова: інформаційні права; інформаційна безпека; електронний парламент; електронний уряд; електронний суд; тенденції безпеки; електронна безпека.