REPUBLIC OF AZERBAIJAN

On the rights of the manuscript

ABSTRACT

of the dissertation for the degree of Doctor of Law

INTERNATIONAL AND DOMESTIC LEGAL DEFENSE MECHANISMS OF INFORMATION SECURITY

Specialization: 5614.01 – "Administrative law; financial law; Information law"

Field of science: Law

Applicant: **Aytakin Nazim Ibrahimova**

Baku – 2024

The dissertation was performed at the Department of Human rights and information law UNESCO of the Faculty of Law of Baku State University.

Supervisor: Doctor of Law, Professor
Amir Aliyev Ibrahim
Doctor of Law, Professor
Oleq Volodimurovich Zaychuk

Official opponents: Doctor of law, associate professor
Anatolii Trofimovich Komziuk
Doctor of law, associate professor
Yuriy Pavlovich Burilo
Doctor of law, associate professor
Petro Vasilovich Dixtievskiy
Doctor of law, associate professor
Khistophor Petrovich Yarmaki

The High Attestation Comission under the President of the Republic of Azerbaijan dated October 27, 2023 on the basis of the order 3-50/3-1-1-235/2023 of the BED 2.44 One-time Dissertation Council operating at Baku State University

Chairman of the Dissertation council: Doctor of law, associate professor
Turgay Imankhulu Huseynov

Scientific secretary of the Dissertation council: Doctor of philosophy in law, associate professor
Alizade Gurbanali Mammadov

Chairman of the scientific seminar: Doctor of law, associate professor
Ramil Mahir Aslanov

BAKI DÖVLƏT UNİVERSİTETİ
Ministry of Science and Education of the Republic of Azerbaijan
BDU ELMİ KATİB
SECRETARY
İmzanı təsdiq edirəm:
26 " 01 (B.A.A.) 2024

GENERAL CHARACTERISTICS OF DISSERTATION

Relevance of the research topic and degree of scientific elaboration of the theme. The concept of information is quite broad, it is used in different meanings and the spheres of activity are also diverse. In addition, there is almost no field of activity where the concept of information is not used. This makes it necessary to look at the problem comprehensively and in the close interaction of different fields of science. One of such directions is the legal regulation of information, including various areas related to information, including issues related to information security. When talking about information, including information security, special attention should be paid to the concept of security. The term "security" can be defined as "national security", "international security", "human security", "global security", etc., depending on the object of the threat[1]. In general, the concept of "security" is also considered a special term. In the generally accepted sense, security in all cases requires the formation of defense mechanisms in the relevant spheres. Thus, it is impossible to ensure security without defense systems. Information security should be understood as the protection of the information environment taking into account the interests of society as a whole, the identification of threats to this environment and their prevention accordingly. It is noted in the legal literature that information security is becoming more and more important day by day and is a very relevant issue that is the main topic of discussion for various categories of subjects all over the world[2]. In another study justifying the relevance of the legal regulation of information security, it is noted that the development and wide use of electronic communication tools, as well as the use and widespread use of the Internet in almost all areas, showing that there is a greater need for information security measures than ever, as well as ensuring the protection of information in the activities of natural persons, as well

[1] Əliyev Ə.İ. İnsan hüquqları. Dərslik. Bakı, 2019, s.180

[2]Soomro, T. R. Information security management: A case study of an information security culture./ Soomro, T. R., Shah, M. H., & Ahmed, J- Information Management & Computer Security 24(1),2016, s.86-102

as ensuring protection from illegal capture of information, use for fraud and fraud purposes, and other security violations, is one of the most urgent topics of discussion today[3]. According to one of its current approaches, information security is viewed as an ever-evolving field that requires attention and updates due to the rapid development of technology and the ever-increasing sophistication of cyber-attacks[4], in another, it is treated as a key challenge for the digital society[5]. The mentioned once again confirms the relevance of information security and its legal regulation.

The main indicator of state security in the information society depends on its information security. Information security is developing in a constantly increasing direction compared to other state security and is becoming a dominant security object. It can be noted that the formation of information security in the states has not only become an important tool for meeting the information needs of the society, but at the same time, it has also created conditions for its implementation in a more secure manner.

Previously, information security was protected individually either by people themselves or by the state in paper carriers, but now the state and society are trying to overcome these problems together, especially the protection of information circulating in electronic carriers is organized. At this time, in solving the issue of security, either in the international-legal framework, or in the national-legal framework, the states take upon themselves the respective responsibilities. Information security is reflected in the national legislative acts of each of the modern states. The first reason why information security is reflected at the constitutional level is related to the importance given to it by the states.

---

[3] Mishra, D., Mishra.S.K. Information security management in organizations: A review of literature./ Journal of Global Information Management 24(4), 2016, s. 36-37

[4] Kumar, R. Emerging trends and challenges in information security management./ Kumar, R., & Shukla, A. K. - Journal of Advances in Management Research 15(1), 2018, s.5-17

[5] Siau, K. Research on information security in organizations: A review of the literature./ Siau, K., Nah, F. F., & Tian, Y. - Information & Management 53(6), 2016, s.804-819

After gaining independence, the Republic of Azerbaijan (AR) began to implement many radical reforms in the field of information, as in all fields: information security became the basis of our state's activities, and the legislation in this field was improved. The additions and changes made to Article 32 of the Constitution of AR in 2009 once again proved that one of the main factors that form the basis of the state is the provision of information security. Of course, not all aspects of information security can be found in the constitution, they are further developed at the level of national legislation. However, information security, which is regulated by separate normative legal acts, should be based on constitutional principles as a whole.

The above-mentioned once again confirms the relevance of the dissertation work. In addition, a number of domestic regulatory and legal acts have been adopted in this direction by AR, which is a party to several international agreements. For example, laws "On information, informatization and protection of information", "On personal data", etc. were adopted, and the reviewed and emerging information environment, including information security issues, were also regulated in detail. In addition, world practice shows that the process of forming a comprehensive legal system for information security cannot be considered complete, as the process of reconciliation of international and national legal norms is still part of a rather comprehensive complex stage.

Currently, in the process of information formation in the Republic of Azerbaijan, it is one of the duties of the state to ensure the fundamentals of human rights and freedoms. The requirements of the 12th version of the AR Constitution are specifically mentioned on this basis. The 1st part of that article, as a whole, acts as the supreme protection of the state to ensure human rights and freedoms, in addition to the 2nd part, it mentions the special role of these powerful laws. It should be noted that it was strengthened and further developed by Articles 71, 148-2 and 151 of the Constitution of the Republic of Azerbaijan.

Although studies have been conducted on separate aspects of the international legal regulation of information security, this issue

has not been developed as a separate research topic. The dissertation presented to the defense is the first scientific work that studies the aspects of international and domestic legal protection mechanisms of information security. Until then, this issue was approached from different aspects and information security was mostly studied within the framework of information law. In this study, the problem was approached from a completely different direction, from the context of human rights and international security, including modern trends and international law. In this regard, the current research work is the first research work dedicated to the study of general and specific development trends of information security. For the first time within the framework of the research work, the international legal norms that determine the current trends in the legal regulation of public relations related to information security and the legislative experience of different states, including the Republic of Azerbaijan, were comparatively analyzed; Initial directions for the formation of the institution and basic elements of information security provision in AR have been determined; theoretical and practical legal contents of the purpose and main features of information security are clarified; all issues related to information security at the doctrinal level were widely reviewed; a number of important gaps and collisions were discovered in this area; a number of improvement suggestions and recommendations have been developed in that sphere.

The dissertation analyzed the scientific works of local and foreign authors who conducted research on the topic. Meanwhile, N.H.Kuran (E-government Model for Turkey)[6], B.Yıldız (Implementation of Information Security Management Standards in Public Institutions in the Scope of Information Security and E-Government)[7], J.E.Fountain (Building the Virtual State: Information Technology and Institutional Change)[8], R.Heeks (Implementing and

[6] Kuran N.H. Türkiye İçin E-devlet Modeli. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, - 2005

[7] Yıldız.B. Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması/Yüksek Lisans Tezi/- 2007

[8] Fountain, J. E. Building the Virtual State: Information Technology and Institutional Change./ Brookings Institution Press/-2001

Managing e-Government: An International Text)[9], T.Olufohunsi (Data Encryption)[10], S.Raghavan (Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists)[11] and we can mention others.

National and international regulation of information security has not been the subject of research in national legal literature. So, although a number of special studies were conducted in this field, with those studies, an attempt was made to explain the national legislation from the context of related sciences and legal fields. Only at the level of textbooks and educational materials - R.M.Aslanov (Development directions of democracy in the information society: digital democracy[12], Fundamentals and actual problems of information law[13]), A.I.Aliyev, G.A.Rzayeva, A.N.Ibrahimova, B.A.Maharramov, Sh.S.Mammadrzali (Information law)[14], M.N.Alizadeh, H.M.Bayramov, A.S.Mammadov (Information security)[15], R.F.Azizov (Comparative legal analysis of regulation in the Internet network)[16] and scientific articles (G.A.Rzayeva, Z.Q.Jabrayilova, R.M.Aliguliyev, B.S.Agayev, etc.) addressed individual issues of information security. Only one research work was conducted at the dissertation level related to informational legal relations in Azerbaijani legal doctrine. Thus, R.M.Aslanov's "Theoretical and constitutional basis of legal guarantee of

[9] Heeks, R. Implementing and Managing e-Government: An International Text./ Sage Publications/- 2006

[10] Olufohunsi, T. Data Encryption./ University of Salford/- 2019

[11] Raghavan, S. Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists/ Cambridge University Press/- 2018

[12] Aslanov R.M. İnformasiya cəmiyyətində demokratiyanın inkişaf istiqamətləri: rəqəmsal demokratiya/ Monoqrafiya/ -Bakı, - 2022

[13] Aslanov R.M. İnformasiya hüququnun əsasları və aktual problemləri/ Dərslik/- Bakı, - 2019

[14] Əliyev Ə.İ., İnformasiya hüququ. Dərslik. / Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S/. -Bakı: Nurlar nəşriyyatı,- 2019

[15] Əlizadə M.N. İnformasiya təhlükəsizliyi. Dərslik. / Bayramov H.M., Məmmədov Ə.S/. -Bakı, İqtisad Universiteti nəşriyyatı, - 2016

[16] Əzizov R.F. "İnternet" şəbəkəsində tənzimləmənin müqayisəli hüquqi təhlili./ - Bakı: Elm. - 2017

information security in the construction of information society in the Republic of Azerbaijan and the Russian Federation"[17] dissertation is dedicated to only one aspect of information legal relations. In addition, in a recently defended dissertation in Azerbaijani legal literature, only theoretical and practical aspects of information law violations and information-legal responsibility were analyzed[18].

Later, separate aspects of the regulation of informational legal relations were researched by foreign authors at the level of coursebooks, textbooks and scientific articles: I.L.Bachilo, V.A.Kopylov, V.N.Lopatin, V.A.Pojilykh, M.M.Rassolov, A.A.Fatyanov, M.A.Fedotov, A.Pazyuk, M.Sokolova, V.D.Elkin, V. M.Baranova, M.Bashlykova, E.Brodsky, M.Y.Yemelyannikova, K.A.Zanina, N.G.Belgorodtseva, I.A.Velder, A.V.Dvoretsky, A.V.Kucherenko, N.I.Petrykin, O.B.Prosvetova, Y.S.Telina, A.S.Fedosin, R.Walters, S.D.Warren, L.D.Brandeis, M.Land, A.F.Westin, D.A.Solove, J.Whitman, D.M.Vicente, L.Feiiler, E.Brauer, M.Zalnirut, P.Fischer, J.Kuner, C.Hoffman, A.C.Evans, M.Owen, S.Gutwirth, F.Bignami, M.Medina, M.Bakhoum, D.Kamarinou, J.Drexl, J.Dumas, J.Hölzel, B.Valtisson, J.F.Albrecht, J.Stoddart, A.L.Gardner, P.Van den Bulk, E.A.Salami, F.Boexm, D.Gray, N.Terry, M.J.Blanke, L.Sotto, S.Hodges, M.U.Brennan, C.L.Reyers, and others. The studies mentioned in the dissertation were widely used as a scientific-theoretical base.

Object and subject of research. The object of the research is the information security of the state and its comprehensive study. The subject of the research is the information security of the state, the legal basis of information security, the issues related to the determination and guarantees of information rights, and the

[17] Aslanov R.M. Azərbaycan Respublikası və Rusiya Federasiyasında informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının nəzəri və konstitusiya əsasları:/ Hüquq üzrə elmlər doktoru elmi dərəcəsi almaq üçün dissertasiya işi/-Bakı, - 2016

[18] Əlizadə H.O. İnformasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət: nəzəri və təcrübi aspektlər. Hüquq üzrə fəlsəfə doktoru elmi dərəcəsi almaq üçün təqdim edilmiş dissertasiyanın avtoreferatı. Bakı, - 2023

international documents, legislative acts, adopted state programs and court practices used in the study of these issues.

Goals and objectives of the study. The purpose of the research is to conduct a comprehensive analysis of the information security of the state, to analyze the international and domestic legal protection mechanisms of information security, to investigate the unique aspects and essence of information security, to conduct an analysis of the information security of the state as a whole in the example of AR, and to fully justify the place and importance of information security in ensuring the security of the state. consists of.

In order to achieve the stated goal, the following tasks were defined in the study:

- To analyze the essence, main characteristics and constituent elements of information security, to determine its place in the international and national security system;
- To review the main directions and aspects of information security, including information security standards;
- To review the main goals of the state's information security policy, to determine the place of information security in the security system of AR;
- To determine the importance of information security in the provision of rights in the field of information;
- To review the main features of the electronic state as a system of ensuring information rights;
- To investigate the features of creating a normative-legal base for the electronic state in AR;
- To consider information rights as the main priority of the state in the context of human rights;
- To analyze the role of personal and biometric data in ensuring information security;
- Broadly analyze social networks and information security issues;
- Mutual consideration of information security and legal liability issues;
- Investigate the role of information security culture in ensuring information security;

- To determine the interaction of international and domestic legal protection mechanisms of information security in a single unity and to determine the development trends of each of them separately;

- To determine the international obligations of AR on ensuring information security, to determine international and national mechanisms in this field;

- To make important suggestions on the elimination of difficulties arising in the field of full fulfillment of AR's obligations in the field of information security;

- To analyze the issues of implementation of international legal norms in the field of information to the national legislation of AR;

- Cooperation in the field of information security in international universal and regional organizations, to determine the tasks set in the direction of further strengthening of this cooperation in the future;

- Taking into account the experience of developed countries in the field of information security, to come up with proposals to implement the codification of the national legislation on ensuring information security in AR.

Research methods. Both general (formal logical, systematic-structural analysis, historical approach, generalization of scientific and practical materials) and special scientific methods (comparative jurisprudence, logic, statistical analysis, monitoring, etc.) were used in the process of writing the dissertation. Thus, a comparative analysis of the legislation of a number of states, which includes information security, was carried out, proposals were put forward regarding the application of exemplary norms reflected in the legislation of developed states to national legislation and practice. In addition, in different periods, the opinions and conclusions of the lawyers of individual states regarding the information security of the state were investigated in detail, various court cases were studied, and social and judicial statistical research methods were used in summarizing the experimental materials of the courts.

The main provisions for the defense. The following new scientific propositions expressing the scientific novelty of the research are submitted for defense:

1. During the analysis of issues related to information security, its main features in interaction in the international and national security system should be considered, and finally, the importance of information security for the international and domestic normative-legal system should be justified. At this time, the main elements of the concept of information in ensuring information security, including important aspects of information security and important factors affecting security, such as confidentiality, integrity, availability, accountability, etc. it should be noted in the interaction, then the role of other factors that will appear in the future should be justified.

2. One of the important factors in detecting and preventing information security is legal creation and effective application of legal norms. For the creation of international law, taking the practice of developed countries as a basis should be an important direction. In addition, legal liability as a preventive measure in ensuring information security, as well as the main features of information protection as a means of ensuring information security, should be noted and a number of scientific theoretical and practical recommendations should be based on this.

3. A number of important directions should be determined by fully justifying the role of information security culture in ensuring information security. Such an opinion should be noted that important positive results of information security can be achieved only in a unified system of domestic and international legal protection mechanisms.

4. International legal protection mechanisms of information security should be considered from the point of view of international normative-legal bases and international organizational mechanisms and as a system of international-legal regulation of information relations. In addition, the concept of cooperation of states in ensuring information security should be justified, and it should be noted that cooperation of states in this field is not only their right, but also their duty. Information security is directly related to human rights, therefore, taking into account the human rights factor and its being one of the main goals of states and the international community,

information security should be treated as a global problem and serious international measures should be implemented in this direction.

5. Information security requires an approach to it from two directions: international information security, which is a part of international security and must be regulated by international law; national information security, which should be regulated by national law as part of national security and by accepting the primacy of international law.

6. The rapid development of information legal relations in the modern era has caused the issue of ensuring security in the information society to be at the center of the main scientific discussions. At the same time, the rapid development of information technologies is the basis for the emergence of new threats. Therefore, continuous monitoring of the development trend of information technologies by the state should be ensured. In addition, encouraging measures should be taken to conduct scientific research, analysis and research in the direction of risk determination, support should be given to the development of theories that meet the requirements of the modern era.

7. Wide application of information technologies in all spheres and widespread use of digital systems necessitates a new approach to international security. Because already different levels of terrorist acts are committed in the digital environment or by using information technology tools. This brings to the agenda the formation and determination of legal mechanisms of information security in the process of ensuring security at the international and national level. At present, the international and national legal framework defining behaviours belonging to the scope of the crime of terrorism should be regulated in relation to cyber-terrorist acts. Appropriate changes should be made in the international agreements that form the basis of international legal regulation in this field, and the scope and responsibility for the commission of terrorist-type socially dangerous acts committed in the information society should be determined.

8. Determining the rights and duties of the participants in the legal relations regarding information security and the proper performance of their obligations by the participants is the basis of information security. In this direction, the scope of subjects, the rights and duties of those subjects should be determined in international level acts and national legislation in matters related to ensuring information security in information legal relations. Basically, the exact definition of the scope of the subjects' obligations should be considered appropriate for minimizing information security risks.

9. It is well known that the provision of information security is not only related to the activity (inactivity) of subjects responsible for the security of information resources or systems. Thus, sudden negligence and carelessness of the user of the information resource or system makes it impossible to ensure the protection of information in relation to that user. In such a case, measures should be taken to increase public literacy. It would be appropriate to define such measures as one of the main tasks of the state. Therefore, consistent measures should be taken in the direction of raising awareness and literacy about information security, educational and promotional materials on strengthening information security measures should be prepared, and accessibility of those materials should be ensured. In this direction, the inclusion of measures to increase awareness and literacy in programs at different educational levels should be considered as one of the necessary measures.

10. One of the characteristics of the information society is that there are no borders. Thus, it can be noted that cyberspace is borderless, and determining the jurisdiction of a specific state is one of the most difficult issues. Taking into account the importance of information security and its role in international security, it should be noted that international cooperation in this field should be effectively established and implemented in a newer format, as well as operational joint action. Since information risks have the potential to cause great damage in a very sudden moment, it can be considered appropriate to establish an international cooperation platform in a new format that ensures the cooperation of states and the

establishment of activities for common interests. Thus, the activities of the organizations (institutions) responsible for ensuring the information security of the states should be ensured through a single digital platform, aimed at ensuring information security, as well as against risks or threats related to information security.

11. Information security is closely related to systems and resources applied in various spheres of society. Studies show that no matter how many standards or norms are defined to ensure information security, information resources or systems are not designed in accordance with those norms or are not followed in the application process. The implementation of relevant expertise activities from the aspect of information security should be defined in national normative legal acts. Including, putting the information resource or system into use should be determined according to the results of that expertise. In this direction, an appropriate institution should be established, which is engaged in the expertise of information resources or systems related to information security, and normative documents on the requirements or standards for those resources and systems should be adopted.

12. Threats to information security are often driven by commercial interests. Thus, the information obtained by means of illegal intervention in information resources is misused and thereby results in material and, in some cases, moral damage to a certain group of subjects. Therefore, it is necessary to manage information security risks and use systems by commercial organizations that operate corporately and have such resources. In such a case, information security management systems that meet international standards should be used.

13. The development of information technologies and the application of innovations manifest themselves at different levels in different countries. In the countries where information technology is developing rapidly, the process of regulating issues related to information security has also followed the same development path. Therefore, developing countries in this field should be interested in learning positive world experience. Carrying out and studying such exchange of experience will make a positive contribution in terms of

ensuring information security, studying threats and risks in advance, and taking measures against them. Thus, a serious international cooperation platform should be established that allows developing countries to study the experiences of developed countries, as well as developed countries to exchange information among themselves.

14. One of the main role holders in ensuring information security is the personnel engaged in activities in this field. Having adequate backup resources and knowledgeable people can help minimize errors in information security detection. Since the development of the mentioned products is a long way, it is necessary to monitor the deepening of the obtained experiences and practices. For this purpose, establishment of specialization programs and courses at special higher education levels, increase of experience opportunities for working people in facilities equipped with energy sources in the field of information security, etc. rules must be followed.

15. Gaps allowed in determining the legal regime for the use of information that is restricted or classified as sensitive information can result in the creation of major threats to information security. The precise regulation of the legal and protection regime of that category of information should be implemented. In addition, the relevant subjects using such information should organize their activities according to certain requirements. The scope of such requirements should be clearly defined by normative documents.

16. Many requirements directly or indirectly related to information security have been legally regulated at the international level and made into international standards. Application of these international standards in the field of information security leads to prevention of many information security risks and threats in a decisive and easy way. The adoption of national standards corresponding to those international standards has become the reality of our modern times, and with this, it will be possible to solve many problems.

17. Information technology tools have already become an integral part of everyday life. We can note that a specific approach should be given to the information security issues of people of

different age categories. One of the main issues here is the protection of children's rights in the cyber environment. This increases the importance of taking information security measures in cases where children's access to the relevant system or resource is ensured. Both from the point of view of human rights and from the point of view of the future prospects of society, security measures should be increased in the cyber environment where children's access is ensured, and access to environments that threaten their development should be limited.

18. Dissemination of information about children causes great harm by causing information security situations, as well as negatively affects the personal development and psychological state of children. Therefore, these cases should be taken into account when determining the legal regime of information about children. Currently, there is a need to make relevant changes in our national legislation in the mentioned direction. The presence of such loopholes in the legislation may result in increased information security risks, as well as human rights violations. In addition, mutual and complementary international and national legal mechanisms for the protection of this information, which we can include in the sensitive category, should be created.

19. It is one of the main requirements to ensure that the control of the protection of the information that is suspended and related to its own particular danger is ensured. Unauthorized access to undisclosed information may be subject to authorization, collection laws, or multiple uses. In turn, a special approach should be established in relation to that type of information. Therefore, resources where relevant information is available or resources using modern verification or authentication methods in providing access to systems. This ensures more efficient use.

20. One of the innovations applied in modern times is the use of biometric data in some documents confirming identity or rights. This is a widespread phenomenon in our country. So, biometric data is used both in citizen's passports and in identity cards. Although this makes a positive contribution in the field of ensuring security and fighting crime, it also causes an increase in information security

risks. So, it should be ensured that the systems where those biometric data are stored and verified meet special security requirements. Any gaps cannot be allowed in such systems. In order to ensure the protection of this type of information, specific requirements for information resources and systems for the storage, processing and use of biometric information should be determined by normative acts, as well as strict state control of the use of these systems should be implemented.

21. The implementation of digitization in various spheres has not bypassed the government services, as well as the inter-institutional documentation process. Legal regulation of electronic government services and the use of electronic document circulation systems is one of the modern legal trends. In this direction, it is necessary to make certain changes in the AR legislation. In addition, relevant legal mechanisms should be formed at the international and national level regarding electronic document, electronic government and electronic document circulation systems. So, this appears as the main requirement of the modern era.

22. Wide use of social networks is noticeable as one of the main features of the modern era. The number of social network users has also increased rapidly in our country. Although the social network is characterized as a positive platform environment for the provision of freedom of opinion, it can be evaluated as an environment where violations of honor and dignity, as well as other such human rights, are widespread. Thus, many threats in the direction of information security or privacy are caused by the use of social networks. Here, the ability to hide the person's identity, the ability to delete the user's profile on the social network at once, etc. situations cause dangers in the direction of information protection. At present, although certain changes have been made in this direction in our legislation, the regulation is not completely satisfactory from the point of view of information security. We believe that specific norms defining legal responsibility for information security risk or threatening activities of social network users should also be adopted. Due to its preventive nature, this will contribute to the provision of information security.

23. The Internet should be considered as one of the main means of access to information resources, systems and platforms. We can even mention that it is impossible to access many digital platforms without internet. Therefore, "internet", "information", "information protection" and "information security" should be given the most accurate definitions, and their interaction and influence should be investigated. According to the obtained results, all possible negative effects in ensuring information security should be eliminated and joint protection mechanisms against threats should be created.

24. The range of activities with direct or indirect risk of information security by using the Internet network should be defined. With this, it is possible to implement effective regulation and ensure information security. On the other hand, the legal responsibility according to the level of their danger should be precisely defined for socially dangerous acts that create an information security risk and cause incidents by using the Internet.

25. Legal responsibility for actions (action or inaction) committed and considered socially dangerous is an important issue in information legal relations. The fact that the scope of such actions must be precisely determined makes it necessary to make changes or additions to the legislation in accordance with the development of information technologies. It would be appropriate to make relevant changes in the current AR legislation in accordance with the development requirements of the modern era.

26. Ensuring human rights and freedoms is one of the main tasks facing all states. There are also new approaches in ensuring information rights, which constitute a new generation of human rights. Examining information security issues in the context of human rights would be useful in the direction of regulating existing legal relations, as well as ensuring and protecting human rights. Thus, some events that occur as a result of failure to ensure information security or information protection result in the restriction of basic human rights and freedoms. Therefore, the interaction and effect of "human rights" and "information security" should be investigated in detail, and the role of information security in ensuring

human rights should be thoroughly clarified. In this aspect, legal mechanisms for ensuring information security in the direction of human rights protection should be clearly defined.

27. The resolution of disputes related to the provision of information security causes difficulties due to the nature of these relations being new and in some parts uncertain. Sometimes, when the disputes related to information security are analyzed from a legal perspective, results cannot be obtained. The use of alternative dispute resolution in this area can also be considered successful. It seems that the parties sometimes do not use alternative dispute resolution methods, they avoid it. In addition, it is necessary to ensure the formation of uniform judicial practice in this direction. If we look at the statistics, even if the number of such disputes is much less than other types of disputes, their resolution is also a very necessary issue. Thus, the formation of a correct uniform judicial practice in this field should be ensured, and the courts hearing disputes should apply this judicial practice correctly.

28. As a result of information security incidents and events, different subjects are harmed in different amounts. It should be noted that legal responsibility for causing this damage is defined in the legislation. One of the defined types of legal responsibility is civil legal responsibility. There are great difficulties in determining the amount of damage in the settlement of disputes about compensation for the damage caused. Determining the economic value of information also becomes a difficult issue in itself. In other words, a single legal mechanism or procedure for determining how much material damage the subject has suffered as a result of an information security incident or event should be defined. In addition, information security incidents and events often cause physical harm to individuals. The amount of damage caused to a person by these moral sufferings should be considered as a matter that should be evaluated subjectively and according to the circumstances of each case. Although there are relevant decisions of the AR Constitutional Court and the Plenum of the AR Supreme Court regarding the determination of moral damage, certain difficulties still arise in determining the amount of this damage. Taking into account the

mentioned and in accordance with international practice, the circumstances to be taken into account in determining the amount of this damage, as well as the precise legal mechanisms of the method and order of determining the amount of this damage should be formed.

29. Information security threat or incident response is the process of detecting, analyzing, and responding to security incidents at the top of today's to-do list. In the event of an information security threat or incident, the relevant responsible subject must immediately react to it (take measures) and, if necessary, inform the relevant executive authority. Protection or security mechanisms for such cases should be formed, incident response plans should be prepared, network traffic monitoring for suspicious activity and expert analysis should be ensured. In addition, precise and detailed legal regulation of the implementation of the mentioned measures is necessary, and in this direction, normative documents should be prepared, and relevant changes should be made in the existing legislation.

30. One of the main mechanisms in ensuring information security is risk management. Taking this into account, it is necessary to ensure the process of identifying, evaluating and reducing risks for information security. This includes assessing risks, implementing security controls and developing emergency plans. Defining the general requirements for the management of the mentioned risks will increase the efficiency of the mentioned mechanism. Therefore, normative acts should be formed in the current direction, and additions or changes should be made to the normative documents according to the requirements of the modern era.

Scientific novelty of the study. A number of foreign authors have studied the important directions of information security in their research works, and have studied the internal defense mechanisms of information security. However, scientific researches in the field of international and domestic legal protection mechanisms of information security have hardly been carried out in the Republic of Azerbaijan, so far no comprehensive research work has been written on the international and domestic legal protection mechanisms of information

security of the state. This topic is studied for the first time at the dissertation level.

The scientific novelty of the dissertation is that, for the first time, information rights as an object of information security, state policy in the field of information security as a mechanism for the implementation of the main function of the state in the field of security, as a system for ensuring electronic state information rights, constitutional legal guarantees of the information law in the context of human rights, domestic legislation related to information security was considered as an important part of the security system, the universal and regional cooperation of our state in the field of information was studied, the features and directions of implementation of international universal and regional legal norms in the field of information security into AR legislation were examined.

Theoretical and practical significance of the study. It should be noted that the results obtained as a result of researching the legal aspects of information security of the state and the proposed proposals are of great practical importance in terms of both scientific-theoretical and improvement of legislation in the field of information. From the theoretical results and practical suggestions of the dissertation, in the law-making activity, as well as in the teaching process in higher schools, especially Information Law, Human Rights, Constitutional Law, Administrative Law, National Security Law, etc. it can be widely used in the development of textbooks, teaching aids, as well as teaching-methodical materials and programs, and in conducting scientific research on information security and improving legislation**.**

Approbation and application. The main provisions, conclusions and practical recommendations of the dissertation were published in the authoritative scientific journals and collections of scientific articles of AR, the USA, the Russian Federation, the Republic of Poland, Kazakhstan and Ukraine, and were reflected in the author's published works, abstracts and speeches of her reports at scientific and practical conferences.

The name of the organization in which the dissertation work is performed. The dissertation was completed at the Human

rights and information law UNESCO department of the Faculty of Law of Baku State University.

The structure of the research work. Dissertation consists of introduction, five chapters, conclusion and list of used literature.

THE MAIN CONTENT OF THE DISSERTATION

In the introductory part of the dissertation, the relevance of the topic is justified, the degree of development, object and subject of the research, goals and objectives, scientific innovation, the theoretical and practical importance of the new scientific propositions submitted to the defense are explained, the approval of the research results and the structure of the research are given.

The first chapter of the dissertation is called "Information security and its place in the national security system" and consists of two paragraphs.

The first paragraph, called "The concept of information security and factors affecting security", consists of two sub-paragraphs and analyzes the concept of information security, its main aspects, and issues such as confidentiality, integrity, availability, and accountability as factors affecting security.

The concept of information is based on the principles of confidentiality, integrity and availability. According to the degree of information use, these principles are also divided into different degrees of importance. In some national studies, priority has been given to the principle of confidentiality. Availability is the priority in the media field. The priority for an organization that broadcasts over the Internet is the continuous and fastest delivery of information to the other party. Sometimes a small caption can stand out from the crowd. Confidentiality is not sought in the given information, completeness may be unexpectedly transferred to the other party. For a judge in a trial, the principle of completeness is paramount. Sometimes this process lasts for years. Sometimes, some matters may lose their confidentiality when taking statements. When the goal is to make vital decisions based on the right information, the information to be obtained becomes even more important. It is gratifying that information security has been understood in the

legislation of the Republic of Azerbaijan. Thus, according to Article 2 of the AR Law "On Information, Informatization and Information Protection", information security is the integrity of information (accurate, clear, relevant and complete), availability (possibility of applying and obtaining, keeping under control), confidentiality (that it can be known only to authorized users and processes) and to protect its credibility (adequacy, objectivity, usefulness). As can be seen, the concept of information security with AR legislation is based on integrity, confidentiality and availability.

In general, confidentiality, integrity, availability, accountability are the main aspects of information security and factors affecting security.

In the second paragraph – "Information security standards and the risk factor in information security" – legal problems related to information security standards and the risk factor in information security are studied and includes three sub-paragraphs.

Information security standards are minimum requirements aimed at ensuring information security. It is particularly important that the places where information is stored and can be operated on, and mainly information systems, meet these tested and approved requirements for ensuring information security.

Before the extensive explanation of the risk factor in information security, it is possible to explain it succinctly as follows: Risk in information security is the occurrence of an event resulting in the illegal capture, use and damage of the information contained therein by using gaps in the information system or its resources.

In the dissertation, the risks affecting information security are classified and the main essence of the classification of information security risks is connected with the fact that the details such as where the risk can come from and how it can be affected in order to take protective measures are known in advance. In such a case, information security mechanisms can be defined and implemented more conveniently. Information security is also viewed as a broad field that includes the protection of intellectual property rights such as trade secrets, patents and copyrights. These differences in the legal

regimes applicable to both intellectual property rights and information complicate the issue of enforcement.

In general, detecting and preventing information security risks raises a number of legal challenges, including compliance with data protection and cybersecurity laws, liability and accountability, cross-border data transfers, and intellectual property protection. Organizations should consider these legal issues when designing and implementing information security strategies. This, in turn, protects them from liability and legal disputes that may arise.

The second chapter of the dissertation entitled "Information security in the electronic state and its importance" consists of two paragraphs. In this chapter, the place of information security in the management system, information security in the e-state, problems of ensuring information security in the e-state, e-signature as a means of ensuring information security, electronic data carriers as an object of information security are analyzed.

In the first paragraph entitled "The place of information security in the management system", it is mentioned that ensuring the interests of the state, society and citizens in the information space is one of the main goals of the state. First of all, ensuring and protecting human and civil rights and freedoms should be the main goal of a legal state. Therefore, ensuring the rights and legal interests of persons with legal subjectivity in the information society is one of the main issues facing the state. There is also a constitutional basis for this provision in AR legislation. Thus, according to the first part of the 12th article of the Constitution of the Republic of Azerbaijan, the highest goal of the state is to ensure human and civil rights and freedoms and a decent standard of living for the citizens of the Republic of Azerbaijan.

Taking into account that the current era is an information age, failure to ensure the protection of restricted state secrets, military secrets, personal data or other information can cause great difficulties in state administration and result in great damage to state and public interests. Currently, the dissemination of information is carried out faster than in the past. The reason for this has been the widespread use of information technology tools by every person in their daily

lives, the ease of access to such tools and the Internet. As a result, integrating the information security management system with the quality management system will significantly save time and resources along with the efficiency and quality of the system.

In the second paragraph entitled "Information security in the e-state", the issues of ensuring information security in the e-state, E-signature as a means of ensuring information security, and electronic data carriers as an object of information security are studied and consists of three sub-paragraphs.

Ensuring the transition to the electronic state in all areas of public life and almost all state bodies brings positive results, such as the easier provision of human rights and freedoms, the transparency of statistical indicators and the activities of state bodies.

Taking into account the above, it can be noted that before talking about the provision of information security in electronic government, the circle of subjects using it, the character and nature of the relations between each of those subjects should be analyzed and taken into account. In general, we can summarize the participants of legal relations related to the use of e-government in 4 categories. These are the categories of government (government-G), employee of a state body or institution (officials-O), business subject (business-B), citizen (citizen-C).

Many problems related to information security in electronic state or government systems are due to the fact that the main elements of information security are not provided. This approach proves itself in practice. In many cases, information security problems in the e-state or government are caused either by the negligent actions (inaction) of users, or by technical malfunctions or gaps in the system created by the entity responsible for information security, privacy policy adopted for the purpose of legal regulation, etc. may be caused by obvious mistakes made in other documents.

On the other hand, it is very necessary to ensure the confidentiality of information, which is one of the main pillars of information security in the electronic state, and to ensure the confidentiality of the electronic state information communication system or network and the operations conducted there. It is the fact

that this confidentiality is not ensured or cannot be ensured at an adequate level, in the future the information available, transmitted, processed or stored on the information platform may be illegally obtained by third parties, resulting in the creation of great threats to information security.

Thus, information security is essential for e-government systems to protect citizens' data, ensure the integrity of government systems, protect public trust, and comply with legal and regulatory requirements. The rapid development of information technologies and its application in all areas necessitates the application of electronic document circulation systems, as well as the application of certain verification methods or mechanisms in order to ensure the authenticity and immutability of documents in electronic form. The special importance of the electronic signature is the identification of the signatory, the fact that the authenticity of the documents signed by means of electronic signatures cannot be disputed, including the fact that the content of documents certified by means of electronic signatures cannot be changed.

Considering the above, electronic signature in its simplest form should be defined as a digital method or form of signing a document or contract. It is a legally recognized method of indicating that the signatory accepts the content of the document or contract and agrees to its terms. The security of electronic data carriers is important because they may contain sensitive or confidential information that, if accessed or intercepted, could have serious consequences such as theft, financial loss, and reputational damage.

The third chapter of the dissertation is entitled "Information security and its legal problems in the protection of civil rights and freedoms" and consists of three paragraphs.

The first paragraph, which consists of two subsections, is called **"Information security of personal data",** and here personal data and the procedure for their use, as well as the issues of ensuring information security of personal data, are considered.

The main issue that needs to be addressed and clarified here is the definition of the category in which the information is placed according to its nature or character. By reviewing and summarizing

the conducted scientific research and literature, we can say that according to the level of accessibility, information can be classified as open information, restricted information, and in some cases, sensitive information. It is also possible to note that the information restricted to access can be classified as information restricted to access by law and contract. Information whose acquisition is restricted by law is classified according to its legal regime and defined as secret and secret (confidential) information. According to confidential information, a state secret is related, while confidential information, as a rule, includes professional, commercial, investigative and court secrets, the acquisition of which is restricted in order to protect the legal interests of citizens, enterprises, departments, organizations, as well as other legal entities. What has been mentioned has been confirmed in AR legislative practice. The definition given to personal data in our legislation can be considered successful considering that the existing legal relations have a new character for our society. However, it would be more appropriate to give personal data a broader definition in our legislation that fully discloses its nature. Therefore, it is necessary to review international agreements in this field, as well as certain normative legal acts in the practice of foreign countries. It would be more correct to make a comparative analysis of the existing concepts in those acts and literature and to make a proposal to amend the legislation taking into account the unique characteristics of our society.

To ensure the security of personal data, all organizations, regardless of their organizational legal form, must establish a comprehensive activity that takes a number of information security measures. First of all, it comes from the obligations of these organizations imposed by law. Ensuring the legal use and protection of confidential personal data is the responsibility of the owner of the information resource where the confidential personal data exists or the operator providing the relevant services. Therefore, failure to take information security measures at the appropriate level and method may result in subjects being held liable under the law. In the context of information security, personal data privacy is important because

personal data is often a prime target for cybercriminals who want to steal or misuse it for their own gain.

The second paragraph, which consists of two sub-paragraphs, is called **"Information security of biometric data"** and it analyzes biometric data and the manner of their use, biometric data in various fields and their information security issues.

Biometric data is used in completely different fields due to its unique feature. Thus, the issues that are the subject of various fields of science, as well as public spheres and remain unclear, can be clarified precisely by using biometric data. First of all, some biometric data are distinguished by their immutability and uniqueness throughout their lifetime. These biometric data play a mysterious role in the process of identifying individuals. For example, individual unique data such as a person's fingerprint, face print, DNA data. They have an important role in providing solutions to the issues raised in areas such as criminal process, criminalistics, operational search activities. Also, biometric data, which includes a person's genetic information, plays a special role in the resolution of some civil disputes. As an example of this, civil cases on disputing paternity, determination of paternity, and claims on inheritance relations can be cited. The mentioned once again confirms the importance of using biometric data and biometric technologies to ensure information security. One of the most convenient ways to ensure information security in the modern digital information society with less risk and more easily includes the use of biometric technology, systems and data.

The third paragraph entitled "Domestic and international legal protection mechanisms for ensuring the information security of personal and biometric data" consists of two sub-paragraphs analyzing the legal aspects of the use and security of personal and biometric data in AR legislation and the use of personal and biometric data and the international legal aspects of their information security.

Determining the legal mechanisms for the use and protection of personal data is necessary because it is directly related to the basic human rights and freedoms of people and citizens. The issue of the

use and protection of personal data is not only an issue related to the information law. Ensuring information rights in the new generation of human rights, including a person's right to privacy in the digital society, has become one of the main goals of the state.

Protection of personal data is one of the main tools that affect privacy. From the mentioned perspective, we see that states must take many measures and conduct special control in this area in order to ensure the protection and proper use of personal data. Because this problem, which is closely related to the provision of basic human rights and freedoms, is in itself one of the factors that make it necessary for the state to pay special attention to this field.

The fourth chapter is entitled "The main problems of society's information security: legal responsibility and information protection" and includes two paragraphs.

The first paragraph is called "Social networks and information threats created by them" and consists of two sub-paragraphs, where social media and its impact on the information society, and then the Internet as a means of influencing the information security of the society, are analyzed.

Although social media is not defined in our legislation, media expression is defined. Thus, according to Article 1 of the AR Law "On Media", which regulates relations in the field of media, media means the tools and means used to carry out the periodic or regular publication and (or) broadcasting of mass information, as well as the information formed through them. the environment is understood.

Based on what has been mentioned, social media is defined in the dissertation as follows: social media allows users to create content, follow, share, exchange content created by themselves or other users, in some cases comment on existing content and exchange ideas, or in general social web-based platforms, applications and technologies that enable participation in networks are understood. However, the Internet also poses serious problems in terms of information security and privacy. This can be considered as its negative aspect.

Large amounts of restricted information transmitted and stored online, i.e. personal information, state secrets, military secrets,

personal and family life secrets, etc. they can be vulnerable to cyber-attacks and hacking. Information security risks on the Internet level in some situations are greater than information stored on printed media. This puts individuals and organizations at risk of data theft, financial fraud and other forms of cybercrime. In a certain sense, sometimes transactions carried out on the Internet can arouse suspicion in the responsible persons and cause them to start an investigation. Although the Internet has made people's daily lives easier, it has been widely criticized by many researchers for the misuse of information and resulting material damage.

Governments, civil society organizations, and the private sector are working together to develop new policies, technologies, and practices to address these challenges and ensure that the Internet remains a safe and open platform for communication, innovation, and development. This includes efforts to promote digital literacy, improve cyber security, and protect the privacy of individuals and organizations.

The second paragraph called "Legal responsibility and information protection" consists of three sub-paragraphs, analyzing current issues such as legal responsibility as a preventive measure in ensuring information security, information protection as a means of ensuring information security, information security culture and its role in ensuring information security.

The institution of legal responsibility is studied as one of the important mechanisms in most legal fields. It is legal responsibility that plays a key role in the regulation of social relations. If we look at the legislative acts regulating various fields, we can determine that in those normative sources, it is determined that its violation will lead to legal responsibility. In addition to ensuring justice, which is the general principle of this right, it is distinguished by its preventive effect on individuals in society. Established legal liability deters a person from committing such illegal acts. The main condition for the emergence of legal responsibility is the commission of a violation that is considered a legal violation. It is only after this situation exists that we can talk about the emergence of legal responsibility and the involvement of individuals. Legal responsibility may not be

sufficient to ensure information security, as it relies on effective enforcement and compliance mechanisms. It is known that information protection is distinguished by its special role in information security. In real practice, information protection acts as one of the most important stages of the process of ensuring information security. Information security culture acts as one of the main factors leading to the reduction of threats and risks in the field of information protection. The first and most important point in the formation of the culture of information security is the organization of educational work. When the participants of information legal relations get information about the knowledge and rules of behavior related to information security, they can better control their activities and achieve more secure operations on information.

The fifth chapter of the dissertation is called "Interaction and development of domestic and international legal mechanisms of information security" and consists of three paragraphs.

The first paragraph is called "Mechanisms of internal protection of information security" and includes two sub-paragraphs. In this paragraph, the state of the normative legal framework that ensures information security, the problems of applying national legislation in ensuring information security in the globalized world are analyzed.

Norms directly or indirectly related to ensuring information security in the Republic of Azerbaijan are defined by normative legal acts at different hierarchical levels.

Although there is no single codified normative legal act on the provision of information security, many legislative acts directly or indirectly contain norms aimed at ensuring information security.

The process of globalization, the activities carried out within this process, elements of globalization are distinguished by their significant impact on information security. Globalization in the field of information security reflects the implementation of information security measures in a single cyberspace and the formation of global defense mechanisms. As a result of globalization, the unified cyberspace defines new approaches to human rights, but it should

also be noted that the general starting principles related to human rights cannot be touched here.

Although globalization has resulted in the complication of existing legal relations, even though it has some negative effects, it also has many positive effects. Thus, globalization shows its positive effect on the need to do more work in the direction of raising the standard of living of people, developing and improving the existing applied standards, and increasing the welfare of the people.

The second paragraph, called "Mechanisms of international legal protection of information security", includes two sub-paragraphs. This paragraph analyzes the international-legal regulation of information relations and the international-legal problems of ensuring the information security of the state from the point of view of information security.

In terms of information security, the international legal regulation of information relations includes the sources of international law, international rules and standards that are designed to protect the privacy, integrity and accessibility of information in the globalized world and regulate relations in this field. In terms of information security, the international legal regulation of information relations is a complex issue that touches on multifaceted legal, technical and political considerations. In the context of information legal relations, the adoption of regulatory international norms in the field of information security is necessary in terms of cooperation in the field of ensuring information security in the global space, as well as the determination of minimum standards. The application of the main international legal framework norms adopted for information is aimed at minimizing risks in the field of information security. In terms of information security, the international legal regulation of information relations is a complex and rapidly developing field and will continue to be shaped by technological, political and social developments in the coming years. There is a direct and some indirect effect of some international acts on ensuring information security. First of all, it should be noted that information security is closely related to basic human rights and freedoms. Therefore,

international acts defining human rights and freedoms also play a role in regulating information security.

The third paragraph entitled "Experiences of individual states in ensuring information security" includes two sub-paragraphs. In this paragraph, the experiences of foreign countries in the regulatory and legal provision of information security and the importance of cooperation of states in the sphere of international information security are analyzed.

Analyzing the legislation of other countries in the sphere of information security is very effective in the direction of developing the normative base. It can be said that a large number of states have started forming the legislative framework on information security. States with a very high level of development of information legal relations have implemented legislative activities aimed at ensuring information security at a high level, and are continuing to do so at the present time. In this paragraph, the United States, Singapore, South Korea, China, Japan, Poland, Ukraine, Turkey, etc. the experiences of such states were analyzed.

Ensuring international security and implementation of cooperation in this field, as well as implementation of the duties of each state in this direction, is one of the main issues of the modern era. First of all, this is due to the common interests of the states. Thus, the activities of the entities that create a threat at the international level are socially dangerous and result in damage to the daily activities of more than one country in the social, economic or political and other spheres. This also requires joint cooperation in order to prevent incidents that may be committed in different spheres. It can also manifest itself in a broader form at the level of regional or universal cooperation. Taking into account the systematic and structural nature of international security, it raises the issue of developing a security system that includes several comprehensive alternatives in modern times.

In the final part of the dissertation, the results obtained as a conclusion of the research are defined in 15 points:

1. Information security was defined according to the amendment (May 27, 2022) to the Law of the Republic of Azerbaijan dated April

3, 1998 "On Information, Informatization and Information Protection". However, the mentioned concept includes confidentiality, integrity and availability as well as the sign of credibility. Considering that in world practice, only 3 elements (CIA) are taken as a basis, and integrity also includes reliability (integer - accurate, relevant, complete, clear information is reliable in every case). From this point of view, it can be considered that the element of authenticity creates repetition without substantial difference.

2. Ensuring information security has become more relevant in the modern era, when the global information society is established. Therefore, many international legal sources have been adopted in this field. When solving the legal problems of information security in domestic law, it is important to take into account and be guided by those international legal sources. At the same time, studying the experience of developed foreign countries in ensuring information security and applying it in our republic is also considered favorable. Also, we should note that information security is a dynamically developing direction, and in connection with the rapid development of ICT, different terms and concepts appear every day. It is very important to give a legal explanation to such concepts at the international level. Because all countries of the world refer to international norms when formulating their national legislation. If we consider that in recent times, the whole world already uses the concept of artificial intelligence, robots, electronic identity, smart things, driverless cars. There is a need to establish these concepts in legislation and regulate the mechanisms of their use.

3. The objects of information security are the problems related to ensuring the information security of the state, society and the individual. The information security of the state serves to protect its national security, constitutional structure, territorial integrity and sovereignty, the information security of the society serves to protect its material and moral well-being, and the information security of the personality serves to protect human rights and freedoms. The solution of legal problems on ensuring the information security of each object is carried out in a unique direction. Thus, one of the problems facing the information security of the state manifests itself

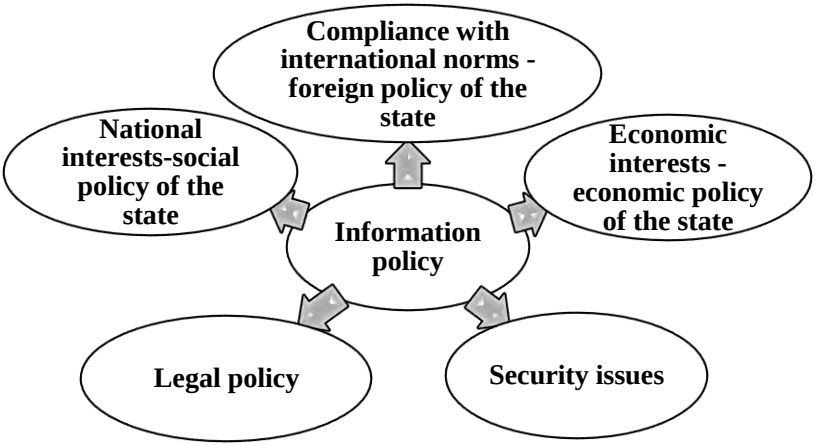
in the lack of local production of microcircuits and other carriers used to store electronic data. This does not exclude the control of those carriers imported from foreign countries by the manufacturer or other countries. The mentioned problem can lead to the transfer of information constituting a state secret in the Republic of Azerbaijan to other states, various information attacks, and as a result, damage to state security. According to the amendment (May 27, 2022) to the AR Law of April 3, 1998 "On Information, Informatization and Information Protection", the critical information structure, its object, subject and the authorized body ensuring the security of this information structure were defined. At the same time, on May 27, 2022, the Code of Administrative Offenses provided for an administrative offense and the type of administrative responsibility for violations of these rules. Taking into account the relevance of the issue from the point of view of the security of the state, it can be considered that the taking of information from the objects belonging to the critical information structure should be considered a crime in terms of the public danger of the act and should be provided for in the chapter of the Criminal Code against the fundamentals of the constitutional structure and security of the state.

4. Ensuring information security should be mentioned among the directions of the state's national information policy. UNESCO's Information for All Program defines five priority directions in the National Information Society Policy (MICS): Information for development; Information literacy; Information preservation; Information ethics; Information accessibility.

The national information policy includes a system of measures and rules aimed at ensuring the availability of information for society as a whole and is divided into 2 parts: information strategy and information tactics. The information strategy is a planned action model aimed at solving large-scale information problems, which is ultimately aimed at the successful completion of the informatization processes and the unhindered provision of information rights and freedoms. Information tactics are formed on the basis of information strategy, and include specific measures implemented to achieve the set goals and objectives. This means that information strategy

answers the "what" and "why" questions, while information tactics answers the "how" question. Unlike strategy, information tactics are characterized by flexibility.

The implementation of the national information policy is impossible without taking into account other aspects of the state's activity. So, it would be somewhat illogical to talk about the informatization and electronicization processes and the provision of information availability in economically inefficient conditions. On the other hand, an information policy that does not take national interests into account cannot be implemented successfully. Also, an information policy that is implemented without observing international norms and has no legal basis will eventually lead to a conflict of interests. Another side manifests itself in the fact that it is impossible to achieve the normal implementation of information policy in a situation where national security is not protected:



Taking into account the above scheme, it can be concluded that the national information policy means a complex system of measures implemented by state bodies. Concentration of national information policy only in state authorities cannot mean restriction of human rights and freedoms. In fact, the provision of rights and freedoms, prevention of violations of rights, and etc. the state has always existed as a governing institution for the performance of such tasks.

At a time when the idea of a legal state is widespread, it is impossible to achieve the goals without the role of the state. Of course, monitoring the activities of the state bodies itself is considered one of the important factors. That is why one of the main principles of the legal state - mutual responsibility, that is, the responsibility of the person to the state and the state to the person - is always guided. At the same time, the promotion of open government, public control, civil society and other ideas has an important impact on the implementation of the state's national information policy. Summarizing our opinion, it can be concluded that the state's national information policy should not be implemented unilaterally, but within the framework of complex measures.

5. As for the information security of the identity, special attention is paid to the prevention of information threats directed against the identity, as the human factor is brought to the fore in the modern information society. The number of computer incidents continues to increase day by day, despite the operation of the Special Communication and Information Security State Service's Computer Incident Response Center, Electronic Security Service under the AR Ministry of Digital Development and Transportand other institutions. In fact, since ICT has become a tool and tool in the commission of most crimes, all this leads to the violation of the integrity, availability and confidentiality of information. By using the network, by obtaining any information of a person, it is possible to encroach on any of his rights and freedoms. All this requires a comprehensive legal approach to personal attacks, changes and amendments in many legislative acts. It is not correct to place all the solutions on the mentioned issue only on the legislator. It is also in accordance with the goal of increasing the number of scientific researches in the field of information security, therefore in the field of information rights, developing proposals and presenting them to the legislative body. In addition, it is not possible to choose some subjects of the main rights persons in the virtual environment. By using various fake profiles, it is possible to perform actions directed against the person (insult, slander, etc.). But with respect to liability issues, there is some development in determining the subject of a breach of the providers'

limited liability. On the other hand, making the detection and prevention of identity threats extremely strong. This means that the latency level of such threats is high. In order to eliminate such listed problems, it is considered more appropriate to receive information or revise these potential legislative acts.

6. Various normative legal acts have been adopted in AR for the purpose of legal regulation of relations related to the use of personal data. It should be noted that it is possible to determine the nature of data based on the definition given in the AR Law "On Personal Data". Thus, according to the requirements of the AR legislation, the information must have one of the following characteristics to be classified as personal information: it must allow direct identification of the person; it should allow to indirectly determine the identity of the person. The definition given to personal data in our legislation can be considered successful considering that the existing legal relations have a new character for our society. However, it would be more appropriate to give personal data a broader definition in our legislation that fully discloses its nature. Therefore, international agreements in this field, as well as certain normative legal acts in the practice of foreign countries, were considered in the dissertation. It is appropriate to make changes to the legislation taking into account the specific characteristics of our society and the comparative analysis of existing concepts in those acts and literature. For example, the 1981 European Convention on the Protection of Individuals with regard to Automated Processing of Personal Data, which AR is also a supporter of, defines personal data.

7. The approach defined in the mentioned Convention, being even more general, refers to the category of personal data any information related to a specific or identifiable individual. Such information may include a person's name, surname, father's name, date of birth, other information contained in identity documents, as well as information about race, ethnic origin, family life, religious belief, belief, health or conviction. But such details are not disclosed in the AR Law "On Personal Data Protection". In order to avoid ambiguities and legal disputes in legal relations arising in this field, the concept can be defined more broadly. When the current practice

is analyzed, it is determined that giving the concept in such a general way will bring up the issue of interpretation of the data category. This can create difficulties in the subjective approach of professionals, lawyers, judges or other officials, including the worsening of the situation of citizens. In this regard, we believe that the category of data that allows direct and indirect identification of a person should be listed as in the Convention, which will prevent different approaches in solving the controversial issue of privacy of personal data in the future.

8. The most developing direction of e-state manifests itself in the electronicization of the executive body. Electronic services provided to the citizen through various websites open wide opportunities for him to realize his rights and freedoms freely and without hindrance. However, in addition to the advantages, this system also has some problems. For example, in order to register through the Electronic Government Portal, it is essential to have a mobile number in the person's name and to have documents that prove their identity. The fact is that at least three main documents are required for registration. In our opinion, it is more appropriate to reduce the number of these requirements. Because many citizens do not have a foreign passport, SSPF card or driver's license. Therefore, it may be more appropriate to require only mobile number and ID card to register in the system. Using the electronic service provided in this way will be easier and more convenient. With the new change, video registration has been added as an alternative to the triple document, but in this case, the result of the video application is checked within 5 working days, and after approval, the account is activated, which is already a waste of time, which is actually against the basic idea of e-government. We believe that only registration with FIN and mobile number is sufficient.

9. General measures to prevent cyber threats are implemented by the state. First of all, it should be noted the determination of responsibility for various violations and the imposition of sanctions. Traditionally, depending on the nature of violations, four types of liability are distinguished – criminal, administrative, civil and disciplinary. However, in modern times, concepts such as

international-legal responsibility and constitutional-legal responsibility are also encountered. What type of information legal responsibility belongs to and how it is regulated becomes relevant at this time. The point is that sanctions for legal violations committed during the implementation of relations in the information field have not been established in the information legislative acts. Violations of information and law that are dangerous to the public are provided for in the criminal legislation, violations characterized by the signs of an administrative offense are provided for in the administrative legislation, various offenses are provided for in the civil legislation, etc. However, taking into account the borderless nature of the information field, the existence of problems and collisions related to information-law violations, it is impossible to interpret those problems in the areas of criminal, civil and administrative law. For example, cyber threats and information threats are not only directed against a specific citizen, but also have a negative impact on the morale of society. Development of proposals and recommendations for prevention of such threats can only be possible within the framework of information law science. Based on all this, the analysis of information-legal responsibility as an independent legal institution can be considered appropriate.

10. The globalization of all spheres of society, the formation of cyberspace makes it possible to commit information violations in an easier and more flexible way. The fight against cyber threats, which is one of the most urgent problems of the modern era, is carried out on a global scale. Any gap or deficiency in electronic information systems results in the destruction of all data. Therefore, both at the international and national level, the information security of the e-state should be highlighted as one of the main directions of the state's information policy. Since information security is a broader concept than electronic security, the provision of electronic security in e-government serves to ensure the integrity, availability and confidentiality of information. Therefore, an ordinary citizen who uses the opportunities created by the e-state should be sure that his rights and freedoms are protected and he will not be subjected to criminal attempts. Because the search for a criminal in a space with

unknown borders is extremely difficult, it requires a "sensitivity" approach to cybercrimes, both nationally and internationally. We can even say that cybercrimes cause more serious consequences than crimes committed by traditional methods. In this regard, the principle of cooperation in the prevention of cyber threats should be guided. If this is done in two directions, more effective results can be achieved: cooperation of states - at the international level and cooperation of citizens and state authorities - at the national level. In the era of rapid development of ICT, traditional crimes are more preferred to be committed using ICT. In today's era, it is not necessary to take money by pulling a gun on a person, with the help of technology, it is possible to get rich in easier ways (cyber fraud, etc.). It is even possible to bring a person to the point of suicide in the virtual world from a distance. Therefore, we consider it appropriate to revise the concept of "cybercrime" in legal sources related to cyber threats. In this case, different classifications of cybercrimes can be used in the theoretical literature. Thus, from the separate categories of crimes established in the 2001 Convention on Cybercrime, to which the Republic of Azerbaijan also joined, Chapter 30 of the Criminal Code of the Republic of Azerbaijan was revised on June 29, 2012, and only access to the computer system (Article 271), illegal seizure of computer data (Article 272), illegal interference with computer system and computer data (Article 273), circulation of tools designed for committing cybercrimes (Article 273-1), falsification of computer data (Article 273-2). However, neither fraud using computer technologies, nor crimes related to the content of information (the crime of child pornography), crimes related to the violation of copyright and related rights, nor crimes related to threats to public safety crimes (this category includes cyberterrorism and terrorist purposes such as the use of cyberspace) are not defined in the Criminal Code. It should be taken into account that since the crimes that occur in the electronic state mostly occur in the electronic environment, it is very important that the crimes listed above are defined as a separate clause within the same article in the Criminal Code of the Republic of Azerbaijan. Among other things, we would like to note that recently, as a result of the theft of personal data

through virtual games and social networks and their use as a method of blackmail, there has been an increase in the statistics of suicide crimes. The mentioned issues make it necessary to add a new Article 125-1 to Article 125 of the Criminal Code of the Republic of Azerbaijan.

11. In order to ensure and protect human rights in cyberspace, it is necessary to form and develop the culture of information security. The formation of the information security culture is particularly important in strengthening the measures for the protection of personal data, in eliminating the negative effects of the cyber environment on human psychology. In this regard, the use of slogans proposed by English authors for both parents and children to ensure information security (for example, do not try to do online what you cannot do face-to-face, try to teach children Internet safety from an early age, etc.) and also with computer incidents it can be considered appropriate to further strengthen the work of the fighting bodies.

12. Considering the importance and role of social media in the field of media today, it would be more appropriate to define the term social media independently in our legislation. Because today many media subjects, information agencies and media platform owners widely use the power of social media and networks. Even the activities of many media organizations are based only on social network platforms. From this point of view, it can be noted that defining the term social media in the Law on Media will eliminate gaps and misunderstandings in legal disputes that may arise. It should also be noted that giving an understanding to online media in that Law should be considered as a commendable case. Based on the above, we can define social media as follows: social media allows users to create content, watch, share, exchange content created by themselves or other users, in some cases comment on existing content and exchange ideas, or in general on social networks web-based platforms, applications and technologies that enable participation are understood. Social media platforms or applications typically involve the use of internet and mobile technologies to facilitate the creation and sharing of content such as text, photos, videos and audio recordings.

13. The formation of a special platform or an institutional organizational mechanism of international cooperation in the field of information security would be appropriate in terms of coordination of information security and international and national security in a wider spectrum. Adoption of international normative acts within the framework of that international platform or organization, as well as formation of intergovernmental universal implementation mechanisms, and etc. is quite necessary. On the other hand, the uniqueness and specificity of cybercrime causes difficulties in its investigation or in the process of responsibility for these acts. At this time, cooperation within the framework of the proposed universal platform or international organization will facilitate the process of investigation and evidence collection by providing experience and legal assistance in this field, and by making interstate cooperation in the mentioned field effective, a high level of combating cybercrime can finally be achieved.

14. The implementation of legal awareness by ensuring the dissemination of educational materials on information security by using the main tools of the globalized world and internet platforms that have become a part of people's daily life makes its positive contribution to ensuring information security at the international level. In order to effectively implement this, the owners of global internet or social network platforms can be involved in the work process, and as social (public) responsibility measures, such educational materials can be ensured to reach a wider audience. The implementation of all these measures will lead to the development of the legal thinking of the subjects of the global information society, the formation and development of the universal information security culture.

15. Establishing effective regional legal mechanisms to combat the growing cybercrime and socially dangerous acts in the field of information security would have made a positive contribution to reducing information security risks. The similar historical, cultural and legal thinking of the countries of the region can be taken as an indicator of the usefulness of such mechanisms. Regional international agreements adopted taking into account the

characteristics of similar social, economic and legal systems become the basis for better regulation of information security. In addition, cooperation within the framework of various organizations or institutions as a regional defense mechanism, fight against cybercrime, development of the normative legal framework regulating information security, exchange of experience that has embodied its positive results in practice, development of personnel potential and human capital operating in the current field, as well as academic and social as a result of joint activity in the field of research, it is possible to fully achieve effective solutions to many legal and practical problems encountered by states.

The following scientific works were published by the author in connection with dissertation research:

1. Информационное общество и глобализация: тенденции развития информационного общества и правовые реформы в Азербайджанской Республике / Рзаева Г.А // Юридична наука і практика: пошук правової гармонії: збірник матеріалів Міжнародної юридичної науково-практичної конференції «Актуальна юриспруденція», - Киев, - 2017, - с.65-69
2. Fərdi məlumatların müdafiəsində informasiya təhlükəsizliyinin rolu // M.N.Ələsgərovun 90 illik yubileyinə həsr olunmuş "Azərbaycanda hüquq elminin müasir inkişaf istiqamətləri və tendensiyaları" mövzusunda beynəlxalq elmi-praktik konfrans, - Bakı, - 2018, - s.197-201
3. İnformasiya mədəniyyətinin informasiya təhlükəsizliyində rolu // BDU Hüquq fakültəsinin 90 illik yubileyinə həsr olunmuş "Azərbaycan Respublikasının Beynəlxalq cəmiyyətə inteqrasiyası və hüquqi dövlət quruculuğunda hüquq elminin müasir inkişaf tendensiyaları" mövzusunda beynəlxalq elmi-praktik konfrans. - Bakı, - 2018, - s. 53-56
4. Информационная безопасность: проблема неприкосновенности личностных прав / Алиев А.И., Рзаева Г.А // Міжнародний журнал право і суспільство, - Івано-Франківськ, -2018, № 7. - с. 5-24
5. Основные тенденции развития информационной сферы: отрасль публичного, или частного права? / Рзаева Г.А // Министерство образования и науки Украины Национальный авиационный університет, VIII Международной научно-

практической конференции «Современное университетское правовое образование и наука» - Киев, - 2018, - с.117-121
6. Понятие информации, ее социальная, правовая природа и специфические особенности / Алиев А.И., Рзаева Г.А // - LUBLIN: Fundacja “Ośrodek Rozwoju Kompetencji Akademickich” area nauki, kwartalne międzynarodowe czasopismo naukowe, - 2019, - с.4-16,
7. Информационное общество и тенденции его развития / Рзаева Г.А // - Волгоград: Актуальная наука: международный научный журнал., - 2019, №1 (18), - с.69-75
8. Information and media rights in the information society: social and legal analysis. / Amir Aliyev, Gulnaz Rzayeva, Nigar Alakbarova // XIV international scientific and practical conference social and economic aspects of education in modern society. - Warsaw, - 2019, - p.41-49
9. Национальный опыт обеспечения информационной безопасности / Алиев А.И // X International scientific conference «juridical science innovative development in conditions of social modernization». - 2020, p.130-133
10. Cybercrimes and struggle agains them// Науковий вісник Дніпропетровського Державного Університету Внутрішніх Справ, - 2020, №2, p.151-157
11. Digital citizen and information security// Proceedings of the 7 th international conference on control and optimization with industrial applications. Baku,-2020, p.326-329
12. Digital divide as an obstacle to the formation of information society / Amir Aliyev, Gulnaz Rzayeva // Proceedings of the 7 th international conference on control and optimization with industrial applications. - Baku, - 2020, - p.107-110
13.Kibertəhlükələr və onların təsnifatı// Bakı: Bakı Univeristetinin xəbərləri sosial-siyasi elmlər seriyası. - 2020, №1, - s.5-14
14. Milli təhlükəsizlik sistemində informasiya təhlükəsizliyinin yeri // - Bakı: Azərbaycan hüquq jurnalı, - 2020, №1, - s.48-59
15. Peşə və kommersiya sirrinin müdafiəsində informasiya təhlükəsizliyinin rolu // Umummilli Lider Heydər Əliyevin anadan olmasının 97-ci ildönümünə həsr edilmiş “Müasir dövrdə hüquq sahələrinin qarşılıqlı əlaqəsi və tətbiqi: nəzəriyyə və təcrübə mövzusunda Beynəlxalq elmi-praktik konfrans. - Bakı,-2020,-s.93-96

16. Information security: theoretical, legal and organizational challenges/ Amir Aliyev, Gulnaz Rzayeva // Journal of Information Science, - 2020, vol.8, - p.1-14
17. Meaning and position of human dignity in the constitution - theoretical and dogmatic dimensions/ Amir Aliyev, Gulnaz Rzayeva, Shahin Mammadrzalı // Global human dignity project, - 2020, - p.1-11
18. Organization of information security in e-government as means of information rights protection/ Gulnaz Rzayeva // Legal Journal "Law of Ukraine". - 2020, №4, - c.225-244
19. The defintions of information and security; history of information security development // Vilnius:The future decade of the eu law, 8th international conference of phd students and young researchers, «teise» journal of Law faculty, - 2020, №.2, - p.48-58
20. Dövlətlərin fərdi məlumatların mühafizəsində öhdəlikləri; Avropa İnsan hüquqları Konvensiyasında fərdi məlumatların mühafizəsi // International conference: XXI century, new challenges and modern development tendencies of law, Baku State University Baku, - 2021, - s. 97-105
21.E-dövlətdə informasiya təhlükəsizliyinin təşkili və informasiya hüquqlarının müdafiəsi anlayışı // - Bakı: Polis Akademiyasının elmi xəbərləri elmi hüquq jurnalı.- 2021, № 2 (30), - s.96-112
22. Fərdi məlumatlar və əlaqədar hüquqlar; fərdi məlumatların mühafizəsi // - Bakı: Bakı Univeristetinin xəbərləri sosial-siyasi elmlər seriyası. - 2021, №4, - s.64-78
23. İnformasiya təhlükəsizliyi; təhlükəsizlik və informasiya anlayışı // - Bakı: Polis Akademiyasının elmi xəbərləri elmi hüquq jurnalı.- 2021, № 4 (32), - s.85-93
24. İnformasiya təhlükəsizliyində standartlar və onların əhəmiyyəti// Ulu Öndər Heydər Əliyevin anadan olmasının 98-ci ildönümünə həsr olunmuş "Heydər Əliyev və Azərbaycanın inkişaf strategiyası" adlı respublika elmi-praktiki konfrans. - Bakı, - 2021, - s.71-74
25. Şəxsi həyat və onun informasiya təhlükəsizliyi / AR DTX Heydər Əliyev adına Akademiyasının "Azərbaycan Respublikasının suverenliyinin, müstəqilliyinin və ərazi bütövlüyünün Konstitusiya əsasları" adlı Respublika elmi-praktik Konfransı. - Bakı. -2021, - s.150-159

26. Virtual məkanda kibertəhlükələr və insan hüquqlarının müdafiəsi: beynəlxalq və milli-hüquqi tənzimetmə // Gülnaz Rzayeva // - Bakı:Azərbaycan hüquq jurnalı, - 2021, №1, - s.42-65
27. Информационная безопасность в информационном обществе// XI міжнародної науково-практичної конференції XI international scientific conference «Сучасне право в епоху соціальних змін» «modern law in the era of social transformation»- Київ, -2021, - с.96-99
28. Понятие персональных данных; информационная безопасность права на неприкосновенность частной жизни согласно анализу статьи 8 Европейской конвенции по правам человека // Северо-кавказский юридический вестник научно-практический журнал, - 2021, №4, - с.92-104
29. Information rights and information security in the context of fair trial / Amir Aliyev, Gulnaz Rzayeva // International Asian congress on contemporary, 2021, p.124-167
30. Artificial intelligence and personal data: international and national framework / Amir Aliyev, Gulnaz Rzayeva // International conference "Data-driven human rights research" University of Padova, -2021, - p.97-123
31. Information security and influencing factors // Право Украини, юридический журнал.- 2021, №4, - с.234-244
32. The factor of the risk and risk management in information security //«Вестник КазНУ. Серия юридическая», Казахский национальный университет имени аль-Фараби, - 2021, №4 (100), - с.97-106
33. The impact of new technologies on human rights in the context of the right to be forgotten and the right to privacy / Gulnaz Rzayeva // Legal Journal "Law of Ukraine". - 2021, №2, - с.125-150
34. The impact of information and communication technologies on intellectual property rights / Zaur Aliyev, Nazrin Aliyeva // Proceedings of the 8th international conference on control and optimization with industrial applications, - Baku, - 2022, Vol II, - p.84-87

The defence will be held at the meeting of BED 2.44 One-time Dissertation Council operating at Baku State University, at 28 on February 2024

Address: Academic Zahid Khalilov street, 23. Postal Code: AZ 1148, Building I, auditorium 805.

Dissertation is accessible at the Baku State University Library.

Electronic versions of dissertation and its abstract are available on the official website of the Baku State University

Abstract was sent to the required addresses on 26 January 2024.

Signed for print:
Paper format:
Volume:
Number of hard copies: