ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICALY

2 (342)

APRIL – JUNE 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*

Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Тиражы: *300 дана.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Physical-mathematical series.

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2, Number 342 (2022),5–18
https://doi.org/10.32014/2022.2518-1726.126

UDC 338(575.2); 340.13

T.I. Ganieva[1], N.S. Semenov[2]*, S.R. Semenov[2]

[1]Kyrgyz National University named after J. Balasagyn,
Bishkek, Kyrgyzstan;
[2]International University of Kyrgyz Republic, Bishkek, Kyrgyzstan.
E-mail: *frindland@mail.ru*

CYBERSECURITY OF INFORMATION RELATIONS IN THE FIELD OF INFORMATION INFRASTRUCTURE OF A GLOBAL SOCIETY

Abstract. The article deals with cybersecurity issues in the field of information relations, with an analysis of the legislation of the countries of the European Union (EU), Japan and the states of the Eurasian Economic Union (EAEU). Information relations in the world are becoming one of the important components of the interaction of various subjects of law, where, in the practical implementation of relationships, legal issues arise in the field of data security. The information environment, expressed in the form of the Internet space, is a key factor that is based on the information infrastructure. The rapid development of information infrastructure gives impetus to the process of the emergence of new legal norms, institutions, branches in the field of law, which makes it possible to ensure legal regulation of cybersecurity both at the national and international levels, taking into account the legislation of certain countries included in the integration associations.

The purpose of the work is to analyze and formulate proposals for the further development of new directions in the field of cybersecurity based on the development of a common information infrastructure based on the development of legal, economic relations aimed at ensuring data security.

Cybersecurity, as an area of information technology protection, is intended to regulate information and communication technologies in the

масын ескере отырып, ұлттық және халықаралық деңгейлерде киберқауіпсіздікті құқықтық реттеуді қамтамасыз етуге мүмкіндік береді.

Жұмыстың мақсаты – деректер қауіпсіздігін қамтамасыз етуге бағытталған құқықтық, экономикалық қатынастарды дамыту негізінде, жалпы ақпараттық инфрақұрылымды дамыту негізінде киберқауіпсіздік саласындағы жаңа бағыттарды одан әрі дамыту бойынша ұсыныстарды талдау және тұжырымдау. Киберқауіпсіздік, Ақпараттық технологияларды қорғау саласы ретінде, ғаламдық желіні және оны пайдаланушылардың қауіпсіздігі мен ақпараттық-коммуникациялық технологияларды реттеуге арналған; бұл сала өзекті болып, жалғасып жатқан жаһанданудың шоғырланған көрінісіне айналады.

Ақпараттық қатынастарды дамыту жөніндегі зерттеулер құқықтық және экономикалық ақпарат алмасу үшін ортақ құрылым құратын ақпараттық заңнаманы, оның ішінде ЕАЭО-ға мүше мемлекеттерді қалыптастыруға ықпал етеді. Цифрлық процестердің қауіпсіздігін халықаралық бақылау тетігін құру ақпараттық-коммуникациялық технологияларды, интернет желілерін дамытудың, жаһандық инфрақұрылымды құруда мемлекеттер мен бірқатар елдердің интеграциялық өзара іс-қимылын қамтамасыз етудің басым бағыты болып отыр.

Түйін сөздер: киберқауіпсіздік, ақпараттық қатынастар, ақпараттық кеңістік, ақпараттық инфрақұрылым, ЕО, ЕАЭО, стратегия, тұжырымдама, заңнама, экономика.

Т.И. Ганиева[1], Н.С. Семенов[2]*, С.Р. Семенов[2],

[1]Кыргызский Национальный Университет им. Ж. Баласагына,
Бишкек, Кыргызстан;
[2]Международный Университет Кыргызской Республики,
Бишкек, Кыргызстан.
E-mail: *frindland@mail.ru*

КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГЛОБАЛЬНОГО ОБЩЕСТВА

Аннотация. В статье рассматриваются вопросы кибербезопасности в области информационных отношений, с проведением анализа законодательства стран Европейского союза (ЕС), Японии и государств Евразийского экономического союза (ЕАЭС). Информационные отношения в мире становятся одним из важных компонентов

взаимодействия различных субъектов права, где при практической реализации взаимоотношений возникают правовые моменты в области обеспечения безопасности данных. Информационная среда, выраженная в виде интернет-пространств является ключевым фактором, который основан на информационной инфраструктуре. Быстрое развитие информационной инфраструктуры дает толчок процессу появление новых правовых норм, институтов, отраслей в области права, что дает возможность обеспечить правовое регулирование кибербезопасности, как на национальном, так и на международном уровнях, с учетом законодательства тех или иных стран входящих в интеграционные объединения.

Цель работы - на основе развития правовых, экономических отношений направленных на обеспечения безопасности данных дать анализ и сформировать предложения для дальнейшего развития новых направлений в области кибербезопасности, основанных на развитии общей информационной инфраструктуры.

Кибербезопасность, как область защиты информационных технологий предназначена для регулирования информационных и коммуникационных технологий в области защиты и безопасности глобальной сети и ее пользователей, это направление приобретает актуальность и становится концентрированным отражением происходящей глобализации.

Исследование по развитию информационных отношений способствует формированию информационного законодательства, в том числе стран-участниц ЕАЭС, которые создают общую структуру обмена правовой и экономической информации. Установления механизма международного контроля за безопасностью цифровых процессов, становится приоритетным направлением развития информационно-коммуникационных технологий, интернет сетей, обеспечивая интеграционное взаимодействие государств и ряда стран в вопросах построения глобальной инфраструктуры.

Ключевые слова: Кибербезопасность, информационные отношения, информационное пространство, информационная инфраструктура, ЕС, ЕАЭС, стратегия, концепция, законодательство, экономика.

Introduction. The development of the information sphere requires the solution of general issues of information security, since the development of the Internet based on technologies of open standards of networks has turned into a developed international commercial infrastructure with extensive information exchange. The basic technology of the Internet structure is

becoming the main factor in the dissemination of information in the global information space. Cyberspace involves more and more new users and new network management capabilities, including the use of the "Internet of Things" systems, that is, the involvement of technically managed objects. Since the Internet web servers contain a variety of information and distribute information resources for the documents sought, the protection of content resources from malicious software becomes the main direction of the fight against cybercrime and ensures the cybersecurity of information relations in information storage and exchange systems.

The development of integration processes in the field of digital transformation of the EAEU member states sets certain tasks in the fight against cybercrime, threats in the information infrastructure are currently becoming relevant for the national and economic security of states. The overall coordination of states in the direction of the development and adoption of appropriate legal documents protecting state structures in the field of information relations, ensuring the security of economic, financial, social, political information resources and the consequences of cybercrime actions should be aimed at improving and interacting with common state security structures. Studying the experience of countries in the field of cybersecurity will help avoid the risks of losing its own information infrastructure and develop legal methods to prevent cybercrime.

Research materials and methods. The research materials were legislation and economic strategies in the field of information relations of a number of countries, including the European Union, Japan and the EAEU member countries in the field of information relations development.

The purpose of the work is a legal and economic analysis of interaction in the study of cybersecurity in information relations in some advanced countries, including the EAEU. An opportunity to assess the regulatory sphere and the current situation, identify gaps and develop recommendations for filling them. Assess the principles of data protection and their proportionality in matters of cybersecurity, taking into account the global crisis and the spread of COVID-19, to develop a number of proposals that can improve the work of the EAEU.

Information relations in the global information space depend on information resources, which are the basis for the exchange, storage and creation of information products. The protection of information products, including information databases, taking into account the global crisis phenomena, is becoming the main criterion for cyber security.

The methodological basis of the research was the use of general and general scientific methods: - the method of the empirical level, where facts

are collected, judgments are developed and theoretical generalizations are made; - the method of the theoretical level, where a systematic, integrated approach to statistical, economic, legal information is applied and a comparative analysis of legal and economic data is proposed.

Results. Cybersecurity of information relations in the 21st century has become a major component of supporting and ensuring the safety of data. The global community is currently concerned about the growth of cybercrime, and the lack of legal regulation of entire sectors of the economy, as well as national information security at the level of states and individual countries, may lead to the risk of losing information / digital sovereignty. Today information technologies are aimed at meeting the information needs of all users, including users of leading businesses using various information databases, electronic directories, financial, scientific and technical information and other electronic resources related to international, national, regional information systems (Semenov S.R., 2018: 55) . Information / digital sovereignty is one of the modern foundations of any state, which should be based on various information content and have a degree of national influence and support for the implementation of an independent information policy. A number of states are already actively promoting the ideas of cybersecurity and its institution, in particular:

European Union (EU). In 2013, at the level of the European Commission, the EU Cybersecurity Strategy is adopted, where in Part 1 it is recognized that Cybersecurity is necessary to integrate the social and political environment together, to support and exercise freedom through democratic institutions, with the possibility of promoting European values in the field of human rights and freedoms and citizen, but the values themselves must be protected from illegal actions (Cybersecurity Strategy of the European Union, 2013: 2). At the same time, clause 1.2 establishes the basic principles of Cybersecurity, such as - The core values of the EU should be applied both in physical and digital space (the same force of EU legal sources), protection of fundamental rights and freedoms (recognition and support of natural rights enshrined in legislation), open access for all subjects of law, democratic governance (participation of many stakeholders represented by the private sector), the presence of shared responsibility (formation of a legal model of responsibility). Accordingly, these principles create priority areas consisting of cyber resilience, cybercrime reduction, the formation of a common cybersecurity policy (including defense policy), the development of cybersecurity production capacities, and the development of a common EU vision on international cyberspace. When developing this strategy, the EU took the 2001 Budapest Declaration as a basis,

which approved a common vision of legal measures (computer-assisted privacy crimes, copyright infringements, etc.), with further harmonization of law, both nationally and at the international level (Convention on Cybercrime, 2021: 5-7). Separately, the scope of procedural law was designated under Article 14, with the possibility of conducting criminal investigations, judicial proceedings. Moments in the field of search and seizure of computer data, data collection in real time, jurisdiction are identified. In 2020, a new EU Cybersecurity Strategy is adopted, where part 2 outlines the key trends in the development of the industry, in particular: 1) technological sovereignty, sustainable politics, leadership; 2) strengthening technological capacity to prevent risks; 3) promotion of global cyberspace (The EU's Cybersecurity strategy for the digital decade, 2020: 1). Thus, the EU intentionally supports and promotes the idea of an open and secure cyber network space with the ability to attract international investment and promote European values (openness of data, freedom of information, freedom of communication, data security, etc.). The EU is a unified data security system, which is supported by the EU Directive 2016/1148, as a major element in the formation and implementation of cyber law in the national legislation of the participating countries in various areas of the economy (implementation and support of online trading with the conclusion of online contracts; banking infrastructure; development of a system of online search engines with multilingual support), building a CSIRT (computer security incident response team to detect risks, warnings, mutual assistance, cross-border data exchange, establish fines in this area, etc.) (Directive (EU) 2016/1148, 2016: 1). Accordingly, support for cybersecurity has been established in the national legislation of the EU member states. For example: the Republic of Poland has introduced its plan for the development of cybersecurity for 2017-2022, where part 4 indicates that secure cyberspace will provide the necessary potential for building the country's digital economy, while ensuring the necessary level of provision of digital services, both from private and public sectors (National framework of cybersecurity policy of the Republic of Poland for 2017-2022, 2017 : 4-5). In addition to general trends, the Czech Republic, in its Cybersecurity Strategy for 2015-2020, has taken a course towards research and scientific work in this area, strengthening educational policy from schools to universities, training government officials, especially paying attention to the training of prosecutors and judges (National cyber security strategy of the Czech Republic for the period from 2015 to 2020, 2015:5-10). An important component of EU cybersecurity is a supranational body - the EU Cybersecurity Agency (ENISA), which aims to promote

and develop the cybersecurity of the EU member states (starting with the construction of a single network, an integration gateway). At the same time, by the end of 2019, all EU countries had implemented cybersecurity at the national level in the format of strategies, concepts, programs or plans.

Japan: In 2000, the Law on the Formation of a Modern Information and Telecommunication Network Society was adopted, which establishes that Japan's society becomes networked, where legal entities are in a single data stream (Basic Act on the formation of an advanced information and telecommunications network society, 2000: 1-5). At the same time, the network society, in accordance with Article 3, gives its possibilities of open access to the Internet, to various technologies, which leads to the emergence of the creative development of the individual and the recognition of his rights of digital rights. In 2013, the first draft of the Cybersecurity Strategy (based on the results of the first conference in Japan on cybersecurity) is being developed, which leads to a rethinking of the process of information flows and information protection (private and public) (Cyberdefense report, 2020: 14). In 2014, the Law on Cybersecurity was adopted, indicating the importance of cyber threats to the information space, which, on the basis of Article 12, leads to the formation of a cybersecurity strategy plan for the country, and, on the basis of Article 24, to form a Strategic Cybersecurity Headquarters under the Cabinet of Ministers, which will allow developing standards and measures for state bodies, adopt functions and plans for intergovernmental cooperation. The Chief of Staff is the Chief Secretary of the Cabinet of Ministers. In 2015, as a product of previous decisions, the Cybersecurity Strategy was adopted, which, according to 4. established the basic security principles, such as the free flow of information (without censorship, political pressure, but with the protection of users' personal data), the rule of law (the ratio of national law to international law) , openness of sources, autonomy (formation of mechanisms that allow legal entities to independently develop legal relations within the information environment), cooperation (in this area) (Cybersecurity strategy, 2015: 1-12). The main goal of this Strategy is to build a safe society where every subject of law can feel safe. Consequently, the planning process (development, analysis and adoption of a three-year plan (2015-2018)) with a display of financial costs, the degree of implementation in the field of state bodies, etc., serves as a tool for implementing the Strategy. In 2018, a new Cybersecurity Strategy is adopted, where from the innovations it can be noted that there is no longer a distinction between cyberspace and real space (Cyberdefense report, 2020:15). Now there is only their synthesis - "mutually interacting subjects". The emphasis was also placed on new

threats in the field of cryptocurrency, the Internet of Things (data exchange between different devices), 5G, etc.

Eurasian Economic Union (EAEU). Information security, and in the future also cybersecurity, should become key trends in the development of information relations among the EAEU member states. It is necessary to distinguish between normative legal acts (NLA) at the level of the EAEU integration law and the national law of the participating countries. Integration law is a number of legal acts approved by the EAEU bodies. First of all, it is possible to single out Article 367 of the Customs Code of the EAEU, which indicates the legal protection of information data based on the legislation of the participating countries, including the authorized customs authorities (Treaty on the Customs Code of the Eurasian Economic Union, 2017: 983). But this article does not indicate the application of cybersecurity and the identification of possible risks in this area. Suggestion: to supplement this article - with the wording "including in the field of cyberspace", thus, the legal level of legal relations will expand. In 2016, a project was laid for the cryptographic protection of information resources and integration gateways, which can become practical elements of cybersecurity (On the implementation of a project for the joint development of specialized means of cryptographic protection of information of the Eurasian Economic Union, 2016: 1-20). Another NLA is the 2017 Decision of the Supreme Eurasian Economic Council on the development of the digital agenda until 2025, where Part 1 states that the EAEU member states independently develop policies in the field of information space (On the main directions for the implementation of the digital agenda of the Eurasian Economic Union until 2025, 2017: 3-5). Thus, there is only the establishment of trends and directions, without a specific program for the information or cybersecurity system. At the same time, the digital agenda itself should not contradict national legislation. National law is expressed in the following legal acts:

-Armenia. In 2017, the Concept of Information Security is adopted, which confirms the main directions of the country's information policy (Concept of Information Security and Information Policy of the Republic of Armenia, 2017: 1-5), and in 2020, the National Security Strategy of the country is adopted, where Part 7 establishes that information security is a key area of the future, while cybersecurity will serve as protection from possible cyberattacks and crimes in the digital field (National Security Strategy of the Republic of Armenia, 2020: 1-10). And the main challenges in this area are: the lack of specialized legislation, issues of critical infrastructure, a unified state policy, but in the future these challenges will be overcome.

-Belarus. In 2019, the Information Security Concept is adopted, which confirms the importance of cyber threats, including the emergence of cybercrimes in the Internet space (Information security concept of the Republic of Belarus, 2019: 1-5). Clause 61 recognizes under the cyber threat the failure of technical equipment, software failures, which may be caused by the illegal actions of certain groups of people. Accordingly, in order to ensure cyber security, it is necessary to create a national security system that would allow responding to modern challenges. The important areas of clause 65.66 confirm the provision of the national segment of the Internet as an important space for interaction between the public and private sectors.

-Kazakhstan. In 2017, the Cybersecurity Concept was approved, which forms a model of approaches to this area, including the development of a data monitoring system, a unified policy in the field of information resources, the display of legal principles (observance of human rights and freedoms, ensuring the legitimate interests of legal entities, personal security and etc.) (Kazakhstan Cyber Shield, 2017: 1-10). An important point of this concept is the idea of promoting "Cyberhygiene" (security rules in the electronic network, when working with information flows). In addition, in 2018, to strengthen the country's financial sector, a separate Cybersecurity Strategy for 2018-2022 was adopted, which should strengthen the banking sector with the formation of a national security system in the field of banking operations (On the approval of the Cybersecurity Strategy of the Financial Sector of the Republic of Kazakhstan for 2018-2022, 2018: 1-10).

-Kyrgyzstan. In 2019, the Cybersecurity Strategy for 2019-2023 was adopted, with the approval in part 5 of the profile directions for the development of state policy in the field of cybersecurity, in particular, the formation of a unified system of measures (strengthening the interaction of state bodies in the field of information; teaching computer / digital literacy among state employees; uniform state policy), organization of information infrastructure security (identification of problematic aspects of infrastructure, development of criteria for assessing critical infrastructure), creation of a threat prevention system, development and implementation of the institution of cybercrime into national legislation, creation of a protection system, etc. (Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023, 2019: 1-10). The issue of security of the country's critical infrastructure is being worked out, with the introduction of the rights and obligations of users into the legislation, the introduction of monitoring and security assessment, which will strengthen the current Cybersecurity Strategy (Semenov N.S., 2020: 190-192).

-Russia. In 2013, a draft Concept of the country's cybersecurity strategy is being developed, which identifies the main problems, such as causing damage to the rights of individuals, government agencies and legal entities; the presence of cyberattacks against information resources; cyber warfare (Concept of the Cybersecurity Strategy of the Russian Federation, 2013:2-6). At the same time, part 2 of this draft mentions that "Cybersecurity" is not yet separated from the concept of "information security", which is an existing gap in the legislation. Part 5 denotes the basic principle of cyber security: guaranteed constitutional human and civil rights in the field of working with information, maximum personal protection, constructive cooperation, balance of responsibility, etc. In the future, the Cybersecurity Strategy will be adopted, and the presented draft of 2013 can serve as a basis for it.

Discussion. Any document, regulatory legal acts approving the idea of cybersecurity should be based on national legislation, with the implementation of the information space, including interaction with information, forms of implementation and information infrastructure and the possibility of economic application. This direction is confirmed in international legislation, since cybersecurity has, first of all, cross-border coverage (two or more countries), expressed in the form of a regional segment (Asia, Europe, etc.), and secondly, in the form of a transcontinental segment (North and South America, etc.). Accordingly, each country, integration association has its own policy and vision. For example: the EU through building information relations and ensuring their protection in the cyber space, where it promotes its European values and rights in the global information space. There is a specialized supranational agency (ENISA) that deals with the cybersecurity of the entire EU, monitoring relevant actions in the field of legislation, information infrastructure, and technical means. Japan is giving impetus to the formation of a number of areas in the field of legislation, from the Laws on the formation of a modern information and telecommunication network society to Cybersecurity, and ending with three profile strategies, which indicates a high level of preparation of the society. The main feature was the creation of a ready-made model of an information and network society and state with specific legal principles, institutions and a security structure, where the differences between cyberspace and real space are becoming a thing of the past. There is a recognition of equal opportunities both in the physical and in the virtual worlds, with different legal relationships. Within the framework of integration law, the EAEU is still inferior to the EU, but at the level of national legislation, the experience of the EU and Japan is taken in

the field of informatization and building information infrastructure. From the general analysis of the development of cybersecurity, a number of proposals are relevant that can improve the work of the EAEU, including:

1. To form a separate area of cybersecurity on the basis of the Information Technology Department of the EAEU, which will harmonize the legislation of the participating countries, develop general recommendations at the national levels.

2. To develop a common strategy and plan for the cybersecurity of the EAEU, which will lead to the formation of a common vision on the problems and prospects.

3. Finalize national strategies and plans for cybersecurity of the EAEU member states.

4. Expand the capabilities of the EAEU integration gateway, as there is the experience of the Customs Union and its information infrastructure.

5. To create conditions for the promotion of national integration projects in the field of cybersecurity, data processing, electronic services, etc.

Conclusion. The unifying structure for both the EU, Japan and the EAEU is the provision of information / digital sovereignty, which plays an important role in the security of the country or any territorial association. The more successfully this sovereignty is protected, the more opportunities the states will have to advance their priority areas in the field of data security, both in the national information field and in the global space. The basis for this will be a strong information infrastructure, with its own scientific and resource base.

Information about authors:

Ganieva Tamara Imangalievna – doctor of law sciences, professor, department of theory and history and law, Kyrgyz National University named after J.Balasagyn; *ganieva1000@gmail.com – https://orcid.org/0000-0003-2930-8722*;

Semenov Nikolai Sergeevich – candidate of law sciences, acting associate professor of Department of jurisprudence and international law, International University of Kyrgyzstan; *frindland@mail.ru – https://orcid.org/0000-0001-5183-7482*;

Semenov Sergei Rudolfovich – candidate of economic sciences; acting associate professor of Department of international business, International University of Kyrgyzstan; *ssr2002@list.ru – https://orcid.org/0000-0001-7871-6541*.

REFERENCES:

Basic Act on the formation of an advanced information and telecommunications network society. Act № 144 of December 6, 2000. URL: *https://japan.kantei.go.jp/it/it_basiclaw/it_basiclaw.html#:~:text=Article%205.-,The%20formation%20of%20an%20advanced%20information%20and%20telecommunications%20network%20society,range%20of%20a%20high%2Dquality* (last visit 14.02.2021) (in Eng.).

Concept of Information Security and Information Policy of the Republic of Armenia. Approved by the Order of the President of the Republic of Armenia dated October 23, 2017 NK-146-A.URL: *http://igf.am/wp-content/uploads/2019/12/%D5%80%D5%80-%D5%8F%D5%A5%D5%B2%D5%A5%D5%AF%D5%A1%D5%BF%D5%BE%D5%A1%D5%AF%D5%A1%D5%B6-%D4%B1%D5%B6%D5%BE%D5%BF%D5%A1%D5%B6%D5%A3%D5%B8%D6%82%D5%A9%D5%B5%D5%A1%D5%B6-%D5%80%D5%A1%D5%B5%D5%A5%D6%81%D5%A1%D5%AF%D5%A1%D6%80%D5%A3_20171023.pdf* (last visit 14.02.2021) (in Russ.).

Concept of the Cybersecurity Strategy of the Russian Federation. Federation Council of the Federal Assembly of the Russian Federation. URL: *http://council.gov.ru/services/discussions/themes/38324/* (last visit 14.02.2021) (in Russ.).

Convention on Cybercrime (Budapest Convention). Adopted on 23 November 2001 in Budapest, Hungary. URL: *https://rm.coe.int/1680081580* (last visit 14.02.2021) (in Russ.).

Cyberdefense report. Japans National cyber security and defense posture. Policy and organizations. Zurich, September 2020. P.14,15. URL: *https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf* (last visit 14.02.2021) (in Eng.).

Cybersecurity Concept (Kazakhstan Cyber Shield). Approved by the Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407. URL: *https://tengrinews.kz/zakon/pravitelstvo-respubliki-kazahstan-premer-ministr-rk/hozyaystvennaya-deyatelnost/id-P1700000407/* (last visit 14.02.2021) (in Russ.).

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European commission. Brussels, 7.2.2013. URL:

Cybersecurity Strategy of the Kyrgyz Republic for 2019-2023 Adopted by the Resolution of the Government of the Kyrgyz Republic dated July 24, 2019 No. 369. URL: *http://cbd.minjust.gov.kg/act/view/ru-ru/15479* (last visit 14.02.2021) (in Russ.).

Cybersecurity strategy. The Government of Japan. September 4, 2015. URL: *https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Japan_2015_cs-strategy-en.pdf* (last visit 14.02.2021) (in Eng.).

Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level security of network and information systems across the Union. Eur-lex. URL: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC*(last visit 14.02.2021) (in Eng.).

https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (last visit 14.02.2021) (in Eng.).

Information security concept of the Republic of Belarus. Approved by the Resolution of the Security Council of the Republic of Belarus dated March 18, 2019 No. 1. *https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html* (last visit 14.02.2021) (in Russ.).

field of protection and security of the global network and its users; this area is gaining relevance and becomes a concentrated reflection of the ongoing globalization.

Research on the development of information relations contributes to the formation of information legislation, including the EAEU member states, which create a common structure for the exchange of legal and economic information. Establishing a mechanism for international control over the safety of digital processes is becoming a priority area for the development of information and communication technologies, Internet networks, ensuring the integration interaction of states and a number of countries in building a global infrastructure.

Key words: Cybersecurity, information relations, information space, information infrastructure, EU, EAEU, strategy, concept, legislation, economics.

Т.И. Ганиева[1], Н.С. Семенов[2]*, С.Р. Семенов[2]

[1]Ж. Баласағын атындағы Қырғыз ұлттық университеті,
Бішкек, Қырғызстан;
[2]Қырғыз Республикасының Халықаралық университеті,
Бішкек, Қырғызстан.
E-mail: *frindland@mail.ru*

ЖАҺАНДЫҚ ҚОҒАМНЫҢ АҚПАРАТТЫҚ ИНФРАҚҰРЫЛЫМЫ САЛАСЫНДАҒЫ АҚПАРАТТЫҚ ҚАТЫНАСТАРДЫҢ КИБЕРҚАУІПСІЗДІГІ

Аннотация. Мақалада Еуропалық Одақ (ЕО) елдерінің, Жапонияның және Еуразиялық экономикалық одақ (ЕАЭО) мемлекеттерінің заңнамасын талдай отырып, ақпараттық қатынастар саласындағы киберқауіпсіздік мәселелері қарастырылады. Әлемдегі ақпараттық қатынастар әртүрлі құқық субъектілерінің өзара әрекеттесуінің маңызды құрамдас бөліктерінің біріне айналады, онда қатынастарды іс жүзінде жүзеге асыру кезінде мәліметтер қауіпсіздігі саласында құқықтық мәселелер туындайды. Интернет кеңістігі түрінде көрсетілген ақпараттық орта ақпараттық инфрақұрылымға негізделген негізгі фактор болып табылады. Ақпараттық инфрақұрылымның қарқынды дамуы құқық саласындағы жаңа құқықтық нормалардың, институттардың, салалардың пайда болу процесіне серпін береді, бұл интеграциялық бірлестіктерге кіретін жекелеген елдердің заңна-

National cyber security strategy of the Czech Republic for the period from 2015 to 2020. URL: *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Czech%20Republic* (last visit 14.02.2021) (in Eng.).

National framework of cybersecurity policy of the Republic of Poland for 2017-2022. EU Agency for cybersecurity. URL: *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf/view* (last visit 14.02.2021) (in Eng.).

National Security Strategy of the Republic of Armenia 2020. URL: *https://mil.am/files/LIBRARY/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%8F%20%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%B D % D 0 % B 0 % D 0 % B B % D 1 % 8 C % D 0 % B D % D 0 % B E % D 0 % B 9 % 2 0 % D 0 % B 1 % D 0 % B 5 % D 0 % B 7 % D 0 % B E % D 0 % B F % D 0 % B 0 % D 1 % 8 1 % D 0 % B D % D 0 % B E % D 1 % 8 1 % D 1 % 8 2 % D 0 % B 8 % 2 0 % D 0 % A 0 % D 0 % B 5 % D 1 % 8 1 % D 0 % B F % D 1 % 8 3 % D 0 % B 1 % D 0 % BB%D0%B8%D0%BA%D0%B8%20%D0%90%D1%80%D0%BC%D0%B5%D0%BD%D0%B8%D1%8F%202020.pdf* (last visit 14.02.2021) (in Russ.).

On the approval of the Cybersecurity Strategy of the Financial Sector of the Republic of Kazakhstan for 2018-2022. Adopted by the Resolution of the Board of the National Bank of the Republic of Kazakhstan dated October 29, 2018 No. 281. URL: *https://cdb.kz/sistema/pravovaya-baza/ob-utverzhdenii-strategii-kiberbezopasnosti-finansovogo-sektora-respubliki-kazakhstan-na-2018-2022-gody/* (last visit 14.02.2021) (in Russ.).

On the implementation of a project for the joint development of specialized means of cryptographic protection of information of the Eurasian Economic Union. Approved by the Order of the Supreme Eurasian Economic Council dated December 26, 2016 No. 7. URL: *https://docs.eaeunion.org/docs/ru-ru/01413600/sco_11042017_7* (last visit 14.02.2021) (in Russ.).

On the main directions for the implementation of the digital agenda of the Eurasian Economic Union until 2025. Approved by the Decision of the Supreme Eurasian Economic Council dated October 11, 2017 No. 12. URL: *https://docs.eaeunion.org/docs/ru-ru/01415258/scd_10112017_12*.

Semenov N.S. Legal features of information security of the Kyrgyz Republic. In the collection: Russian entrepreneurs - philanthropists and patrons. Collection of materials of the III All-Russian Morozov readings. Orekhovo-Zuevo, 2020. Pp.187-192. (in Russ.).

Semenov S.R. Information infrastructure development and digital transformation. / Scientific and practical journal of the Almaty Academy of Economics and Statistics - “Statistics, accounting and audit”, No. 3 (70) 2018, pp. 50-56 (in Russ.).

The EU’s Cybersecurity strategy for the digital decade. Brussels, 16.12.2020. URL: *https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade* (last visit 14.02.2021) (in Eng.).

Treaty on the Customs Code of the Eurasian Economic Union. Adopted on April 11, 2017. URL: *https://docs.eaeunion.org/docs/ru-ru/01413569/itia_12042017* (last visit 14.02.2021) (in Russ.).

МАЗМҰНЫ

Т.И. Ганиева, Н.С. Семенов, С.Р. Семенов
ЖАһАНДЫҚ ҚОҒАМНЫҢ АҚПАРАТТЫҚ ИНФРАҚҰРЫЛЫМЫ САЛАСЫНДАҒЫ АҚПАРАТТЫҚ ҚАТЫНАСТАРДЫҢ КИБЕРҚАУІПСІЗДІГІ.....5

Е.С. Голенко, А.А. Исмаилова, А.С. Жумаханова
«GENE ONTOLOGY» БАЗАСЫН ЖӘНЕ МАШИНАЛЫҚ ОҚЫТУ ҮЛГІЛЕРІН ПАЙДАЛАНА ОТЫРЫП АҚУЫЗ ФУНКЦИЯЛАРЫН БОЛЖАУ.....19

Р.Н. Молдашева, А.А. Исмаилова, А.К. Жамангара, А.М. Задағали
СУ ЭКОЖҮЙЕЛЕРІН ЗЕРТТЕУДІҢ АҚПАРАТТЫҚ ТАЛДАУ ЖҮЙЕСІН ӘЗІРЛЕУ.....39

А.А. Мырзатай, Л.Г. Рзаева, Г. Абитова, М.А. Жакенов
ОҚИҒАЛАРДЫ БОЛЖАУ ЖҮЙЕЛЕРІНІҢ КІРІСТЕРІН ЖҮЙЕЛЕУ ҮШІН LAN МОНИТОРИНГ ЖҮЙЕСІН ЕНГІЗУ ЖӘНЕ ПАЙДАЛАНУ.....54

Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова
ГАНТ ДИАГРАММАСЫН ҚҰРУДЫҢ АҚПАРАТТЫҚ ЖҮЙЕСІ.....64

Қ.Т. Қырғызбай, Е.Х. Какимжанов, Ж.М. Сагинтаев
ГАЖ-ТЕХНОЛОГИЯЛАРЫ НЕГІЗІНДЕ АЛМАТЫ ОБЛЫСЫН АГРОКЛИМАТТЫҚ АУДАНДАСТЫРУ.....76

А.А. Мухитова, А.С. Еримбетова, В.Б. Барахнин, Э.Н. Дайырбаева, А. Адалбек
РЕЛЯЦИЯЛЫҚ ЖӘНЕ УАҚЫТҚА ТӘУЕЛДІ XML-ДЕРЕКТЕР ҚОРЫНДАҒЫ XML-ДЕРЕКТЕРДІ ӨҢДЕУДІҢ ЗАМАНАУИ ӘДІСТЕРІ....92

Б.Б. Оразбаев, Ж.Ж. Молдашева, В.И. Гончаров, К.Н. Оразбаева
МАГИСТРАЛДЫ ҚҰБЫРЛАРМЕН МҰНАЙ ТАСМАЛДАУДЫ ДИАГНОСТИКАЛАУ ЖӘНЕ БАСҚАРУ ЖҮЙЕЛЕРІ.....112

Б.Б. Тастемір
ЭЛЕКТРОНДЫҚ ПОШТА СПАМДЫ СҮЗГІЛЕУГЕ АРНАЛҒАН RANDOM FORESTS МАШИНАЛЫҚ ОҚЫТУ ӘДІСІ.....130

А. Урынбасарова, Д. Урынбасарова, Э. Ал-Хуссам
ҚАЗАҚ ТІЛІНІҢ ЛАТЫН ГРАФИКАСЫНА АРНАЛҒАН ВЕБ-САЙТ.....142

Э.Э. Эльдарова, В.В. Старовойтов, К.Т. Искаков
БҰРМАЛҒАН КОНТРАСТТЫ ЦИФРЛЫҚ БЕЙНЕНІҢ ВИЗУАЛДЫ САПАСЫН ЖАҚСАРТУ.....153

СОДЕРЖАНИЕ

Т.И. Ганиева, Н.С. Семенов, С.Р. Семенов
КИБЕРБЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГЛОБАЛЬНОГО ОБЩЕСТВА.....5

Е.С. Голенко, А.А. Исмаилова, А.С. Жумаханова
ПРЕДСКАЗАНИЕ ФУНКЦИЙ БЕЛКОВ ПРИ ПОМОЩИ БАЗЫ ДАННЫХ «GENE ONTOLOGY» И МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ.....19

Р.Н. Молдашева, А.А. Исмаилова, А.К. Жамангара, А.М. Задағали
К РАЗРАБОТКЕ ИНФОРМАЦИОННОЙ АНАЛИТИЧЕСКОЙ СИСТЕМЫ ИССЛЕДОВАНИЯ ВОДНЫХ ЭКОСИСТЕМ.....39

А.А. Мырзатай, Л.Г. Рзаева, Г. Абитова, М.А. Жакенов
ВНЕДРЕНИЕ И ИСПОЛЬЗОВАНИЕ СИСТЕМ МОНИТОРИНГА ЛВС ДЛЯ СИСТЕМАТИЗИРОВАНИЯ ВХОДНЫХ ДАННЫХ СИСТЕМ ПРОГНОЗИРОВАНИЯ ИНЦИДЕНТОВ.....54

Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова
ИНФОРМАЦИОННАЯ СИСТЕМА ПОСТРОЕНИЯ ДИАГРАММЫ ГАНТА.....64

Қ.Т. Қырғызбай, Е.Х. Какимжанов, Ж.М. Сагинтаев
АГРОКЛИМАТИЧЕСКОЕ РАЙОНИРОВАНИЕ АЛМАТИНСКОЙ ОБЛАСТИ С ПРИМЕНЕНИЕМ ГИС-ТЕХНОЛОГИЙ.....76

А.А. Мухитова, А.С. Еримбетова, В.Б. Барахнин, Э.Н. Дайырбаева, А. Адалбек
СОВРЕМЕННЫЕ МЕТОДЫ ОБРАБОТКИ XML-ДАННЫХ В РЕЛЯЦИОННЫХ И ВРЕМЕННЫХ XML-БАЗАХ ДАННЫХ.....92

Б.Б. Оразбаев, Ж.Ж. Молдашева, В.И. Гончаров, К.Н. Оразбаева
ДИАГНОСТИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ТРАНСПОРТИРОВКИ НЕФТИ ПО МАГИСТРАЛЬНЫМ ТРУБОПРВОДАМ.....112

Б.Б. Тастемир
МЕТОД МАШИННОГО ОБУЧЕНИЯ RANDOM FORESTS ДЛЯ ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНОЙ ПОЧТЫ.....130

А. Урынбасарова, Д. Урынбасарова, Э. Ал-Хуссам
ВЕБ-САЙТ ЛАТИНСКОЙ ГРАФИКИ КАЗАХСКОГО ЯЗЫКА.....142

Э.Э. Эльдарова, В.В. Старовойтов, К.Т. Искаков
УЛУЧШЕНИЕ ВИЗУАЛЬНОГО КАЧЕСТВА КОНТРАСТНО ИСКАЖЕННЫХ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ.....153

CONTENTS

T.I. Ganieva, N.S. Semenov, S.R. Semenov
CYBERSECURITY OF INFORMATION RELATIONS IN THE FIELD OF INFORMATION INFRASTRUCTURE OF A GLOBAL SOCIETY.....5

Y.S. Golenko, A.A. Ismailova, A.S. Zhumakhanova
PREDICTING PROTEIN FUNCTIONS USING THE «GENE ONTOLOGY» DATABASE AND MACHINE LEARNING MODELS.....19

R.M. Moldasheva, A.A. Ismailova, A.K. Zhamangara, A.M. Zadagali
ABOUT DEVELOPMENT OF AN INFORMATION ANALYTICAL SYSTEM FOR THE STUDY OF AQUATIC ECOSYSTEMS.....39

A.A. Myrzatay, L.G. Rzayeva, G. Abitova, M.A. Zhakenov
THE IMPLEMENTATION AND THE USE OF THE LAN MONITORING SYSTEMS FOR SYSTEMATISATION OF THE INPUT DATA OF THE INCIDENT FORECASTING SYSTEMS.....54

Zh.S. Ixebayeva, K. Jetpisov, Zh.M. Muratova
INFORMATION SYSTEM FOR CONSTRUCTING GANTT CHARTS.....64

K.T. Kyrgyzbay, E.Kh. Kakimzhanov, Jay Sagin
AGRO-CLIMATIC ZONING OF ALMATY REGION USING GIS TECHNOLOGIES.....76

A.A. Mukhitova, A.S. Yerimbetova, V.B. Barakhnin, E. Daiyrbayeva, A. Adalbek
MODERN METHODS OF PROCESSING XML DATA IN RELATIONAL AND TEMPORARY XML DATABASES.....92

B.B. Orazbayev, Zh.Zh. Moldasheva, B.I. Goncharov, K.N. Orazbayeva
DIAGNOSTICS AND SYSTEMS OF OIL TRANSPORTATION THROUGH MAIN PIPELINES.....112

B.B. Tastemir
RANDOM FORESTS MACHINE LEARNING TECHNIQUE FOR EMAIL SPAM FILTERING.....130

A. Urynbassarova, D. Urynbassarova, E. Al-Hussam
WEBSITE FOR THE LATIN SCRIPT OF THE KAZAKH LANGUAGE.....142

E.E. Eldarova, V.V. Starovoytov, K.T. Iskakov
IMPROVED VISUAL QUALITY OF CONTRAST DISTORTED DIGITAL IMAGES.....153

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д. Жадыранова*

Подписано в печать 29.06.2022.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
9,0 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19