Современная наука и инновации.
2024. № 1 (45). С. 129-135.
Modern Science and Innovations.
2024; 1 (45):129-135.

*ПОЛИТИЧЕСКИЕ НАУКИ /
POLITICAL SCIENCE*

Научная статья / Original article

УДК 327
https://doi.org/10.37493/2307-910X.2024.1.15

Александр Иванович Бедаев
[Alexander I. Bedaev][1*],
Анзор Муаедович Ногмов
[Anzor M. Nogmov][2]

Информационные угрозы и международная информационная безопасность в работе ООН и ШОС

Information threats and international information security in the work of the United Nations and the OSCE

[1, 2]Астраханский государственный университет им. В.Н. Татищева, г. Астрахань, Россия /
Astrakhan State University named after V.N. Tatishchev, Astrakhan, Russia

****Автор, ответственный за переписку: Александр Иванович Бедаев, sascha.bolgow2012@yandex.ru/***
Corresponding author: Alexander I. Bedaev, sascha.bolgow2012@yandex.ru

Аннотация. *Целью настоящей статьи является сравнительный анализ работы, осуществляющейся ведущими странами в ООН и ШОС по вопросам международной информационной безопасности (МИБ). Деятельность ООН в сфере МИБ раскрывается в рабочих форматах ГПЭ и РГОС. Авторы показывают, что, российская сторона переходит от цели установления международного режима нераспространения информационного оружия к созданию международного режима неприменения информационного оружия на критически важные инфраструктуры. В статье отмечается, что западный подход эволюционировал от признания отсутствия необходимости создания дополнительных норм к нормам международного права и необходимости разработки международного универсального, юридически обязывающего документа к прямо противоположным задачам. На основе выделенных направлений сравнения работы ООН и ШОС авторы приходят к выводу, что в отличии от ООН, в ШОС проблема МИБ решается оперативно и последовательно через несколько форм взаимодействия (не менее четырёх): подписание международных документов, создание и развитие региональных институтов борьбы с киберугрозами и т.д. На уровне ООН работа происходит лишь по двум направлениям, что требует совершенствования и расширения данных направлений.*

Ключевые слова: информационные угрозы, кибертерроризм, международная информационная безопасность (МИБ), ООН, ШОС, Группа правительственных экспертов (ГПЭ), Рабочая группа открытого состава (РГОС), Региональная антитеррористическая структура (РАТС), Специальная рабочая группа (СРГ)

Для цитирования: *Бедаев А. И., Ногмов А. М. Информационные угрозы и международная информационная безопасность в работе ООН и ШОС // Современная наука и инновации. 2024. № 1 (45). С.* 129-135. *https://doi.org/10.37493/2307-910X.2024.1.15*

Abstract. *The purpose of this article is to comparatively analyze the work carried out by the leading countries in the UN and the SCO on international information security (IIS). The UN activities in the sphere of IIoS are disclosed in the working formats of the GGE and the OEWG. The authors show that the Russian side is moving from the goal of establishing an international regime of non-proliferation of information weapons to the creation of an international regime of non-use of information weapons on critical infrastructures. The article notes that the Western approach has evolved from recognizing that there is no need to create additional norms to the norms of international law and the need to develop an international*

universal, legally binding instrument to the exact opposite objectives. Based on the highlighted areas of comparison between the UN and the SCO, the authors conclude that, unlike the UN, the SCO addresses the problem of cyber threats promptly and consistently through several forms of interaction (at least four): signing international documents, creating and developing regional institutions to combat cyber threats, etc. At the UN level, work is carried out only in two areas, which requires improvement and expansion of these areas.

Keywords: information threats, cyberterrorism, international information security (IIS), UN, SCO, Group of Governmental Experts (GGE), Open-Ended Working Group (OEWG), Regional Anti-Terrorism Structure (RATS), Ad Hoc Working Group (AWG)

For citation: *Budaev AI, Naumov AM. Information threats and international information security in the work of the United Nations and the SCO. Modern Science and Innovations. 2024;1(45):129-135. https://doi.org/10.37493/2307-910X.2024.1.15*

Introduction. The problem of information threats has become firmly established in modern political and scientific discourse. Numerous research works, as a rule, include a section devoted to modern information threats. Quite often, the concept of "information threat" or "cyber threat" is identified with the concept of "threat to international information security" (IIS). If from the entire scope of these concepts we exclude the spatial aspect as a mandatory one, from the position of formal logic, indeed, one could agree to recognize this identity. Meanwhile, based on the international practice of their application, these concepts should still be separated, even without taking into account the spatial component.

In 1998, for the first time, the work of the UN General Assembly, on the initiative of Russia, included the issue of developing a document regulating the activities of states in the information sphere. According to the draft resolution developed, UN member countries were required to inform the UN Secretary-General about their own vision of the problem of international information security, the corresponding conceptual apparatus and about draft international legal regimes ensuring international security in the field of information and computer technologies (ICT) [7, c . 257-258]. The Russian initiative was not approved by the international community at that time. Meanwhile, it was then that issues of international information security were first proposed for international discussion. A peculiarity of Russian initiatives regarding international security issues is that they give them the character of military threats, which the United States opposed, classifying information security issues as cybercrime (cyber espionage, creation and distribution of viruses, etc.). Despite this, a Group of Governmental Experts (GGE) was created to consider cybersecurity issues at the UN. Five UN GGEs functioned with the participation and initiative of Russia: 2004-2005, 2009-2010, 2012-2013, 2014-2015, 2016-2017. In 2019-2021 The work of the sixth GGE was carried out without the participation of Russia, because Russia, disappointed with the work of the previous GGE, initiated the creation of the UN Open-Ended Working Group (OEWG) in 2018. During the work of the GGE, a number of priority issues were discussed. Firstly, it was necessary to answer the question about the advisability of developing a unified conceptual apparatus in relation to information threats. The difficulty here was that the Russian side understood information threats more broadly, including in their list the psychological impact of information on users of cyber systems, the influence of propaganda, unreliability of information, etc. The United States insisted on exclusively technological threats to information systems. At the same time, if you introduce the concept of "information weapon," objective difficulties arise with its definition, since a computer, in the literal sense, is not a weapon, just like spyware. Due to the vagueness of the conceptual apparatus, it becomes unclear what measures a state that has been subjected to cyber aggression can take and how the international community should respond to this. Another topic for discussion was the recognition of the possibility of applying already functioning international law to the information sphere and the need to create a corresponding unified, legally binding document regulating the rules of behavior of states in the field of information technology. Russia insists on such a need, but encounters objections from counterparties who believe that the low threshold for entry into the infosphere and the extremely rapid pace of its development make it impossible to effectively monitor the implementation of such a document, if adopted. According to the Russian side, a single document, binding on everyone, could

become key in creating a regime for the non-proliferation of information weapons. The goal of creating such a regime was set by Russia until 2013. Based on the results of the work of the GGE in 2014-2015. 11 norms of responsible behavior of states in cyberspace were adopted, however, without recognizing their legal force [7, p. 357-374].

Thus, compliance with these 11 norms is only voluntary and not mandatory. At the same time, their adoption should be recognized as a certain positive point, since before this the United States opposed the adoption of additional international documents of a restrictive nature to the already existing norms of international law. At the same time, the procedure for implementing the adopted standards remained not fully defined. Establishing the procedure for their transfer from the theoretical to the practical plane was entrusted to the UN GGE, which worked in 2016-2017, however, due to the mutually exclusive goals of the leading international players - Russia and the United States - it was not possible to draw up a consensus report then. The Russian side sought, using the international security architecture built during the Cold War (and based on the position of military parity of the parties), to create conditions for preventing a possible conflict in the ICT sector. At the same time, Western countries, taking into account the changed international situation (including a critical assessment of the military power of modern Russia), sought to create a regulatory framework for the implementation of cyber operations in the future. If we talk about the effectiveness of the work of the UN GGE, we can note the increased interest of international players in this problem. Thus, more than 110 states co-sponsored the Russian resolution in the UN General Assembly on international security issues in 2006-2017. and more than 70 states sent their vision of solving these problems to the UN Secretary General [12, p. 561-562]. Finally, the number of participants in the work of the GGE has increased significantly - from 15 in 2004-2005. up to 25 in 2016-2017 [2, p. 53-71]. One of the problems that prevents unambiguous support for both the Russian and American positions is the fact that the discussion of international security issues is initially conducted in the 1st UN Committee, which is responsible for international military security issues. This means that cyber threats that do not reach a critical level to be classified as military threats are not considered in this Committee, nor are they considered in other UN committees. Thus, a fairly significant amount of issues related to the problems of international information security are completely beyond the sight of the UN member countries.

In 2019-2021 within the UN, parallel work was carried out by the GGE (without the participation of Russia) and the OEWG (on the initiative and with the participation of Russia). As a result of the work done, on December 6, 2021, a joint Russian-American consensus draft resolution of the UN General Assembly was adopted on the possibility of developing a single, legally binding international document - “Achievements in the field of information and telecommunications in the context of international security and promoting responsible behavior of states in the use of ICT " [8]. According to Russian experts, this project should be considered a breakthrough, since its adoption will make it possible in the future to work on the development of specific norms regulating the activities of states in the information space, taking into account their legally binding nature. At the same time, as noted by S.A. Sebekin, judging by the amendments in 2021 to the “Fundamentals of the state policy of the Russian Federation in the field of international information security for the period until 2020” [7, p. 83-89] Russia changed the goals of its own work at the UN [10]. As the scientist notes, in the 2013 edition, this document saw the creation of a regime of non-proliferation of information weapons as a possible goal of participation in the UN GGE, however, in the edition dated April 12, 2021, there is no longer such a goal [10]. It was replaced by the desire to achieve the creation of an international regime of non-use of information weapons on critical infrastructure [10]. For a number of reasons, in terms of implementation, this approach to international information security looks more realistic than the first. The Russian side planned to discuss specific agreements based on the results of the next OEWG (operation period: 2021-2025). In July 2023, within the framework of the OEWG, an agreement was reached to create a global intergovernmental registry of contact points for the exchange of information on computer attacks/incidents [4]. As a general goal, the current OEWG sees preventing the outbreak of conflicts in the information sphere between states, and if they arise, ensuring their peaceful resolution [4].

Another international organization whose activities, among other things, are aimed at ensuring international security is the Shanghai Cooperation Organization (SCO). With the development of information technologies and threats, the focus of this organization began to cover, along with traditional security threats, threats caused by the rapid development of information technologies. At the same time, there are a number of differences in the specifics of countering information threats characteristic of the SCO. Thus, if at the UN, under the influence of Western players, cyber threats are understood exclusively as threats to computer systems, the SCO countries understand them as threats to individuals, society and the state, including information terrorism, extremist activities, the spread of terrorist and separatist ideology, etc.

The smaller composition of the organization's participants (compared to the UN) and a common understanding of the essence of information threats allowed the participating countries to achieve certain successes in creating an information security system. Note that here it is quite possible to talk about the entire system of international information security, since the organization's activities include a number of relevant areas: the development of international documents, the creation of an institutional framework to ensure compliance with established international legal norms, conducting exercises to combat cyber terrorism and cooperation with international organizations (for example, the UN) on international information security issues.

Within the first direction (development of international documents), the following successes of the SCO should be noted: in 2006, at the 6th summit of the SCO countries, the "Statement of the Heads of State of the Shanghai Cooperation Organization on International Information Security" was signed, which decided to create a group of government experts (GGE) SCO on international security issues [7, p. 625-626]; in 2009, as part of the 9th SCO summit, the participating countries signed the "Agreement between the governments of the SCO member states on cooperation in the field of ensuring international information security", which recorded the definitions of specific threats in the field of international information security, main directions, principles, forms and mechanisms cooperation in this area [Ibid., p. 627-635]; in 2015, a budget was formed for the further work of the SCO in the field of information threats and the document "Rules of Conduct in the Field of Ensuring International Information Security" was prepared [Ibid., p. 231-236]. In addition, in 2015, within the SCO, the following were adopted: "Program of cooperation between SCO member states in the fight against terrorism, separatism and extremism for 2016-2018." dated July 10, 2015 and "SCO Development Strategy until 2025" dated July 10, 2015 [3, p. 188]; in 2017, at the 17th summit of the SCO countries, the question was raised about the need to create a universal set of norms and rules for the behavior of states in the infosphere; in 2020, at the 20th summit of the SCO countries, the following documents were adopted: "Statement of the Council of Heads of State of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security" [6] and "Statement of the Council of Heads of State of the Shanghai Cooperation Organization on countering the spread of terrorist, separatist and extremist ideology, including on the Internet" [5]; In 2021, a document was developed (as part of the work of the SCO Group of Government Experts) "Plan for interaction of SCO member states on issues of ensuring international information security for 2022-2023" [1]. In addition, there are bilateral agreements between the SCO member countries to ensure international security.

Within the framework of the second direction (creating an institutional framework to ensure compliance with established international legal norms), the following SCO structures should be noted: in 2004, the Regional Anti-Terrorist Structure (RATS) was created (the main tasks of this structure are the exchange of information and coordination of actions in the course of countering extremist activities, transnational crime and illicit drug trafficking); in 2006, the SCO Group of Governmental Experts (GGE) on international security was created (tasks of the structure: developing common approaches at the intercountry level to countering threats of international security); in 2006, a Special Working Group (SWG) was created on modern information and telecommunication technologies of the SCO member states (tasks of the structure: development of intercountry cooperation projects in the field of ICT, exchange of relevant information, ensuring information

security and equality of member countries in the field of information technology; active work has been carried out since 2013).

As part of the third area, a number of exercises conducted by SCO member countries can be noted: in 2015, 2017 and 2019. In Xiamen (China), joint exercises of the participating countries to combat cyber terrorism were held [14; eleven; 13]; in 2023, a joint anti-terrorism exercise was held in New Delhi (India) "... to suppress the use of the Internet for terrorist, separatist and extremist purposes" [9].

Within the framework of the fourth direction (cooperation between international organizations on international security issues), it is worth noting some initiatives emanating from the SCO countries to work at UN sites: in 2011, the SCO member countries sent a document to the 66th UN General Assembly for consideration: "Rules of conduct in field of international information security" [7, p. 227-231]; in 2015, the SCO member countries sent an updated document to the 69th UN General Assembly for consideration: "Rules of conduct in the field of ensuring international information security (IIS)" [Ibid., p. 231-236].

Both documents presented at the UN by the SCO countries aroused great interest in the international community and contributed to the organization's work on issues of ensuring international security. Even the signing of the "Agreement between the governments of the SCO member states on cooperation in the field of ensuring international information security" in 2009 played a positive role in the work of the UN, as it became, in a way, an incentive for further work of the UN on international information security issues (remember, that the time interval between the work of the first and second GGE was quite long).

Conclusion. To summarize, it is necessary to emphasize that, unlike the UN, in the SCO, international security problems are resolved through several forms of interaction at once: signing international documents (at least 8), creating and developing regional institutions to combat cyber threats (RATS, GGE, SRG), conducting exercises on countering cyber terrorism and interaction with the UN (in 2015, 2017, 2019 and 2023). At the UN level, work takes place in only two directions - the creation of a documentary base to ensure international security (the work of the GGE and OEWG is only temporary) and cooperation with international organizations (for example, with the SCO). At the same time, at the moment, the UN recognizes the possibility of developing an international universal, legally binding document in addition to the norms of international law. Nevertheless, the latest successes of the UN's work in the field of information security include the creation of a global intergovernmental register of contact points for the exchange of information on computer attacks/incidents. Recent successes in the work of the UN are associated with the parallel work of the GGE and the OEWG, however, a significant part of the issues related to ensuring international security remains outside the scope of the UN negotiating platform, since issues related to cyber threats are considered in the 1st UN Committee, which excludes absolute support countries of the Western or Russian side. At the same time, apparently, on Russia's side, one can observe a transition from the goal of establishing an international regime for the non-proliferation of information weapons to the creation of an international regime for the non-use of information weapons on critical infrastructure.

ЛИТЕРАТУРА

1. Ахмедов Т. Обеспечение информационной безопасности актуальная задача государств-участников ШОС // Национальное информационное агентство Узбекистана. 20.08.2022. [Электронный ресурс]. URL: https://uza.uz/ru/posts/obespechenie-informacionnoy-bezopasnosti-aktualnaya-zadacha-gosudarstv-uchastnikov-shos_400624 (дата обращения: 20.01.2024).
2. Бойко С. М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. 2016. № 8. С. 53–71.
3. Васильев Л. Е. Борьба с терроризмом на пространстве ШОС: монография. М.: ИДВ РАН, 2017. 216 с.
4. Выступление представителя Российской Федерации И. А.Тяжловой на шестой сессии Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025 по пункту повестки дня «Регулярный институциональный диалог» [Электронный ресурс]. URL: https://russiaun.ru/ru/news/1151223 (дата обращения: 20.01.2024).
5. Заявление Совета глав государств-членов Шанхайской организации сотрудничества о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети

Интернет (Москва, 10 ноября 2020 г.) // Посольство Китайской Народной Республики в Российской Федерации: официальный сайт. 10.11.2020. [Электронный ресурс]. URL: http://ru.china-embassy.gov.cn/rus/zgxw/202011/t20201110_2941249.htm (дата обращения: 20.01.2024).
6. Заявление Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Москва, 10 ноября 2020 г.) // Посольство Китайской Народной Республики в Российской Федерации: официальный сайт. 10.11.2020. [Электронный ресурс]. URL: http://ru.china-embassy.gov.cn/rus/zgxw/202011/t20201110_2941245.htm (дата обращения: 21.01.2024).
7. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. М.: Издательство «Аспект Пресс», 2019. 784 с.
8. Обращение заместителя Министра иностранных дел Российской Федерации О. В. Сыромолотова к участникам ежегодной международной конференции «Киберстабильность: подходы, перспективы, вызовы», Москва, 13-14 декабря 2021 года // Посольство Российской Федерации в Соединённом Королевстве Великобритании и Северной Ирландии. [Электронный ресурс]. URL: https://www.rus.rusemb.org.uk/article/643 (Дата обращения: 21.01.2024).
9. О проведении совместного антитеррористического учения по пресечению использования сети Интернет в террористических, сепаратистских и экстремистских целях // Региональная антитеррористическая структура Шанхайской организации сотрудничества [Электронный ресурс]. URL: https://ecrats.org/ru/press/news/7900/ (дата обращения: 21.01.2024).
10. Себекин С. А. Возможен ли режим контроля за распространением кибервооружений? Подходы России и США // Пути к миру и безопасности. 2021. № 2 (61). С. 139-152.
11. Страны ШОС провели учения по борьбе с кибертерроризмом // Северо-Восточный сайт [Электронный ресурс]. URL: https://russian.dbw.cn/system/2017/12/07/001241470.shtml (дата обращения: 21.01.2024).
12. Тикк Э. Контроль над кибероружием и устойчивость // Ежегодник СИПРИ. 2019. С. 561-562.
13. ШОС провела учения по борьбе с кибертерроризмом в Китае // Китайский информационный интернет-центр. 12-12-2019. [Электронный ресурс]. URL: http://russian.china.org.cn/china/txt/2019-12/12/content_75507226.htm (дата обращения: 21.01.2024).
14. Штабные киберучения стран ШОС по борьбе с терроризмом проходят в Китае // РИА Новости. 14.10.2015. [Электронный ресурс]. URL: https://ria.ru/20151014/1301603766.html (дата обращения: 21.01.2024).

REFERENCES

1. Akhmedov T. Ensuring information security is an urgent task of the SCO member states. National Information Agency of Uzbekistan. 20 August 2022. Available from: https://uza.uz/ru/posts/obespechenie-informacionnoy-bezopasnosti-aktualnaya-zadacha-gosudarstv-uchastnikov-shos_400624 [Accessed 20 January 2024]. (In Russ.).
2. Boyko SM. Group of UN government experts on achievements in the field of information and telecommunications in the context of international security: a look from the past to the future. International Affairs. 2016;8:53-71. (In Russ.).
3. Vasiliev LE. The fight against terrorism in the SCO space: monograph. M.: IFES RAS, 2017. 216 p. (In Russ.).
4. Speech by the representative of the Russian Federation IA Tyazhlova at the sixth session of the UN Open-ended Working Group on Security in the Use of ICTs and ICTs themselves 2021-2025 on the agenda item “Regular institutional dialogue”. Available from: https://russiaun.ru/ru/news/1151223 [Accessed 20 January 2024]. (In Russ.).
5. Statement of the Council of Heads of State of the Shanghai Cooperation Organization on countering the spread of terrorist, separatist and extremist ideology, including on the Internet (Moscow, November 10, 2020). Embassy of the People's Republic of China in the Russian Federation: official website. 10 November 2020. Available from: http://ru.china-embassy.gov.cn/rus/zgxw/202011/t20201110_2941249.htm [Accessed 20 January 2024]. (In Russ.).
6. Statement of the Council of Heads of State of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security (Moscow, November 10, 2020). Embassy of the People's Republic of China in the Russian Federation: official website. 10 November 2020. Available from: http://ru.china-embassy.gov.cn/rus/zgxw/202011/t20201110_2941245.htm [Accessed 21 January 2024]. (In Russ.).
7. International information security: Theory and practice: In three volumes. Volume 2: Collection of documents. Ed. by AV Krutskikh. M.: Aspect Press Publishing House, 2019. 784 p. (In Russ.).
8. Address by Deputy Minister of Foreign Affairs of the Russian Federation OV Syromolotov to the participants of the annual international conference “Cyberstability: approaches, prospects, challenges”, Moscow, December 13-14, 2021. Embassy of the Russian Federation in the United Kingdom of Great Britain and Northern Ireland. Available from: https://www.rus.rusemb.org.uk/article/643 [Accessed 21 January 2024]. (In Russ.).
9. On conducting a joint anti-terrorism exercise to suppress the use of the Internet for terrorist, separatist and extremist purposes // Regional Anti-terrorist Structure of the Shanghai Cooperation Organization. 15 December 2023. Available from: https://ecrats.org/ru/press/news/7900/ [Accessed 21 January 2024]. (In Russ.).
10. Sebekin SA. Is the regime of control over proliferation of cyber weapons feasible? The Russian and U.S. approaches? Approaches of Russia and the USA. Paths to peace and security. 2021;2(61):139-152. (In Russ.).
11. SCO countries conducted exercises to combat cyberterrorism. North-Eastern website. Available from: https://russian.dbw.cn/system/2017/12/07/001241470.shtml [Accessed 21 January 2024]. (In Russ.).
12. Tikk E. Cyber weapons control and sustainability. SIPRI Yearbook. 2019. P. 561-562. (In Russ.).

13. The SCO conducted exercises to combat cyberterrorism in China. Chinese Information Internet Center. 12 Decemver 2019. Available from: http://russian.china.org.cn/china/txt/2019-12/12/content_75507226.htm [Accessed 21 January 2024]. (In Russ.).
14. Staff cyber exercises of the SCO countries to combat terrorism are taking place in China. RIA Novosti. 10/14/2015. Available from: https://ria.ru/20151014/1301603766.html [Accessed 21 January 2024]. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Александр Иванович Бедаев – кандидат исторических наук, доцент кафедры востоковедения и политических наук, Астраханский государственный университет им. В.Н. Татищева, +79618160058, sascha.bolgow2012@yandex.ru

Анзор Муаедович Ногмов – кандидат политических наук, Астраханский государственный университет им. В.Н. Татищева, +79999865462, karlos07@list.ru

INFORMATION ABOUT THE AUTHORS

Alexander I. Bedaev – PhD in History, Associate Professor, Department of Oriental Studies and Political Science, Astrakhan State University named after V.N. Tatishchev, +79618160058, sascha.bolgow2012@yandex.ru

Anzor M. Nogmov – Cand. Sci. (Polit.), Astrakhan State University named after V.N. Tatishchev, +79999865462, karlos07@list.ru

Вклад авторов: все авторы внесли равный вклад в подготовку публикации.
Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.
Conflict of interest: the authors declare no conflicts of interests.

Статья поступила в редакцию: 22.01.2024;
одобрена после рецензирования: 19.02.2024;
принята к публикации: 10.03.2024.

The article was submitted: 22.01.2024;
approved after reviewing: 19.02.2024;
accepted for publication: 10.03.2024.