ЭКСПЕРТНОЕ МНЕНИЕ

ОСНОВНЫЕ ПОДХОДЫ РОССИЙСКОЙ ФЕДЕРАЦИИ К ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О. С. Макаров, В. А. Романовский

Белорусский институт стратегических исследований,
г. Минск, Республика Беларусь

Статья представляет собой рецензию на доклад экспертов Центра международной информационной безопасности МГИМО (У) МИД России «Международная информационная безопасность: подходы России». Отмечается, что в современных условиях информационная безопасность представляет собой отдельную сферу безопасности. Обращается внимание на ведущую роль Российской Федерации в инициировании и развитии переговорного процесса по проблематике международной информационной безопасности в рамках Организации Объединенных Наций. Дается указание на специфику российского и американского подходов: в то время как Вашингтон и союзники воспринимают информационное пространство как еще одну сферу ведения военных действий, для Российской Федерации и ее единомышленников неприемлемы любые попытки милитаризации информационного пространства и использования информационно-коммуникационных технологий в военно-политических целях. Большое внимание уделено важности создания юридически обязывающих норм для регулирования отношений в киберпространстве. Представлены некоторые подходы Республики Беларусь к обеспечению международной информационной безопасности, которые согласуются с основными положениями доклада. Отмечено, что Республика Беларусь придерживается собственных концептуальных взглядов на проблематику международной информационной безопасности и стремится к формированию целостной системы ее нормативного обеспечения. Особый акцент делается на необходимости принятия специального универсального международно-правового документа, который предусматривал бы критерии применения существующих норм международного права к использованию информационно-коммуникационных технологий и прямо указывал бы на необходимость разработки новых норм. Подчеркивается важность создания в структуре Организации Объединённых Наций инклюзивного механизма, который позволит государствам вести системные и тематически специализированные переговоры по вопросам обеспечения международной информационной безопасности. Отмечается, что стратегической целью таких переговоров должно являться содействие закреплению на международном уровне подхода, основанного на предотвращении межгосударственных конфликтов в глобальном информационном пространстве, недопущении его милитаризации и поощрении мирного использования информационно-коммуникационных технологий.

Ключевые слова: информационная безопасность; международная безопасность; Рабочая группа ООН открытого состава (РГОС ООН); международное право.

Образец цитирования: *Макаров О. С., Романовский В. А.* Основные подходы Российской Федерации к обеспечению международной информационной безопасности // Актуальные проблемы международных отношений и глобального развития : сб. науч. ст. Минск, 2022. Вып. 10. С. 8–17. https://doi.org/10.33581/2311-9470-2022-10-8-17

THE MAIN APPROACHES OF THE RUSSIAN FEDERATION TO ENSURING INTERNATIONAL INFORMATION SECURITY

O. Makarov, V. Romanovski

Belarusian Institute of Strategic Research, Minsk, Republic of Belarus

The article is a review of the report of the Center for International Information Security of the MGIMO University of the Russian Ministry of Foreign Affairs "International Information Security: Russian Approaches". Today, information security is a separate area of security. Attention is given to the leading role of the Russian Federation in the initiation and development of the negotiation process on the issues of international information security within the framework of the United Nations. Specifics of the Russian and American approaches is highlighted: while Washington and its allies perceive the information space as another sphere of military operations, any attempts to militarize the information space and use information and communication technologies for military-political purposes are unacceptable for the Russian Federation and it's like-minders. Particular attention is paid to the importance of creating legally binding norms for regulating relations in cyberspace. The article describes approaches of the Republic of Belarus to ensuring international information security, which are consistent with the main provisions of the report. Republic of Belarus adheres to its own conceptual views on the issues of international information security and strives to form an integral system of its normative support. Particular emphasis is placed on the need to adopt a universal international legal document that would provide criteria for applying existing norms of international law to the use of information and communication technologies and would directly indicate the need to develop new norms. There is a growing importance of creating an inclusive mechanism in the structure of the United Nations that will allow states to conduct systemic and thematically specialized negotiations on issues of ensuring international information security. The strategic goal of such negotiations should be prevention of interstate conflicts in the global information space, avoidance of its militarization and peaceful use of information and communication technologies.

Key words: information security; international security; OEWG UN; international law.

For citations: Makarov O. S., Romanovskij V. A. (2022). Osnovnye podhody Rossijskoj Federacii k obespecheniyu mezhdunarodnoj informacionnoj bezopasnosti [The main approaches of the Russian Federation to ensuring international information security]. In: *Actual problems of international relations and global development: collection of scientific papers*. Minsk. Vol. 10, pp. 8–17. https://doi.org/10.33581/2311-9470-2022-10-8-17

Введение. Развитие глобального информационного общества и процессов цифровизации повысили степень уязвимости общественных процессов от информационных воздействий [1, с. 11; 2, с. 50; 3; 4, с. 10; 5, с. 57; 6, с. 99]. Закономерной реакцией в международном сообществе стало концептуальное и нормативное выделение информационной безопасности в отдельную сферу безопасности [7, с. 73].

Выступая на VI Всебелорусском народном собрании, Президент Республики Беларусь А. Г. Лукашенко отметил, что «из всех рисков национальной безопасности безопасность информационная становится главной

болевой точкой»[1]. Действительно, формирование новых общественных укладов напрямую связано с развитием информационной сферы и способностью обеспечить ее защищенность на национальном и международном уровнях.

В условиях трансформации системы международных отношений и повышением конфликтного потенциала мировой политики все большую значимость приобретает глобальная дискуссия по проблемам обеспечения международной информационной безопасности (далее – МИБ) [8, с. 3] и созданию соответствующего международно-правового режима. Отсутствие консенсуса по данному вопросу между великими державами, особенно КНР, Российской Федерацией и США, осложняет переговорный процесс и сотрудничество в области МИБ. На этом фоне происходит усиление угроз МИБ со стороны не только негосударственных акторов, занимающихся киберпреступностью и пропагандой терроризма в информационном пространстве, но и ряда государств, проводящих милитаризацию киберпространства и использующих информационно-коммуникационные технологии (далее – ИКТ) в военно-политических целях.

Анализу этих процессов посвящён доклад экспертов Центра международной информационной безопасности МГИМО (У) МИД России «Международная информационная безопасность: подходы России», который составлен под руководством доктора исторических наук, специального представителя Президента России по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности МИД России А. В. Крутских.

Основная часть. Доклад состоит из введения, шести глав и заключения. Во введении и первой главе определяются и детализируются основные угрозы МИБ. Базируясь на утверждённых в апреле 2021 г. основах государственной политики Российской Федерации в области международной информационной безопасности, авторы справедливо отмечают наличие трех типов угроз – военно-политических, террористических и криминальных[2]. Подчёркивается, что, в отличие от США и их союзников, Россия отстаивает наличие не только технических, но и политико-идеологических угроз в сфере МИБ.

---

[1] Доклад Президента Беларуси на VI Всебелорусском народном собрании // Официальный Интернет-портал Президента Республики Беларусь [Электронный ресурс]. URL: https://president.gov.by/ru/events/shestoe-vsebelorusskoe-narodnoe-sobranie (дата обращения: 18.05.2022).

[2] Основы государственной политики Российской Федерации в области международной информационной безопасности: Утв. Ук. Президента Росс. Федерации, 12 апреля 2021 г., № 21 // Официальный сайт Совета Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 19.05.2022).

Вторая и третья главы посвящены анализу переговорного процесса по МИБ на площадке ООН. Красной нитью проходит мысль о том, что именно Российская Федерация выступала главным вдохновителем подобного глобального сотрудничества, сформулировав триаду угроз МИБ и инициировав создание Группы правительственных экспертов по МИБ (далее – ГПЭ) в 2001 г. и Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникации (далее – РГОС) в 2018 г. [9, с. 85]. Авторы подробно анализируют деятельность ГПЭ и, признавая её позитивные аспекты, выделяют тенденцию политизации Группы, что привело к непринятию итогового доклада ГПЭ первого и пятого созывов ввиду разногласий России и США.

Отмечается, что при поддержке государств, разделяющих позицию Москвы, России удалось продвинуть на уровне ГПЭ отдельные элементы собственного подхода к проблематике. В частности, применимость общепризнанных принципов международного права к использованию ИКТ и необходимость обоснования обвинений государств в противоправных деяниях в киберпространстве. Однако попытки США и их союзников «обосновать возможность применения отдельных международно-правовых норм, включая нормы международного гуманитарного права, к силовым действиям в информационном пространстве» и обойти стороной проблему атрибуции вызвали неприятие России.

Был дан старт новому этапу переговорного процесса по МИБ в рамках ООН – РГОС, который, по мнению авторов доклада, способствовал частичному преодолению межгосударственных разногласий по обеспечению МИБ и продвижению идеи о необходимости разрешения конфликтов в информационном пространстве мирным путём.

В докладе говорится о том, что «работа РГОС способствовала повышению доверия и взаимопонимания между государствами, однако раскол в позициях не был преодолен полностью, что показывают альтернативные проекты в области сотрудничества по МИБ, предлагаемые западными партнерами». Соответствующие подходы к МИБ, предлагаемые региональными организациями и рядом государств на глобальном, региональном и национальном уровнях, рассматриваются в четвертой главе.

Особенно выделяются инициативы ЕС и ее государств – членов, в частности, Франции, по развитию и углублению международного сотрудничества, направленные на выработку норм ответственного поведения государств в глобальном информационном пространстве – Парижский призыв к доверию и безопасности в киберпространстве [3] и Программа

[3] Парижский призыв к доверию и безопасности в киберпространстве: Париж, 12 ноября 2018 г. // Официальный сайт Парижского призыва к доверию и безопасности в киберпространстве [Электронный ресурс]. URL: https://pariscall.international/en/ (дата обращения: 19.05.2022).

действий по продвижению ответственного поведения государств в киберпространстве[4]. Рассматривая указанные инициативы в контексте стремления ЕС продемонстрировать свою нормативную силу, авторы подчеркивают, что «в отличие от РГОС ООН данные инициативы не подразумевают участия всех представителей международного сообщества и не являются официально признанными структурными единицами в системе ООН, что подрывает их репрезентативность и легитимность».

На основе изучения различных страновых подходов к проблеме МИБ сделан вывод, что США и их союзники по НАТО ориентированы на оборонительно-наступательную политику. В то же время позиция Китая в сфере международной информационной безопасности близка к российской, носит оборонительный характер и нацелена на защиту суверенитета и выработку юридически обязывающих международных норм.

В пятой главе описывается комплекс мер, предпринимаемых российской стороной для обеспечения МИБ. На глобальном уровне Москва продвигает универсальные, юридически обязывающие нормы ответственного поведения государств в информационном пространстве, борьбу с киберпреступностью и интернационализацию управления Интернетом под эгидой Международного союза электросвязи. Региональный и двусторонний уровни ориентированы на международное сотрудничество в области МИБ с государствами-единомышленниками. Эти приоритеты закреплены в докладе российских доктринальных документах по МИБ. К ним относятся Конституция Российской Федерации[5], Стратегия национальной безопасности Российской Федерации[6], Основы государственной политики Российской Федерации в области международной информационной безопасности [3] и Доктрина информационной безопасности Российской Федерации[7]. Авторы подчеркивают, что «документы стратегического плани-

[4] Программа действий по продвижению ответственного поведения государств в киберпространстве // Официальный сайт ООН [Электронный ресурс]. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://front.un-arm.org/wp-content/uploads/202010/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (дата обращения: 19.05.2022).

[5] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.): Утв. Ук. Президента Росс. Федерации, 3 июля 2020 г., № 445 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/ (дата обращения: 19.05.2022).

[6] Стратегия национальной безопасности Российской Федерации: Утв. Президентом Росс. Федерации, 2 июля 2021 г., № 400 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=602263723 (дата обращения: 18.05.2022).

[7] Доктрина информационной безопасности Российской Федерации: Утв. Ук. Президента Росс. Федерации, 5 декабря 2016 г., № 646 // Официальный сайт Совета Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/ security/information/document5/ (дата обращения: 19.05.2022).

рования страны и ее внешняя политика ставят в качестве ориентира формирование режима МИБ, причем именно РГОС как постоянно действующая институциональная открытая и инклюзивная структура на сегодняшний день является оптимальной площадкой для достижения внешнеполитических целей РФ на данном направлении».

В шестой главе предметом анализа является обсуждение применимости норм международного права к информационному пространству на площадке РГОС второго созыва с мандатом на 2021–2025 гг. В этом контексте авторы снова подчёркивают различие подходов России и НАТО к милитаризации киберпространства и отмечают, что, в то время как «Российская Федерация предлагает международному сообществу (особенно на уровне ООН) принять свод специальных правил поведения [в киберпространстве]… США и их союзники уже договариваются о правилах ведения кибервойны». В этой связи проект «Таллинского руководства 3.0» рассматривается авторами доклада в качестве инструмента легитимизации военного использования ИКТ. Авторы доклада делают особый акцент на том, что «Российская Федерация и ее партнеры выступают не только за предотвращение милитаризации киберпространства, но в принципе за запрет на применение кибероружия» и предлагают принять соответствующий юридически обязывающий комплекс мер.

Республика Беларусь руководствуется собственными концептуальными взглядами на проблематику МИБ и последовательно формирует целостную систему нормативного обеспечения информационной безопасности. Отказ от милитаризации или создания информационно-коммуникационных технологий, специально предназначенных для нанесения вреда информационным ресурсам, инфраструктуре и критически важным объектам третьих стран является одним из ключевых принципов, который Республика Беларусь продвигает на национальном, региональном и глобальном уровнях.

В современных условиях особую важность приобретает обеспечения безопасности критической инфраструктуры государства. Крайне важно на международно-правовом уровне согласовать запрет на проведение санкционированных государствами кибератак в отношении ее объектов. Необходимо строго придерживаться достигнутых межгосударственных договоренностей в сфере кибербезопасности и воздерживаться от использования механизмов санкционной политики в отношении данной сферы. Последствия возможных кибератак на объекты критической инфраструктуры государств, которые не обладают современными системами кибербезопасности, могут быть разрушительными для целых регионов.

В этом контексте необходимо отметить возросшую значимость обеспечения кибернетической безопасности критических объектов инфраструктуры системы здравоохранения и топливно-энергетического комп-

лекса [10, с. 1], в том числе генерирующих объектов низкоуглеродной энергетики – установок по использованию возобновляемых источников энергии, атомных электростанций, гидроэлектростанций, установок по использованию вторичных энергоресурсов, электростанций, функционирующие в режиме когенерации и оснащенных технологиями улавливания выбросов парниковых газов.

Распространение фальсифицированной, недостоверной или неполной информации, которая позиционируется как достоверная и исчерпывающая, может представлять угрозу общественной безопасности государства. Наличие такого рода информации, например, о неисправностях в работе АЭС, уже может представлять угрозу для международной безопасности в целом. Особенно опасными являются созданные с использованием технологий искусственного интеллекта синтезированные аудиовизуальные продукты, т.н. дипфейки, которые с растущей правдоподобностью демонстрируют то, чего никогда не было. В связи с этим необходимо скорейшее согласование перечня объектов, в частности, критической инфраструктуры государств, в отношении которых будет запрещено распространять недостоверную, фальсифицированную или неполную информацию.

Следует согласиться с точкой зрения, согласно которой важность МИБ в современном мире недооценена: отсутствует надлежащая институционализация, работа ведется в рамках групп, на площадках ООН, ОБСЕ и региональных объединений, зачастую дублируя отдельные вопросы либо противореча друг другу. Безусловно, широкая поддержка и мандат, зафиксированный в резолюции Генассамблеи ООН являются преимуществом РГОС. Однако формирующаяся конкурентная среда в скором времени потребует от РГОС более ощутимых результатов.

Вопрос о принципах правового обеспечения международной информационной безопасности – один из камней преткновения в межгосударственном диалоге по данной проблематике, в том числе на полях РГОС. Беларусь как представитель романо-германской правовой семьи придерживается подхода, согласно которому отношения, складывающиеся в информационной сфере, регулируются нормами, которые могут быть отнесены к отдельной отрасли права.

Не вызывает сомнений необходимость принятия специального универсального международно-правового документа, который предусматривал бы критерии применения существующих норм международного права к использованию ИКТ и прямо указывал бы на необходимость разработки новых норм. Очевидно, что в условиях отсутствия юридически обязательных норм регулирования отношений в информационной сфере в обозримом будущем представляется маловероятной перспектива создания механизма привлечения государств и негосударственных акторов к ответ-

ственности за злонамеренные кибернетические воздействия в отношении объектов критической инфраструктуры государств.

В структуре ООН важно сформировать инклюзивный механизм, который позволит государствам вести системные и тематически специализированные переговоры по всему спектру вопросов обеспечения МИБ. Стратегической целью таких переговоров должно являться содействие закреплению на международном уровне подхода, основанного на предотвращении межгосударственных конфликтов в глобальном информационном пространстве, недопущении его милитаризации и поощрении мирного использования ИКТ. При сохранении государственного контроля за нормотворческими процессами в сфере использования ИКТ, участие в переговорном процесс иных заинтересованных сторон позволит сформировать более инклюзивную архитектуру международной информационной безопасности.

Заключение. Активизация процессов цифровой трансформации открыла уникальные возможности для социального прогресса. Одновременно, цифровая среда породила новые вызовы и угрозы для национальной и международной безопасности, требующие адекватного реагирования.

В своем докладе эксперты Центра международной информационной безопасности МГИМО (У) МИД России «Международная информационная безопасность: подходы России» убедительно продемонстрировали, что проблема обеспечения МИБ сегодня является одним из важнейших вопросов глобального значения. Авторам успешно удалось всесторонне проанализировать подходы государств и межгосударственных объединений к сфере международной информационной безопасности с особым упором на позицию России, а также историю и перспективы переговоров по данной проблематике.

Важным достоинством доклада является точное указание на характер разногласий между Россией и ее единомышленниками, с одной стороны, и США и их союзниками, с другой. Вашингтон и НАТО воспринимают информационную сферу как очередной театр военных действий и желают закрепить своё доминирование, в то время как для России и её партнёров неприемлемы любые попытки милитаризации информационного пространства и использования информационно-коммуникационных технологий в военно-политических целях. Особое внимание уделено важности создания юридически обязывающих норм для регулирования отношений в киберпространстве.

Отметим, что ранее таких обобщающих докладов, в которых описаны российские подходы к тематике международной информационной безопасности, не существовало. Дать панорамную картину, особенно такого сложного и многогранного явления как МИБ – сложная задача. И авторы с ней блестяще справились.

Библиографические ссылки

1. *Арчаков В. Ю., Баньковский А. Л.* Зарубежный опыт применения «мягкой силы» в контексте обеспечения национальной безопасности Республики Беларусь // Журнал международного права и международных отношений. 2021. № 2 (97). С. 10–19.

2. *Прохорова Д. А.* Основные угрозы международной информационной безопасности на современном этапе // Информационные войны. 2022. № 1 (61). С. 50–54.

3. *Полякова Т. А., Стрельцов А. А.* Организационное и правовое обеспечение информационной безопасности. М.: Юрайт. 2016. 325 с.

4. *Евстафьев Д. Г.* Современное информационное общество и глобальная безопасность: диалектика взаимовлияния // Вестн. Моск. ун-та. Сер. 12, Политические науки. 2018. № 1. С. 7–25.

5. *Арчаков А. А., Баньковский А. Л., Коваленя А. А.* Обеспечение национальной безопасности в контексте тенденций развития современного мира // Беларуская думка. 2021. № 8. С. 54–60.

6. *Коваленя А. А.* Основы информационной безопасности // Беларуская думка. 2020. № 12. С. 99–100.

7. *Смирнов А. А.* Эволюция угроз информационной безопасности // Информационные войны. 2015. № 2 (34). С. 69–74.

8. *Арчаков А. А.* О теоретико-методологических подходах к обеспечению международной информационной безопасности // Журнал международного права и международных отношений. 2019. № 3-4 (90-91). С. 3–11.

9. *Ромашкина Н. П.* Международная деятельность по обеспечению информационной безопасности в XXI веке // Информационные войны. 2015. № 2 (34). С. 75–88.

10. *Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г.* Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2–10.

References

1. Archakov, V. Y., Bankovskiy A. L. (2021). Zarubezhnyi opyt primenenia “miagkoi sily” v kontekste obespechenia natsionalnoi bezopasnosti Respubliki Belarus [Foreign experience of using “soft power” in the context of ensuring the national security of the Republic of Belarus]. In: *Zhurnal mezhdunarodnogo prava i mezhdunarodnyh otnosheniy.* Vol. 97. Iss. 2. P. 10–19 (in Russ.).

2. Prohorova, D. A. (2022). Osnovnye ugrozy mezhdunarodnoi informatsionnoi bezopasnosti na sovremennom etape [The main threats to international information security at the present stage]. In: *Informatsionnye vojny.* Vol. 61. Iss. 1. P. 50–54 (in Russ.).

3. Poliakova, T. A., Streltsov, A. A. (2016). Orzanizatsionnoe i pravovoe obespechenie informatsionnoi bezopasnosti [Organizational and legal support of information security]. M: Yurait. 325 p. (in Russ.).

4. Evstafiev, D. G. (2018). Sovremennoe informatsionnoe obschestvo i globalnaia bezopasnost: dialektika vzaimovliania [Modern information society and global security: dialectics of mutual influence]. In: *Vestn. Mosk. un-ta.* Vol. 12. Politicheskie nauki. Iss. 1. P. 7–25 (in Russ.).

5. Archakov, A. A., Bankovskiy, A. L., Kovalenia, A. A. (2021). Obespechenie natsionalnoi bezopasnosti v kontekste tendentsyi razvitia sovremennogo mira [Ensuring national security in the context of development trends of the modern world]. In: *Belaruskaia dumka.* Vol. 8. P. 54–60 (in Russ.).

6. Kovalenia, A. A. (2020). Osnovy informatsionnoi bezopasnosti [Fundamentals of information security]. In: *Belaruskaia dumka.* Vol. 12. P. 99–100 (in Russ.).

7. Smirnov, A. A. (2015). Evoliutsia ugroz informatsionnoi bezopasnosti [Evolution of threats to information security]. In: *Informatsionnye vojny.* Vol. 34. Iss. 2. P. 69–74 (in Russ.).

8. Archakov, A. A. (2019). O teoretiko-metodologicheskih podhodah k obespecheniu mezhdunarodnoi informatsionnoi bezopasnosti [On theoretical and methodological approaches to ensuring international information security]. In: *Zhurnal mezhdunarodnogo prava i mezhdunarodnyh otnosheniy.* Vol. 90–91. Iss. 3–4. P. 3–11 (in Russ.).

9. Romashkina, N. P. (2015). Mezhdunarodnaia deiatelnost po obespecheniu informatsionnoi bezopasnosti v XXI veke [International activities to ensure information security in the XXI century]. In: *Informatsionnye vojny.* Vol. 34. Iss. 2. P. 75–88 (in Russ.).

10. Massel, L. V., Voropai, N. I., Senderov, S. M., Massel, A. G. (2016). Kiberbezopasnost kak odna iz strategicheskih ugroz energeticheskoi bezopasnosti Rossii [Cybersecurity as one of the strategic threats to the energy security of Russia]. In: *Voprosy kiberbezopasnosti*. Vol. 17. Iss. 4. P. 2–10 (in Russ.).

Статья поступила в редакцию 29.08.2022
Received by editorial board 29.08.2022

Авторы: Макаров Олег Сергеевич – доктор юридических наук, доцент, директор Белорусского института стратегических исследований; e-mail: makarov@bisr.by;

Романовский Виталий Анатольевич – главный советник Белорусского института стратегических исследований, соискатель кафедры международных отношений факультета международных отношений Белорусского государственного университета; e-mail: romanovskiy@bisr.by.

About authors: Makarov Oleg – Dr.Sc. in Law, Associate Professor, Director of the Belarusian Institute of Strategic Research; e-mail: makarov@bisr.by;

Romanovski Vitali – Senior Advisor of the Belarusian Institute for Strategic Studies, PhD candidate for the Department of International Relations, Faculty of International Relations, Belarusian State University; e-mail: romanovskiy@bisr.by.