ПАЛІТАЛОГІЯ

УДК 327(476+470)

***Игорь Михайлович Авласенко*[1]*, Карина Игоревна Ярмошук*[2]**
[1]*канд. ист. наук, доц., доц. каф. международных отношений Белорусского государственного университета*
[2]*канд. полит. наук, преподаватель каф. международных отношений Белорусского государственного университета*
***Ihar Aulasenka*[1]*, Karina Yarmoshuk*[2]**
[1]*Candidate of Historical Sciences, Associate Professor, Associate Professor of the Department of International Relations of Belarusian State University*
[2]*Candidate of Political Sciences, Lecturer of the Department of International Relations of Belarusian State University*
e-mail: [1]AvlasenkIM@bsu.by; [2]YarmoshukKI@bsu.by

КОНТУРЫ ЕВРАЗИЙСКОГО ПАРТНЕРСТВА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕСТО И РОЛЬ СОЮЗНОГО ГОСУДАРСТВА*

Раскрыты особенности формирования партнерства стран Большой Евразии в сфере информационной безопасности. На основе анализа документов Шанхайской организации сотрудничества и других организаций путем сопоставления с концептуальными документами стран Запада определена трактовка термина «международная информационная безопасность» в евразийском контексте, установлена ее взаимосвязь с особенностями системы международных отношений на континенте, выделены основные направления сотрудничества государств Евразии. Показаны место и роль Союзного государства в международном сотрудничестве по вопросам обеспечения информационной безопасности на Евразийском континенте.

Ключевые слова: *международная информационная безопасность, Шанхайская организация сотрудничества, Союзное государство, Большое Евразийское партнерство.*

Outlines of Eurasian Partnership in the Sphere of Information Security: Place and Role of the Union State

The article reveals the features of the formation of partnership of the countries of Greater Eurasia in the field of information security. The specifics of the interpretation of the term «international information security» in the Eurasian context is determined, based on the analysis of documents of the Shanghai Cooperation Organization and other structures by comparing them with conceptual documents of Western countries. Its connection with the features of the system of international relations on the continent is established, the main areas of cooperation of the Eurasian states are highlighted. The place and role of the Union State in international cooperation on issues of information security on the Eurasian continent are shown.

Key words: *international information security, Shanghai Cooperation Organization, Union State, Greater Eurasian Partnership.*

Введение

На фоне внешнеполитического разворота Минска и Москвы, а также актуализации идеи Большого евразийского партнерства у экспертов и дипломатов-практиков возник интерес к созданию обновленной системы безопасности на евразийском континенте: ряд материалов на эту тему опубликован на сайте Российского совета по международным делам [1; 2]. О намерении Республики Беларусь принять активное участие в ее формировании свидетельствует проведение Первой и Второй Минских конференций по евразийской безопасности осенью 2023 и 2024 гг. Однако особенности и потенциал партнерства на евразийском континенте по вопросам информационной безопасности в новых условиях изучены

**Статья подготовлена при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований в рамках НИР «Трансформация военно-политических, энергетических и социально-гуманитарных аспектов системы европейской безопасности: значение для Союзного государства» (№ госрегистрации 20240046 от 12.01.2024).*

недостаточно глубоко, пока слабо артикулирована роль Республики Беларусь и Союзного государства. Ранее отдельные работы, посвященные политическим и юридическим аспектам международной информационной безопасности, были затронуты в трудах Е. С. Зиновьевой, А. Н. Сытник, М. М. Базлуцкой, Н. О. Мороз [3–5].

В последнее время появились публикации, посвященные фактору искусственного интеллекта в региональном и глобальном измерениях информационной безопасности [6, с. 72–81].

Целью статьи является выявление роли и места Союзного государства в рамках формирующегося партнерства в сфере информационной безопасности на пространстве Большой Евразии. Актуальность данного исследования дополнительно обусловлена активизацией интеграционных процессов в рамках Союзного государства, подготовкой обновленной Концепции безопасности Союзного государства, а также утверждением Всебелорусским народным собранием новой редакции Концепции национальной безопасности в апреле 2024 г. [7].

Основными методами для достижения данной цели являются контент-анализ текста документов, метод сравнения, а также структурно-функциональный анализ международных институтов на евразийском пространстве, ответственных за обеспечение информационной безопасности. В качестве ключевых источников были выбраны нормативные правовые акты, которые дают представление в т. ч. и о политических приоритетах государств-участников. В их числе – Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г., Концепция информационной безопасности Союзного государства (утверждена Постановлением Высшего Государственного Совета Союзного государства Беларуси и России от 22.02.2023, № 1) [8–10].

Основная часть

В Концепции информационной безопасности Республики Беларусь, принятой в 2019 г., информационная безопасность трактуется как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве» [11], а международная информационная безопасность – как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве» [11]. Практически идентичные определения содержатся в нормативных правовых актах Союзного государства, Шанхайской организации сотрудничества [8; 10]. Однако исследователи обращают внимание на различные интерпретации понятия «информационная безопасность», на его технический и информационно-психологический аспекты [3, с. 37–38].

В концептуальных документах западных стран четкое определение данному понятию не дается, однако можно заметить, что в качестве основного термина там используется «кибербезопасность» («cybersecurity»). В публикациях и научных дебатах два термина нередко взаимозаменяются, однако хотелось бы обратить внимание на отличия в их трактовке.

Кибербезопасность рассматривается прежде всего как техническая защищенность от единичных атак, направленных на информационную инфраструктуру с помощью информационно-коммуникационных технологий (далее – ИКТ).

В частности, в Стратегии кибербезопасности ЕС, принятой в 2020 г., отмечается, что «для продвижения и защиты своего видения киберпространства на международном уровне Евросоюзу необходимо активизировать свое участие и проявить лидерство в международных процессах стандартизации, расширить свое представительство в соответствующих международных и европейских органах» [12, p. 20]. Также в этом документе ставится задача безопасного внедрения передовых информационных технологий, в частности интернет-сетей пятого поколения (5G) [12, p. 26].

В Национальной стратегии кибербезопасности США, опубликованной в 2023 г., акцент сделан не только на технических аспектах этого понятия, но и на нарастающем геополитическом факторе, на превращении киберпространства в арену противостояния

великих держав. В этом документе очерчен круг стран, которые Вашингтон считает своими ключевыми противниками: «Правительства Китая, России, Ирана, Северной Кореи и других автократических государств с ревизионистскими намерениями агрессивно используют передовые возможности в киберпространстве для достижения целей, которые противоречат нашим интересам и общепринятым международным нормам» [13, p. 3]. При этом технический аспект безопасности в документе все равно остается превалирующим: фактически геополитическое противостояние трактуется как стремление отдельных участников международных отношений с помощью информационно-коммуникационных технологий нарушить тот глобальный порядок, который за последние десятилетия сформировался под эгидой Вашингтона.

Активизировалось и сотрудничество в рамках Североатлантического альянса в киберпространстве. В текущей редакции Стратегической концепции НАТО 2022 г. отмечено, что кибератака может стать поводом для активации ст. 5 Североатлантического договора о коллективной обороне (п. 25) [14, с. 7]. В п. 24 документа отмечается намерение «ускорить цифровую трансформацию, адаптировать структуру органов военного управления НАТО к информационному веку и укрепить киберзащиту, сети и инфраструктуру» [14, с. 7].

Дальнейший рост напряженности в отношениях между странами Альянса с одной стороны и Российской Федерацией, с другой – существенно снизили возможность диалога в этой сфере и выработки консолидированного общеевропейского подхода к проблемам информационной безопасности. Взаимодействие в отдельных случаях осталось на уровне специальных служб, занимающихся предотвращением атак со стороны террористических организаций, однако в концептуальном плане наметились серьезные расхождения. Кроме того, в рамках специализации стран НАТО в 2008 г. в Таллине был создан Центр передового опыта НАТО в области компьютерной безопасности (NATO Cooperative Cyber Defense Center of Excellence, CCD COE), а в 2014 г. в Риге – Центр передового опыта НАТО в области стратегической пропаганды (NATO Strategic Communication Center of Excellence, STRATCOM COE) [15]. Резкое обострение отношений между странами Запада и Россией в 2022 г., которая в текущей редакции Стратегической концепции названа «наиболее значительной и прямой угрозой безопасности государств – членов НАТО, а также миру и стабильности в евроатлантическом регионе» [14, с. 4], привело к усилению враждебности и переориентации указанных центров на противодействие Москве. Таким образом, усиление политического и санкционного экономического давления со стороны США и Евросоюза на фоне кризисной трансформации системы европейской безопасности подтолкнуло Российскую Федерацию и Республику Беларусь к активизации евразийского вектора внешней политики.

Сотрудничество стран Большой Евразии в отдельных аспектах информационной безопасности практикуется уже два десятилетия. На роль ключевой институциональной основы для этого претендует Шанхайская организация сотрудничества (ШОС), охватывающая 26 государств: 10 полноправных членов, два наблюдателя и 14 партнеров по диалогу. За это время в организации сформировалась и собственная трактовка понятия «международная информационная безопасность», отраженная в различных документах. Ключевую роль в выработке дефиниций сыграли Российская Федерация и Китайская Народная Республика. В целом в ШОС делается упор на выработку универсальных правил и норм ответственного поведения государств в информационной сфере, выстроенных на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран. Тем не менее пока преждевременно говорить о формировании завершенной системы безопасности в информационной сфере на континенте, а необходимо наметить контуры формирующегося партнерства государств Евразии и выявить специфику их взаимодействия.

Анализ ряда документов ШОС, в частности Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. (далее – Соглашение 2009 г.), а также Астанинской декларации 2024 г., позволяет определить специфику трактовки информационной безопасности и выявить

ряд особенностей евразийского партнерства в данной сфере.

Сотрудничество стран Большой Евразии в сфере информационной безопасности прежде всего заключается в противодействии использования ИКТ преступными и террористическими группировками. В частности, на это повлияла первоначальная функциональная специфика Шанхайской организации сотрудничества, роль которой изначально сводилась к стабилизации ситуации в Центральной Азии после распада СССР. В ее Хартии 2002 г. в качестве основополагающей цели было постулировано «совместное противодействие терроризму, сепаратизму и экстремизму» [16]. Поэтому в Соглашении 2009 г. выделена такая угроза, как «информационный терроризм» (п. 2 Приложения 2), т. е. «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях» [8]. В Астанинской декларации 2024 г. особое внимание уделено недопустимости использования информационно-коммуникационных технологий в террористических и экстремистских целях. Государства-члены подчеркнули стремление выработать «документ ШОС о сотрудничестве в борьбе с преступлениями в сфере информационных технологий», а также «добиваться консенсуса по вопросу принятия в рамках ООН всеобъемлющей Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях» [17].

В 2002 г. в рамках ШОС была учреждена Региональная антитеррористическая структура (РАТС), основные задачи и функции которой сводятся к таким направлениям, как координационно-оперативное, международно-правовое и информационно-аналитическое.

Особое значение во взаимодействии государств Большой Евразии по вопросам информационной безопасности придается такой угрозе, как дестабилизация общественно-политической обстановки в государствах-участниках с помощью ИКТ. При этом в соглашениях и резолюциях ШОС не акцентируется внимание на злонамеренных кибератаках со стороны конкретных государств. То есть, в отличие от рассмотренных выше концептуальных документов стран Запада, документы Шанхайской организации сотрудничества официально не постулируют свою направленность против других участников международных отношений. В ее текстах отмечается важность многостороннего сотрудничества в борьбе с неконвенциональными угрозами, с активностью террористических и экстремистских организаций.

Еще одним направлением сотрудничества, которое не вызывает существенных разногласий, является обеспечение защищенности информационной инфраструктуры от катастрофического воздействия техногенных и природных факторов [8, п. 6]. Учитывая сложные природно-климатические условия в отдельных регионах Евразии, взаимопомощь в поддержании стабильности и технической безопасности информационной инфраструктуры государств-участников является актуальной. Этот аспект взаимодействия носит неполитический характер.

Вместе с тем в отличие от концептуального подхода стран Запада, в формирующемся евразийском партнерстве весомая роль отводится социально-психологическим аспектам информационной безопасности. В частности, в это понятие включается защищенность от угрозы нанесения вреда «общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств» [8, п. 5]. Однако сложно определить перечень источников или определенных критериев, которым должна соответствовать информация такого рода для каждого государства Евразии. Поэтому на практике данное положение носит декларативный характер и является, скорее, принципом, характеризующим отказ от вмешательства во внутренние дела друг друга с помощью ИКТ. Как отмечено в Астанинской декларации ШОС 2024 г., «государства-члены подчеркивают ключевую роль ООН в сфере противодействия угрозам в информационном пространстве, создания безопасного информационного пространства, построенного на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран» [17].

Данный принцип нашел отражение и в инициативе государств ШОС по выработке «Правил поведения в области обеспечения международной информационной безопасности» (A/69/723), которые были представлены в письме Генеральном секретарю

ООН [18]. Как отмечалось на официальном сайте МИД России, в этом документе «закрепляется обязательство государств не применять информационно-коммуникационные технологии в целях нарушения международного мира и безопасности, а также для вмешательства во внутренние дела других государств и подрыва их политической, экономической и социальной стабильности» [19].

Наконец, формирующееся евразийское партнерство в сфере информационной безопасности носит и геополитическое измерение. В Соглашении 2009 г. отмечена такая угроза безопасности, как «использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран» [8]. Хотя члены ШОС имеют разный характер отношений со странами Запада: от партнерских (Индия, Казахстан) до весьма напряженных (Беларусь, Иран, Китай, Россия), все они разделяют тезис о недопустимости монополизации информационной сферы со стороны США и их союзников, поддерживая идею многополярности в мировой информационной сфере.

Этот принцип сотрудничества перекликается с основной идеей инициированного белорусской стороной многостороннего документа под названием «Евразийская хартия многообразия и многополярности», в которой были бы отражены «базовые принципы управления международной жизнью, учитывающие многообразие (подходов к организации политической, экономической и социальной жизни в разных странах) и отвергающие гегемонию» [20, p. 129]. В настоящее время идет концептуальная проработка его названия и содержания. Не исключено, что в случае успешного юридического оформления системы евразийской безопасности в будущем эта Хартия станет одним из основополагающих документов, определяющих принципы ее функционирования.

Таким образом, по сравнению с западными странами, которые во главу угла ставят борьбу с точечными информационными атаками, евразийские государства делают больший акцент на иных (социально-политических) аспектах международной информационной безопасности. Это различие коренится, во-первых, в двойственной природе самого концепта «информационная безопасность», которая имеет как техническую составляющую, так и информационно-психологическую, связанную с воздействием на человека и на общество в целом.

Во-вторых, ключевой причиной, которая определила использование различных терминов, стало то, что обеспечение «кибербезопасности» подразумевает обмен данными (в т. ч. и чувствительными) между партнерами на международной арене. В странах Запада, уже принадлежавших к военно-политическому блоку – Североатлантическому альянсу, – такое сотрудничество не вызывало особых затруднений.

В Большой Евразии глубина доверия по вопросам безопасности еще весьма далека от этого. Вместе с тем многие страны континента разделяют общие взгляды на развитие политической составляющей мировой информационной среды: среди них сформировался консенсус о необходимости преодоления западной монополии на каналы коммуникации, на монополию западных стандартов в сфере обеспечения информационной безопасности, о недопустимости социально-политической дестабилизации и вмешательства во внутреннюю политику с помощью ИКТ. Поэтому в странах континента общей платформой стало политическое измерение сотрудничества в сфере информационной безопасности. С расширением состава и разнообразия членов ШОС (со второй половины 2010-х гг.) этот уклон в трактовке сохранился и даже усилился.

Таким образом, различное использование терминов «кибербезопасность» и «информационная безопасность» в официальных документах отражает особенности и различия между евроатлантической системой безопасности и евразийским партнерством. В то время как первая построена на принципе коллективной защиты, сотрудничество евразийских государств пока носит характер взаимодействия в отдельных точечных сферах. Невозможность выстроить систему коллективной безопасности в Большой Евразии обусловлена как различными противоречиями между государствами-участниками (например, Индией и Пакистаном), сложностью обмена между ними важной информацией, так и осознанием любым руководством политических рисков, которые влечет за собой взятие обязательств в сфере коллективной обороны. Поэтому на практике такое сотрудничество

сводится главным образом к пресечению информационного сопровождения действий террористического, экстремистского и сепаратистского характера.

Тем не менее в Евразии также есть примеры организаций, построенных на принципе коллективной безопасности.

Во-первых, это Организация Договора о коллективной безопасности (ОДКБ). В 2017 г. в ее рамках было подписано Соглашение о сотрудничестве государств – членов Организации в области обеспечения информационной безопасности [9].

Во-вторых, это Союзное государство, в котором совместный характер противодействия различным вызовам и угрозам постулирован в уже существующих документах, таких как Военная доктрина 2021 г., а также дополнительно прорабатывается в проектах новых соглашений. В частности, общее понимание содержания, основных угроз и задач по обеспечению информационной безопасности отражено в соответствующей Концепции, которая была утверждена Постановлением Высшего Государственного Совета Союзного государства Беларуси и России от 22.02.2023 № 1 [10].

Специфика сотрудничества в вопросах информационной безопасности между Республикой Беларусь и Российской Федерацией, отраженная в указанном документе, определяется усилением политического и санкционного давления на оба государства в начале 2020-х гг. В связи с этим многие положения Концепции информационной безопасности Союзного государства не только повторяли отдельные тезисы из Соглашения Шанхайской организации сотрудничества 2009 г., но в ряде случаев даже усиливали определенные акценты. Например, с учетом кризисной трансформации системы европейской безопасности в начале 2020-х гг. особое внимание было привлечено к противодействию внешнему вмешательству с помощью ИКТ: «В целях дестабилизации общественно-политической ситуации на территории государств-участников распространяется недостоверная и искаженная информация. В сети Интернет размещаются материалы террористических экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка» [10, п. 12].

Также в Концепции 2023 г. значительное место отведено социально-гуманитарному аспекту информационной безопасности и угрозам в этой сфере. В частности, отмечено «активное информационное воздействие, направленное на разрушение национальной самобытности, культурных и традиционных духовно-нравственных ценностей народов России и Беларуси, искажение исторической правды, дискредитацию традиционных нравственных, семейных ценностей и ориентиров» [10, п. 12]. Кроме того, указано, что «по политическим причинам пользователям сети Интернет навязывается искаженный взгляд на исторические факты, процессы и события, происходящие в Российской Федерации, Республике Беларусь и других странах» [10, п. 13]. Противодействие указанным угрозам может быть обеспечено путем гармонизации исторической политики двух государств и государственной политики в гуманитарной сфере.

Эти направления отражают глубину интеграционных процессов в рамках Союзного государства. Безусловно, такое тесное сотрудничество имеет историческую обусловленность и объективные географические ограничения, поэтому преждевременно рассчитывать, что оно охватит большинство государств Большой Евразии.

Тем не менее опыт Союзного государства может оказать как техническую, так и политическую поддержку евразийскому партнерству в области обеспечения информационной безопасности на отдельных направлениях. Во-первых, продвинутый уровень технологического развития Беларуси и России дает возможность реализовать идею строительства «цифрового альянса» с другими заинтересованными сторонами на континенте [21, с. 10]. Построение такого альянса в рамках расширенного информационного сотрудничества на пространстве Большой Евразии позволит снизить эффект санкционного давления на Республику Беларусь и на Российскую Федерацию, преодолеть негативные последствия полного либо частичного блокирования доступа к западным информационным платформам, незащищенность собственных информационных ресурсов, находящихся за пределами Союзного государства. Перспективным представляется и передача опыта Союзного

государства странам-партнерам по координации взаимодействия в рамках расследования преступлений в сфере информационно-коммуникационных технологий.

Во-вторых, общие взгляды руководства Республики Беларусь и Российской Федерации могут оказать поддержку политическому измерению формирующегося широкого евразийского партнерства в сфере информационной безопасности. Минск и Москва продвигают идею «информационного суверенитета», разделяя такие взгляды в отношении управления Интернетом на международном уровне, как «недопущение доступа к Сети как инструмента влияния на другие государства, воздержание государств от действий, направленных на ограничение функционирования или доступа к сети Интернет на территории других государств, суверенные права государств на управление национальным сегментом сети Интернет» [21, с. 24]. Республика Беларусь стала соавтором резолюции Генеральной Ассамблеи ООН 77/36 «Достижения в сфере информатизации и телекоммуникаций в сфере международной безопасности», принятую в декабре 2022 г. по инициативе России. В этом документе отражен призыв к государствам-членам в рамках Рабочей группы открытого состава «продолжать обмениваться мнениями о регулярном институциональном диалоге по вопросам безопасности в сфере использования информационно-коммуникационных технологий с целью выработки общего понимания о наиболее эффективном формате будущего регулярного институционального диалога при широком участии государств под эгидой Организации Объединенных Наций, который будет создан по завершении деятельности Рабочей группы открытого состава в 2021–2025 гг.» [22] Таким образом, Союзное государство вносит вклад в реализацию идеи многополярности в информационной сфере на евразийском континенте.

Заключение

Подводя итог, следует отметить, что контуры и содержание формирующегося евразийского партнерства в сфере информационной безопасности в значительной степени определяются особенностями системы международных отношений на континенте, которая характеризуется наличием не только нескольких центров влияния, но и противоречий между ними. В связи с этим практическая составляющая многостороннего партнерства сводится к отдельным аспектам обеспечения информационной безопасности, в частности к борьбе с информационным терроризмом, экстремизмом, к поддержанию стабильности и технической безопасности информационной инфраструктуры. Вместе с тем противоречия ряда крупнейших государств Евразии (России, КНР, Ирана) в отношениях с США обусловливают все более выраженную артикуляцию политической составляющей, которая сводится к продвижению идей многополярности мирового информационного пространства, информационного суверенитета и невмешательства во внутренние дела других государств с помощью ИКТ.

Союзное государство является примером более глубокого сотрудничества по вопросам информационной безопасности, что обусловлено соответствующим уровнем развития двусторонних отношений Республики Беларусь и Российской Федерации.

Взаимное политическое доверие руководства и общий взгляд на фундаментальные основы современного миропорядка позволяют не только декларировать, но и углубить сотрудничество в социально-гуманитарной сфере, работа в которой также является одним из аспектов обеспечения информационной безопасности. Преждевременно полагать, что такая степень взаимоотношений охватит большинство государств континента в силу их многообразия и сложности некоторых двусторонних взаимоотношений. В то же время Республика Беларусь и Российская Федерация совместно могут сформулировать ряд императивов по формированию контуров будущей системы евразийского партнерства по вопросам евразийской безопасности. Во-первых, сотрудничество в рамках Союзного государства может стать основой для формирования одного из цифровых альянсов в Евразии. Во-вторых, в политическом отношении Минск и Москва являются одними из наиболее активных сторонников идеи многополярного мира в международной информационной среде. Эта идея, как ожидается, будет отражена и в финальном варианте Евразийской хартии многообразия и многополярности, разработку которой инициировала Республика Беларусь.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Тимофеев, И. Н. Евразийская структура безопасности: от идеи к практике [Электронный ресурс] / И. Н. Тимофеев // Рос. совет по междунар. делам. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/evraziyskaya-struktura-bezopasnosti-ot-idei-k-praktike/. – Дата доступа: 10.10.2024.

2. Мельникова, Ю. Ю. Евразийская безопасность как коммуникативная практика: задачи для России и Китая [Электронный ресурс] / Ю. Ю. Мельникова // Рос. совет по междунар. делам. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/evraziyskaya-bezopasnost-kak-kommunikativnaya-praktika-zadachi-dlya-rossii-i-kitaya/?sphrase_id=163455540. – Дата доступа: 10.10.2024.

3. Зиновьева, Е. С. Международная информационная безопасность: проблемы двустороннего и многостороннего сотрудничества / Е. С. Зиновьева. – М. : Моск. гос. ин-т междунар. отношений (ун-т) М-ва иностр. дел Рос. Федерации, 2021. – 280 с.

4. Базлуцкая, М. М. Игровое пространство «информационного беспорядка» / М. М. Базлуцкая, А. Н. Сытник // Россия в глоб. политике. – 2024. – Т. 22, № 4. – С. 122–136.

5. Мороз, Н. О. Международно-правовое регулирование поддержания информационной безопасности / Н. О. Мороз // Право.by. – 2022. – № 6 (80). – С. 138–144.

6. Русакович, А. В. Проблемы безопасности на постсоветском пространстве в начале 2020-х гг.: глобальный и региональный аспекты / А. В. Русакович. – Минск : РИВШ, 2024. – 170 с.

7. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] : утв. Решением Всебелорус. нар. собрания 25.04.2024, № 5 // Национальный правовой Интернет-портал Республики Беларусь : [сайт]. – Режим доступа: https://pravo.by/document/?guid=-12551&p0=P924v-0005. – Дата доступа: 10.10.2024.

8. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года (вступило в силу с 5 января 2012 г.) [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/-document/?guid=12551&p0=I00900114. – Дата доступа: 20.10.2024.

9. Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/-document/?guid=12551&p0=E01700001. – Дата доступа: 10.10.2024.

10. О Концепции информационной безопасности Союзного государства [Электронный ресурс] : постановление Высшего Государственного Совета Союзного государства Беларуси и России от 22.02.2023, № 1 // Информационно-правовой портал «Гарант». – Режим доступа: https://base.-garant.ru/407406480/. – Дата доступа: 10.10.2024.

11. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] : утв. постановлением Совета Безопасности Респ. Беларусь 18.03.2019, № 1 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/-document/?-guid=12551&p0=P219s0001. – Дата доступа: 10.10.2024.

12. Joint Communication: The EU’s Cybersecurity Strategy for the Digital Decade [Electronic resource] // European Commission. – Mode of access: https://ec.europa.eu/newsroom/dae/-redirection/document/72164. – Date of access: 20.10.2024.

13. National Cybersecurity Strategy (March 2023) [Electronic resource] // The White House. – Mode of access: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. – Date of access: 20.10.2024.

14. Стратегическая концепция НАТО 2022 года (принята главами государств и правительств на встрече в верхах НАТО в Мадриде 29 июня 2022 г.) [Электронный ресурс] // Организация Североатлантического договора. – Режим доступа: https://www.nato.int/nato_static_-fl2014/assets/pdf/-2022/6/pdf/290622-strategic-concept-ru.pdf. – Дата доступа: 20.10.2024.

15. Centres of Excellence [Electronic resource] // North Atlantic Treaty Organization. – Mode of access: https://www.nato.int/cps/en/natohq/topics_68372.htm. – Date of access: 20.10.2024.

16. Хартия Шанхайской организации сотрудничества (6 июня 2002 года) [Электронный ресурс] // Президент России. – Режим доступа: http://www.kremlin.ru/supplement/3450. – Дата доступа: 20.10.2024.

17. Астанинская декларация Совета глав государств – членов Шанхайской организации сотрудничества (4 июля 2024 г.) [Электронный ресурс] // Шанхайская организация сотрудничества. – Режим доступа https://rus.sectsco.org/20240704/1420683.html. – Дата доступа: 20.10.2024.

18. Правила поведения в области обеспечения международной информационной безопасности : Приложение к письму постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря (A/69/723) [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://documents.un.org/doc/undoc/gen/n15/-014/04/pdf/n1501404.pdf. – Дата доступа: 20.10.2024.

19. Об инициативе стран – членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» [Электронный ресурс] // М-во иностр. дел Рос. Федерации. – Режим доступа: https://www.mid.ru/ru/foreign_policy/international_safety/-mezdunarodnaa-informa-cionnaa-bezopasnost/1582268/. – Дата доступа: 20.10.2024.

20. Makei, V. V. Liberal International Order: Can It Be Saved in Today's Non-Hegemonic World? / V. V. Makei // Russia in Global Affairs. – 2023. – Nr 21 (1). – P. 114–130.

21. «Цифра» и искусственный интеллект на службе дипломатии : аналит. докл. / Е. С. Зиновьева [и др.] ; под ред. Е. С. Зиновьевой. – М. : МГИМО, 2024. – 47 с.

22. Резолюция Генеральной Ассамблеи ООН 77/36 «Достижения в сфере информатизации и телекоммуникаций в сфере международной безопасности» : принята 7 декабря 2022 г. [Электронный ресурс] // Национальная ассоциация международной информационной безопасности. – Режим доступа: https://namib.online/wp-content/uploads/2023/01/A_RES_77_36RU%-D0%9C%-D0%98%D0%91-7.12.2022.pdf. – Дата доступа: 15.10.2024.

REFERENCES

1. Timofiejev, I. N. Jevrazijskaja struktura biezopasnosti: ot idiei k praktikie [Eliektronnyj riesurs] / I. N. Timofiejev // Ros. soviet po miezhdunar. dielam. – Riezhim dostupa: https://russiancouncil.ru/-analytics-and-comments/analytics/evraziyskaya-struktura-bezopasnosti-ot-idei-k-praktike/. – Data dostupa: 10.10.2024.

2. Miel'nikova, Yu. Yu. Jevrazijskaja biezopasnost' kak kommunikativnaja praktika: zadachi dlia Rossii i Kitaja [Eliektronnyj riesurs] / Yu. Yu. Miel'nikova // Ros. soviet po miezhdunar. dielam. – Riezhim dostupa: https://russiancouncil.ru/analytics-and-comments/analytics/evraziyskaya-bezopasnost-kak-kommunikativnaya-praktika-zadachi-dlya-rossii-i-kitaya/?sphrase_id=163455540. – Data dostupa: 10.10.2024.

3. Zinov'jeva, Ye. S. Miezhdunarodnaja informacionnaja biezopasnost': probliemy dvustoronniego i mnogostoronniego sotrudnichiestva / Ye. S. Zinov'jeva. – M. : Mosk. gos. in-t miezhdunar. otnoshenij (un-t) M-va inostr. diel Ros. Fiedieracii, 2021. – 280 s.

4. Bazluckaja, M. M. Igrovoje prostranstvo «informacionnogo biesporiadka» / M. M. Bazluckaja, A. N. Sytnik // Rossija v global. politikie. – 2024. – T. 22, № 4. – S. 122–136.

5. Moroz, N. O. Miezhdunarodno-pravovoje rieguliravanije poddierzhanija informacionnoj biezopasnosti / N. O. Moroz // Pravo.by. – 2022. – № 6 (80). – S. 138–144.

6. Rusakovich, A. V. Probliemy biezopasnosti na postsovietskom prostranstvie v nachalie 2020-kh gg.: global'nyj i riegional'nyj aspiekty / A. V. Rusakovich. – Minsk : RIVSh, 2024. – 170 s.

7. Koncepcija nacional'noj biezopasnosti Riespubliki Bielarus' [Eliektronnyj riesurs] : utv. Rieshenijem Vsiebielorus. nar. sobranija 25.04.2024, № 5 // Nacional'nyj pravovoj Internet-portal Riespubliki Bielarus'. – Riezhim dostupa: https://pravo.by/document/?guid=12551&p0=P924v0005. – Data dostupa: 10.10.2024.

8. Soglashenije miezhdu pravitiel'stvami gosudarstv – chlienov Shankhajskoj organizacii sotrudnichiestva o sotrudnichiestvie v oblasti obiespiechienija miezhdunarodnoj informacionnoj biezopasnosti ot 16 ijunia 2009 goda (vstupilo v silu s 5 janvaria 2012 g.) [Eliektronnyj riesurs] // Nacional'nyj pravovoj Internet-portal Riespubliki Bielarus'. – Riezhim dostupa: https://pravo.by/-document/?guid=12551&p0=-I00900114. – Data dostupa: 20.10.2024.

9. Soglashenije o sotrudnichiestvie gosudarstv – chlienov Organizacii Dogovora o kolliektivnoj biezopasnosti v oblasti obiespiechienija informacionnoj biezopasnosti [Eliektronnyj riesurs] // Nacional'nyj pravovoj Internet-portal Riespubliki Bielarus'. – Riezhim dostupa: https://pravo.by/-document/?guid=12551&p0=E01700001. – Data dostupa: 10.10.2024.

10. O Koncepcii informacionnoj biezopasnosti Sojuznogo gosudarstva [Eliektronnyj riesurs] : postanovlienije Vysshego Gosudarstviennogo Sovieta Sojuznogo gosudarstva Bielarusi i Rossii ot 22.02.2023, № 1 // Informacionno-pravovoj portal «Garant». – Riezhim dostupa: https://base.garant.ru/407406480/. – Data dostupa: 10.10.2024.

11. Koncepcija informacionnoj biezopasnosti Riespubliki Bielarus' [Eliektronnyj riesurs] : utv. postanovlienijem Sovieta Biezopasnosti Riespubliki Bielarus' 18.03.2019, № 1 // Nacional'nyj pravovoi Internet-portal Riespubliki Bielarus'. – Riezhim dostupa: https://pravo.by/document/?guid=-12551&p0=P219s0001. – Data dostupa: 10.10.2024.

12. Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade [Electronic resource] // European Commission. – Mode of access: https://ec.europa.eu/newsroom/dae/-redirection/document/72164. – Data dostupa: 20.10.2024.

13. National Cybersecurity Strategy (March 2023) [Electronic resource] // The White House. – Mode of access: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. – Data dostupa: 20.10.2024.

14. Stratiegichieskaja koncepcija NATO 2022 goda (priniata glavami gosudarstv i pravitiel'stv na vstriechie v vierkhakh NATO v Madride 29 ijunia 2022 g.) [Eliektronnyj riesurs] // Organizacija Sievieroatlantichieskogo dogovora. – Riezhim dostupa: https://www.nato.int/nato_static_fl2014/-assets/pdf/2022/6/pdf/290622-strategic-concept-ru.pdf. – Data dostupa: 20.10.2024.

15. Centres of Excellence [Electronic resource] // North Atlantic Treaty Organization. – Mode of access: https://www.nato.int/cps/en/natohq/topics_68372.htm. – Date of access: 20.10.2024.

16. Khartija Shankhajskoj organizacii sotrudnichiestva (6 ijunja 2002 goda) [Eliektronnyj riesurs] // Priezidient Rossii. – Riezhim dostupa: http://www.kremlin.ru/supplement/3450. – Data dostupa: 20.10.2024.

17. Astaninskaja dieklaracija Sovieta glav gosudarstv – chlienov Shankhajskoj organizacii sotrudnichiestva (4 ijulia 2024 g.) [Eliektronnyj riesurs] // Shankhajskaja organizacija sotrudnichiestva. – Riezhim dostupa: https://rus.sectsco.org/20240704/1420683.html. – Data dostupa: 20.10.2024.

18. Pravila poviedienija v oblasti obiespiechienija miezhdunarodnoj informacionnoj biezopasnosti [Eliektronnyj riesurs] : Prilozhenije k pis'mu postojannykh priedstavitieliej Kazakhstana, Kitaja, Kyrgyzstana, Rossijskoj Fiedieracii, Tadzhikistana i Uzbiekistana pri Organizacii Objedinionnykh Nacij ot 9 janvaria 2015 goda na imia Gienieral'nogo siekrietaria (A/69/723) // Organizacija Objedinionnykh Nacij. – Riezhim dostupa: https://documents.un.org/doc/undoc/gen/n15/014/04/pdf/n-1501404.pdf. – Data dostupa: 20.10.2024.

19. Ob iniciativie stran – chlienov ShOS «Pravila poviedienija v oblasti obiespiechienija miezhdunarodnoi informacionnoj biezopasnosti» [Eliektronnyj riesurs] // M-vo inostr. diel Ros. Fiedieracii. – Riezhim dostupa: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bez-opasnost/1582268/. – Data dostupa: 20.10.2024.

20. Makei, V. V. Liberal International Order: Can It Be Saved in Today's Non-Hegemonic World? / V. V. Makei // Russia in Global Affairs. – 2023. – Nr 21 (1). – P. 114–130.

21. «Cifra» i iskusstviennyj intielliekt na sluzhbie diplomatii : analit. dokl. / Ye. S. Zinov'jeva [i dr.] ; pod ried. Ye. S. Zinov'jevoj. – M. : MGIMO, 2024. – 47 s.

22. Riezoliucija Gienieral'noj Assambliei OON 77/36 «Dostizhenija v sfierie informatizacii i tieliekommunikacii v sfierie miezhdunarodnoj biezopasnosti» [Eliektronnyj riesurs] : priniata 7 diekabria 2022 g. // Nacional'naja associacija miezhdunarodnoj informacionnoj biezopasnosti. – Riezhim dostupa: https://namib.online/wp-content/uploads/2023/01/A_RES_77_36-RU-%D0%9C%D0%98%-D0%917.12.2022.pdf. – Data dostupa: 15.10.2024.

Рукапіс паступіў у рэдакцыю 12.11.2024