DOI 10.35775/PSI.2025.73.8.005
УДК 32.327

Д.Ю. КОЧЕРИНСКИЙ
магистр Факультета управления и политики
МГИМО МИД России, Россия, г. Москва
E-mail: kocherinskiy.danil@mail.ru

ВНЕШНЯЯ ПОЛИТИКА РОССИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: РЕГИОНАЛЬНОЕ ИЗМЕРЕНИЕ

В статье анализируются основные направления сотрудничества Российской Федерации в области информационной безопасности на региональном измерении. Несмотря на то, что Россия сталкивается в последние годы с растущим сопротивлением со стороны Запада, она по-прежнему сохраняет внешнеполитическую инициативу на данном направлении в рамках таких форматов как ШОС, БРИКС, СНГ и ОДКБ, поскольку сотрудничество на международном уровне остается надежным инструментом для решения глобальных проблем. Методология данной работы носит комплексный характер, так как использовалось историческое изложение с тематическим анализом актуальных и дискуссионных вопросов; анализ нормативно-правовой базы, позволяющий изучить как осуществляется регулирование информационной сферы, а также качественный анализ для выявления тенденций. Результаты работы носят как теоретическую, так и практическую значимость, так как в работе осуществляется попытка сбора, обобщения и анализа имеющейся информации по теме исследования. По итогам проделанной работы автор приходит к выводу, что Россия исходит из кооперативного подхода в вопросах обеспечения международной информационной безопасности, а результативность регионального сотрудничества прослеживается во время голосования по инициативам, выдвигаемым Россией, на площадке Генеральной Ассамблеи ООН.

Ключевые слова: *международная информационная безопасность, ШОС, БРИКС, СНГ, ОДКБ, сотрудничество, угрозы безопасности.*

Введение. В Концепции внешней политики России [21] прослеживается подход политического реализма, так как на постоянной основе заявляется о необходимости наращивать военный потенциал для обороны страны, выводить экономику страны на новый уровень и стремление к автономности, то есть разработка своих собственных продуктов, инноваций и снижение взаимозависимости. Однако в сфере международной безопасности Россия исходит из кооперативного подхода, согласно которому призывает мировое сообщество совместными усилиями бороться с угрозами международной информационной безопасности (МИБ), путем создания общих механизмов сотрудничества, единой правовой базы, основываясь на принципах взаимопомощи. Это объяснимо тем, что если

информационное измерение превратить в перспективное поле боя, то это неизбежно приведет к новой гонке вооружений. Именно поэтому Россия призывает все страны демилитаризировать данную сферу и еще в 1998 году на 53-ей сессии Генеральной Ассамблеи ООН начала выдвигать свои инициативы в проекте резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [15].

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 4; 6; 7; 12; 13; 14; 24; 27; 28; 30; 31].

Однако проблему совершенствования внешней политики России в области информационной безопасности нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Результаты. На сегодняшний день киберпреступность имеет сетевой характер, поэтому регулирование данного вопроса должно осуществляться на международном уровне. На повестке находится достаточно много узловых вопросов, среди которых можно выделить: единая нормативно-правовая база с общепринятым понятийным аппаратом, которая позволит единообразно разрешать споры по поводу ответственности в цифровом пространстве; доверие, открытость и сотрудничество; механизмы межгосударственного и межведомственного диалога, позволяющие ускорить процесс выработки решения, при сохранении автономности и независимости. Здесь речь идет о возможности государства самостоятельно принимать решения, основываясь на едином регламенте и с учетом прав человека. Предпочтительным был бы исход, при котором соглашение было бы подписано всеми странами без оговорок и носило бы обязательный характер. Именно поэтому Российская Федерация в рамках таких региональных организаций как ШОС, БРИКС, СНГ и ОДКБ активно придерживается кооперативного подхода для реализации общих интересов по защите граждан и информационной инфраструктуры от атак, преступлений и краж. Еще многосторонний формат важен тем, что все страны-члены региональных организаций являются членами ООН, в рамках которого возможно совместное продвижение региональных инициатив на глобальном уровне и с большей долей вероятности есть шанс заручиться поддержкой большинства.

Что касается взаимодействия России с Шанхайской Организацией Сотрудничества, то впервые еще в 2006 году на саммите в Шанхае была зафиксировано согласованность стран-членов организации по вопросу международной информационной безопасности [29]. Государства пришли к выводу, что ИКТ являются неотъемлемой частью жизни человека, важной составляющей оборонной, экономической и политической сфер национальных интересов страны, а также технологии качественно влияют на уровень жизни. В рамках единого региона проще выработать общий подход ввиду культурной и ценностной близости, именно поэтому по итогам создается группа экспертов государств-членов ШОС по вопросам МИБ. Целью данной группы было создание плана действий

по противодействию угрозам МИБ, поэтому в период с 2006 по 2009 год был успешно реализован план и был написан проект соглашения между правительства государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности [32]. Данное соглашение является важным этапом, так как именно в нем в международно-правом контексте были освещены угрозы, приоритетные направления и механизмы сотрудничества в этой сфере. Среди основных угроз в документе упоминаются: терроризм и преступность в информационной среде, разработка и создание оружия для ведения информационных войн, ущемление прав других стран из-за собственного превосходства в технологическом прогрессе, дезинформация, препятствование работе критически важной инфраструктуры.

В дальнейшем ШОС предложила направить письмо генеральному секретарю ООН Пан Ги Муну в 2011 году с целью принять на рассмотрение проект «Правил поведения в области обеспечения международной безопасности», однако он не получил поддержки и даже подвергся критике. Спустя год, после того как правила были скорректированы, на 70-ой Генеральной Ассамблеи ООН ГПЭ приняла доклад, основным посылом которого был запрет использования ИКТ в военных целях и призыв к заблаговременному предотвращению конфликтов в информационном пространстве [5]. Это был первый совместно согласованный документ России и ШОС, тем самым подтвердив приверженность единых подходов стран-участниц к обеспечению международной информационной безопасности.

В дальнейшем данная инициатива получила развитие и в городе Циндао в 2018 году на конференции ШОС была подписана декларация, закрепляющая главенствующую роль ООН по написанию глобальных норм и правил в информационном пространстве, призывающая к формированию специального рабочего механизма при ООН для обеспечения мониторинга и контроля за реализацией и соблюдением правил поведения и мер ответственности в сети-Интернет [20].

Самаркандская декларация [22] ШОС 2022 года вновь подтвердила приверженность стран-участниц к обеспечению международной информационной безопасности, а также продолжению реализации намеченного в 2009 году плана взаимодействия в данной сфере.

Важной платформой для реализации инициатив выступает макрорегиональная площадка БРИКС. С момента итогового объединения всех стран (с 2011 года) в единое целое постоянно ведутся дискуссии, обсуждения на тему обеспечения информационной безопасности. Идея укрепления сотрудничества по противодействию информационным угрозам прослеживается во всех документах данного объединения и уже в 2013 году при подготовке к саммиту БРИКС были предложены форматы объединения в Группу правительственных экспертов. В 2015 году будет создана данная группа, в функционал которой предполагал курирование вопросов ИКТ, разработка правил ответственного поведения государств и механизмов сотрудничества. По итогам шестого саммита БРИКС была принята Уфимская декларация [26], которая показала, что страны-участницы

формата имеют общий подход к проблеме именно поэтому был взят курс на распространение только уже на уровне ООН идеи о создании юридически-обязывающего документа в сфере МИБ. В юбилейный для России год в области информационной безопасности, по итогам Десятого саммита БРИКС была принята Йоханнесбургская декларация [8], закрепляющая первостепенную роль ООН как главного координатора и разработчика норм, принципов ответственного поведения государств в использовании ИКТ, затем юридически-обязывающего нормативного акта по методам противодействия угрозам ИКТ. Отмечались две тенденции, которые идут параллельно друг другу: развитие возможностей ИКТ и рост угроз от использования этих же технологий [3. С. 1-22]. Для этого в отдельный пункт выделили приоритетность разрешения вопроса противодействия использованию ИКТ в террористических и преступных целях. Помимо этого государства отметили с положительной стороны развитие возможностей сети-Интернет в социальной, политической и экономической сферах, однако подтвердили свою приверженность к созданию нормативных актов, регулирующих сотрудничество и противодействие применения ИКТ в преступных и террористических целях. В продолжении сохранения позиции по МИБ являются Пекинская [18] и Казанская декларации [9] от 2022 года и 2024 года соответственно. В них осуществляется призыв к мировому сообществу о необходимости в комплексном подходе при решении данного вопроса, поскольку несмотря на многочисленные положительные стороны технологий, все больше и больше появляется случаев применения в преступных целях. Важна техническая помощь при создании прозрачной, безопасной и стабильной среды для использования информационных технологий, при этом отводится главенствующая роль ООН в вопросах развития диалога в данной сфере и подчеркивается эффективность рабочей группы открытого состава ввиду своего всеобъемлющего механизма.

Таким образом, можно говорить о консолидации мнений в рамках ШОС и БРИКС, поскольку выступления с общим документом показывают приверженность каждой из стран-участниц к единому мнению, а также наблюдается тенденция в постоянной поддержке позиции России. Помимо этого, на постоянной основе подчеркивается главенствующая роль ООН в обеспечении информационной безопасности, и заявляется готовность организации оказывать поддержку инициативам со стороны ООН для выведения универсальных норм и правил по регулированию поведения в интернете [23. С. 276-287].

Затем стоит привести пример еще одной региональной организации –СНГ. Важным этапом в становлении сотрудничества была Концепция информационной безопасности государств-участников СНГ в военной сфере от 1999 года, которая впервые закрепила «белые пятна» на пути к информационной безопасности (отсутствие нормативно-правовой базы) и ряд угроз, которым необходимо противостоять, а именно преступность с применением ИКТ, чрезмерный объем запрашиваемых персональных данных, возможная разведка со стороны других государств [19]. Следующим этапом было учреждение комиссии

по информационной безопасности в 2004 году, а уже в 2011 была преобразована в комиссию при Региональном содружестве связи.

Следующим и не менее важным документом, которое и по сей день является базовым для разработки и реализации стратегий стран СНГ, можно выделить Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года [16]. Россия ратифицировали данное соглашение лишь 1 июля 2021 года с оговорками. Так, например, Российская Федерация оставляет за собой право признавать отдельные деяния, предусмотренные соглашением, как преступлениями, так и административными правонарушениями. Сотрудничество в рамках данного соглашения предполагает обмен информацией о возможных будущих преступлениях в сфере компьютерной информации, о формах и средствах выявления, в дальнейшем оказание содействия в проведении операций по пресечению преступлений, создание совместных информационных систем для предотвращения преступлений и иные формы содействия и оказания помощи.

Таким образом, важно понимать, что интересы каждого государства в Содружестве нашли общие точки соприкосновения, поэтому всем документам в рамках организации свойственен единый и комплексный подход противодействию угрозам МИБ [11. С. 500-508]. При этом прослеживаются сразу два аспекта: техническая составляющая безопасности (защищенность информационной инфраструктуры), и идеологическая (осведомленность населения о возможной дезинформации). И поскольку одной из стран-участниц является Россия, то в большинстве соглашений есть призыв о демилитаризации информационной среды, противодействии использованию ИКТ в террористических и преступных целях [2. С. 181-186].

На площадках ШОС и БРИКС ведутся обсуждения и вырабатываются правила ответственного поведения государств, в то время как ОДКБ и СНГ занимаются противодействием информационным угрозам [10. С. 342-351]. В рамках ОДКБ проводилась операция «Прокси» – противодействие криминалу в информационной среде в 2009 году, а уже через год Прокси-Юг для поддержания социально-политической стабильности в Кыргызстане, препятствуя деструктивному влиянию ИКТ. Данные операции способствуют стабилизации ситуации, блокируют сайты-мошенники и не допускают распространения идеологии терроризма. В 2017 году на саммите ОДКБ в Минске было подписано Соглашение о сотрудничестве стран-членов ОДКБ в области обеспечения информационной безопасности [17], что показало доверительный уровень отношений. Помимо налаживания межведомственного и межгосударственного сотрудничества для противодействия информационной угрозам, в соглашении речь идет о совместной выработке позиции для дальнейшего представления уже на уровне ООН.

Выводы. Ранее рассмотренные инициативы важным тем, что среди приоритетных регионов внешней политики России выступают и страны постсоветского пространства, и страны АТР, то есть Российская федерация видит будущее сотрудничество с этим регионами не только в сфере национальных интересов,

но и в сфере обеспечения международной информационной безопасности. В сфере МИБ Российская Федерация исходит из кооперативного подхода. Важно обратить внимание, что повестка угроз во всех документах сохраняется и зачастую представляет позицию России по данному вопросу и это вполне логично, потому что Россия пытается донести миру идею, что информационная безопасность – это неотъемлемая часть безопасности страны и что подрыв информационного суверенитета приравнивается к вмешательству во внутренние дела государства [25. С. 1-8]. Это война совсем другого уровня, возможно с меньшим количеством потерь среди гражданского населения, но возможно с большими затратами для государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.
2. **Амельчакова В.Н., Кокорев А.Н.** Анализ опыта государств–участников содружества независимых государств по обеспечению безопасности информационного пространства и его имплементация в законодательство России // Вестник Московского университета МВД России. 2021. № 5.
3. **Бойко С.М.** Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. 2019. № 1.
4. **Гавров С.Н., Еремкин М.П.** Использование искусственного интеллекта в контексте информационной войны // Вопросы политологии. 2025. № 2.
5. Генеральная Ассамблея ООН: Семидесятая сессия. Пункт 93 повестки дня: Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности от 22 июля 2015 / Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174 // https://undocs.org/pdf?symbol=ru/a/70/174.
6. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
7. **Иващенко З.С., Васильченко О.В., Григорян Д.К., Малявина А.Б.** Фейковые новости о ходе проведения Специальной военной операции как угроза национальной безопасности Российской Федерации // Евразийский Союз: вопросы международных отношений. 2024. № 9.
8. Йоханнесбургская декларация Десятого саммита БРИКС от 26 июля 2018 года // http://www.kremlin.ru/supplement/5323.
9. Казанская декларация Шестнадцатого саммита БРИКС от 23 октября 2024 года // http://static.kremlin.ru/media/events/files/ru/MUCfWDg0QRs3xfMUiCAmF3LEh02OL3Hk.pdf.

10. **Крутских А.В.** Международная информационная безопасность: в поисках консолидированных подходов: интервью с Андреем Владимировичем Крутских, специальным представителем президента российской федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д.А. Пискунов // Вестник РУДН. Серия: Международные отношения. 2022. № 2.
11. **Лебедева Е.В.** Информационная безопасность государств СНГ: этапы реализации // Национальная безопасность. 2016. № 4.
12. **Медведева В.К., Медведев Н.П.** Информационная политика государства: современные вызовы и направления совершенствования (Часть 1) // Вопросы политологии. 2025. № 1.
13. **Муравых А.И., Никитенко Е.Г., Стародуб И.В.** Интегральная мировая война (Часть 1) // Вопросы политологии. 2025. № 3.
14. **Никитин К.А.** Международный терроризм: опыт стран Содружества независимых государств // Вопросы политологии. 2025. № 6.
15. Организация Объединенных Наций: официальный сайт / Документы / Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» // https://www.un.org/ru/ga/53/docs/53res1.shtml.
16. Официальный интернет-портал правовой информации: официальный сайт / Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: Ратифицировано Федеральным законом от 01.07.2021 № 237-ФЗ. с оговоркой, вступило в силу для Российской Федерации 17 июля 2022 года // http://publication.pravo.gov.ru/Document/View/0001202207180005.
17. Официальный интернет-портал правовой информации: официальный сайт / официальное опубликование Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. Российская Федерация // http://publication.pravo.gov.ru/Document/View/0001201904260001?index=0&rangeSize=1.
18. Пекинская декларация XIV саммита БРИКС от 23 июня 2022 года // http://kremlin.ru/supplement/5819.
19. Постоянное представительство Российской Федерации при СНГ: официальный сайт / Список конвенций, концепций и программ, принятых в рамках СНГ // http://cismission.mid.ru/ii6.html.
20. Президент России: официальный сайт. Циндаоская декларация Совета глав государств-членов Шанхайской организации сотрудничества, 10 июня 2018 // http://kremlin.ru/supplement/5315.
21. Российская Федерация. Указы. Об утверждении Концепции внешней политики Российской Федерации: утверждена указом Президента Российской Федерации 31 марта 2023 г. // Собрание Законодательства Российской

Федерации № 14 от 3 апреля 2023 года, ст. 2406 // https://www.szrf.ru/api/issues/images?volid=1002023014000&docid=45#zoom=100&page=10.
22. Самаркандская декларация Совета глав государств-членов Шанхайской организации сотрудничества. 2022 год // https://rus.sectsco.org/images/07e8/0b/16/1600203.pdf.
23. **Себекин С.А.** Роль шанхайской организации сотрудничества и БРИКС в обеспечении международной информационной безопасности в условиях продолжающегося конфликта на Украине // Российско-китайские исследования. 2022. № 4.
24. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
25. **Стожко Д.К., Стожко К.П.** Информационная безопасность в контексте развития цифровой экономики и международного сотрудничества // АОН. 2019. № 3.
26. Уфимская декларация по итогам VII саммита БРИКС от 9 июля 2015 года // ГАРАНТ-Образование // https://base.garant.ru/71480256/.
27. **Форостянный Н.С., Тёмкина А.М.** Политический потенциал БРИКС в трансформации системы международной безопасности // Евразийский Союз: вопросы международных отношений. 2024. № 7.
28. **Хопёрская Л.Л.** Евразийская безопасность: концепции и инициативы // Евразийский Союз: вопросы международных отношений. 2025. № 1.
29. Центральный интернет-портал Шанхайской Организации Сотрудничества / Заявление глав государств-членов ШОС по международной информационной безопасности г. Шанхай, 15 июня 2006 года // http://infoshos.ru/ru/?id=94.
30. **Чжао Лэй.** Сотрудничество в области кибербезопасности и борьбы с кибертерроризмом в рамках ШОС // Евразийский Союз: вопросы международных отношений. 2024. № 5.
31. **Шавлохов А.К., Максименко Д.И.** Актуальные вопросы обеспечения информационной безопасности населения в условиях военных конфликтов: правовые аспекты // Региональное и муниципальное управление: вопросы политики, экономики и права. 2023. № 3.
32. Электронный фонд правовых и нормативно-технических документов / Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // https://docs.cntd.ru/document/902289626.

D.YU. KOCHERINSKII
Master's degree in politics from School
of Governance and Politics, MGIMO University,
Moscow, Russia

RUSSIA'S FOREIGN POLICY IN THE FIELD OF INFORMATION SECURITY: REGIONAL DIMENSION

This article analyzes the main directions of cooperation between the Russian Federation and other countries in the field of cybersecurity at the regional level. Despite facing growing resistance from the West in recent years, Russia continues to maintain its foreign policy initiative in this area within such formats as the SCO, BRICS, CIS, and CSTO, as international cooperation remains a reliable tool for solving global problems. The methodology of this work is comprehensive nature, as it uses a historical narration with a thematic analysis of current and controversial issues; an analysis of the regulatory framework, which allows us to study how the information sphere is regulated; and a qualitative analysis to identify trends. The results of the work are both theoretically and practically significant, as the work attempts to collect, summarize, and analyze available information on the research topic. Based on the results of the work, the author concludes that Russia takes a cooperative approach to ensuring international information security, and the effectiveness of regional cooperation can be seen in the voting on initiatives proposed by Russia at the UN General Assembly.

Key words: *international information security, SCO, BRICS, CIS, CSTO, cooperation, security threats.*