УДК 349

ОСНОВНАЯ РОЛЬ БРИКС, КАК МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ, В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Владислав Сергеевич Сахаров,

ФГБОУ ВО «РЭУ им. Г.В. Плеханова»

Научный руководитель: ***Галина Петровна Лозовицкая, Док-р юрид.наук, доцент,***

профессор кафедры государственно-правовых и уголовно-правовых дисциплин

ФГБОУ ВО «РЭУ им. Г.В. Плеханова»,

г. Москва, Россия

Аннотация: В данной статье исследуется основная роль БРИКС (Бразилия, Россия, Индия, Китай и Южная Африка) в борьбе с киберпреступностью – в качестве международной организации. Автор анализирует стратегии и меры, предпринимаемые БРИКС для противодействия киберугрозам, а также роль организации в разработке международных норм и стандартов в области кибербезопасности. Исследование подчеркивает важность и роль БРИКС в борьбе с киберпреступностью и предлагает рекомендации по дальнейшему развитию сотрудничества в этой области.

Ключевые слова: кибербезопасность, защита данных, персональная информация, киберпреступность, международная киберпреступность, киберугрозы,Россия, БРИКС.

The main role of BRICS as an international organization in the fight against cybercrime

V. S. Sakharov

Scientific supervisor: ***G. P. Lozovitskaya***, Professor, Doctor of Sciences, Associate Professor

PLEKHANOV Russian University of Economics, PLEKHANOV Russian University of Economics, Moscow, Russia

Abstract: This article explores the main role of the BRICS (Brazil, Russia, India, China and South Africa) in the fight against cybercrime as an international organization. The author analyzes the strategies and measures taken by BRICS to counter cyber threats, as well as the role of the organization in the development of international norms and standards in the field of cybersecurity. The study highlights the importance and role of BRICS in the fight against cybercrime and offers recommendations for further development of cooperation in this area

Keywords: *cybersecurity, data protection, personal information, cybercrime, Russia.*

Кибербезопасность БРИКС — это международная межправительственная - экономическая деятельность организации, которая объединяет крупнейшие развивающиеся экономики, такие как Бразилия, Россия, Индия, Китай и Южная Африка. Помимо геополитики, в центре внимания группы находится экономическое сотрудничество и расширение многосторонней торговли и развития.

В 2023 году был проведен 15-й саммит БРИКС, который был посвящён принятию в блок возможных новых членов, поскольку в преддверии саммита более 40 стран выразили заинтересованность в присоединении к БРИКС, около 20 из них официально обратились с просьбой о приеме. И по итогам этой встречи был подписан документ – Йоханнесбургская декларация-II. Где помимо одобрения, озвученного еще на саммите президентом Южной Африки Сирилом Рамафоса, который объявил, что Аргентине, Египту, Эфиопии, Ирану, Саудовской Аравии и Объединенным Арабским Эмиратам было предложено присоединиться к блоку, был так же декларированы вопросы связанные с кибербезопасностью. Развитие информационного пространства, а также процесс цифровизации экономики, в том числе в области хранения гражданских и правительственных данных обосновывает стремление БРИКС сотрудничать в области политики кибербезопасности, что можно проследить с

принятой в 2013 г. Этеквинской декларации и Плана действий на закрытии саммита БРИКС в Дурбане, Южная Африка, в которых впервые была заявлена необходимость «вносить вклад в мирное, безопасное и открытое киберпространство и участвовать в нем» и содержался призыв к разработке «общепринятых норм, стандартов и практик»[5, с. 4].

Следующим важным этапом работы в области кибербезопасности и защиты цифрового пространства стали положения Уфимской декларации 2015 года по итогам 7-го-го саммита БРИКС, организованного Россией, лидеры учредили «Рабочую группу экспертов государств БРИКС по безопасности при использовании ИКТ» с мандатом, среди прочего, «развивать практическое сотрудничество друг с другом для решения общих проблем безопасности при использовании ИКТ» [4, с. 6]. Также в том же году министры ИКТ стран БРИКС подписали Меморандум о взаимопонимании по сотрудничеству в области науки, технологий и инноваций с целью развития сотрудничества в этих областях. За этими событиями последовало несколько конкретных результатов [2, с. 7], включая Цифровое партнерство БРИКС, Партнерство БРИКС по новой промышленной революции (PartNIR), Инновационную сеть БРИКС (iBRICS Network) и Институт сетей будущего БРИКС – все это способствовало построению расширенного процесса сотрудничества, сочетающего политические, технологические и исследовательские инициативы[1, с. 21].

Как было сказано выше на 15 саммите так же большое внимание было уделено кибербезопасности. Йоханнесбургская декларация-II постулирует следующие положения, в частности в пункте 23 говорится о том, что БРИКС признает «огромный потенциал информационно-коммуникационных технологий (ИКТ) для роста и развития», но то же осознаёт «связанные с ними существующие и новые возможности для преступной деятельности и угроз и выражаем обеспокоенность растущим уровнем и сложностью использования ИКТ в преступных целях». [3, с. 6]. В этом же пункте отмечается что

международная организация поддерживает «работу, ведущуюся в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях», помимо этого, говорится, что они подтверждают свою совместную деятельность «в реализации мандата».

24 пункт на наш взгляд наиболее полно показывает значимость кибербезопасности для БРИКС. ИКТ используются для экономических, социальных и межличностных транзакций и взаимодействий. И для этого необходимо создание безопасного пространства с использованием новейшей технической. Создание безопасного пространства для информационно-коммуникационных технологий необходимо по следующим причинам:

1. Защита данных: Безопасное пространство обеспечивает защиту конфиденциальности, целостности и доступности данных, предотвращая несанкционированный доступ, изменение или уничтожение информации.

2. Предотвращение кибератак: Безопасное пространство помогает предотвратить кибератаки, такие как взломы, вирусы, фишинг и другие виды злоумышленной деятельности, защищая информацию и системы от вредоносного программного обеспечения и несанкционированного доступа.

3. Защита личной информации: Безопасное пространство обеспечивает защиту личной информации пользователей, такой как пароли, финансовые данные и другая чувствительная информация, предотвращая ее утечку или злоупотребление.

4. Обеспечение надежности и непрерывности работы: Безопасное пространство помогает обеспечить надежность и непрерывность работы информационных систем, предотвращая сбои, потерю данных и проблемы с доступностью.

5. Защита от нарушений законодательства: Безопасное пространство помогает предотвратить нарушения законодательства в области информационной безопасности, такие как несанкционированный доступ к

данным, кража интеллектуальной собственности или нарушение авторских прав.

Все эти меры способствуют обеспечению доверия пользователей и сохранению стабильности и безопасности информационно-коммуникационных технологий.

Так рассматриваемый пункт отражает намерение глав государств БРИКС, создать общепризнанные нормативно-правовые рамки в этой области. Создание единого правового пространства для кибербезопасности имеет несколько важных целей:

1. Унификация норм и стандартов: Единое правовое пространство позволяет разработать и принять общепризнанные нормы и стандарты в области кибербезопасности. Это способствует упорядоченному и согласованному подходу к защите информации и киберинфраструктуры в различных странах и регионах.

2. Сотрудничество и координация: Единое правовое пространство способствует сотрудничеству и координации между государствами в области кибербезопасности. Оно позволяет обмениваться информацией о новых угрозах, атаках и методах защиты, обучать специалистов, проводить совместные учения и оперативные мероприятия.

Все это будет являться современными решениями по борьбе с киберпреступлениями. Но поскольку на данный момент еще не существует подобной единой системы, необходимо проанализировать нормативную базу каждого государства члена БРИКС и понять, насколько эти методы эффективны.

1.Бразилия. Киберпреступность регулируется законом 12.737/2012, уголовным кодексом, Законом о защите детей (8069/1990), Законом Marco Civil da Internet (12.965/2014) и Законом о защите данных (13.709/2018). Закон 12.735 /2012 регулирует создание полицейских подразделений, расследующих киберпреступности.

2. Россия. Глава 28 «Преступления в области компьютерной информации» Уголовного кодекса Российской Федерации.

3. Индия. Основным законом Индии, специально регулирующим киберпреступность, является Закон об информационных технологиях (поправка) Закон 2008 года. Однако другие законы также включают соответствующие разделы, такие как, например, Закон об авторском праве 1957 года и Закон о защите детей от сексуальных преступлений (поправка) Закон 2019 года. Кроме того, продолжают применяться Уголовный кодекс Индии и Индийский закон о доказательствах 1872 года.

4. Китай. Киберпреступность в Китае регулируется рядом законов и политик на следующих уровнях: Законы и решения национального уровня:

- статьи 253-1, 285, 286, и 287 Уголовного кодекса (1997)
- Поправки VII (2009) и IX (2015) к Уголовному законодательству
- Решение Постоянного комитета Всекитайского собрания народных представителей о сохранении безопасности компьютерных сетей (2000)
- Решение Постоянного комитета Всекитайского собрания народных представителей об усилении защиты информации в сетях (2012)
- Закон Китайской Народной Республики о борьбе с терроризмом (2015)
- Закон Китайской Народной Республики о кибербезопасности.

5. Южная Африка. Закон об электронных коммуникациях и транзакциях № 25 от 2002 года регулирует ряд киберпреступлений. Законопроект о киберпреступлениях (2017).

Данные законы способствуют повышению эффективности борьбы с киберугрозами, обеспечению безопасности информации и киберинфраструктуры, а также защите прав и свобод граждан в киберпространстве.

Кроме этого, следует учитывать и необходимость защиты прав детей [6, с. 4], многие проблемы регулирования искусственного интеллекта [7, с. 517-521].

В целом законы имеют схожие черты, но также есть и различия. Каждая из стран делает планомерные шаги в сторону развития своего законодательства под изменяющуюся реальность. Растущая статистика киберпреступности демонстрирует недостаточную эффективность механизмов борьбы с киберпреступностью, поскольку трансграничный характер высокотехнологичных преступлений делает невозможным эффективную борьбу с ними только в рамках национальных правовых систем. Вот почему очень важно, что Государства начали процесс сотрудничества в рамках различных международных организаций для противодействия угрозам, создаваемым новейшими технологиями.

Литература

1. Belli, Luca, ed. CyberBRICS: Cybersecurity regulations in the BRICS countries. Springer Nature, 2021.

2. Belli, Luca. «Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation.» The African Journal of Information and Communication 28 (2021): 1-14.

3. Йоханнесбургская декларация-II. БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности, Сэндтон, Гаутенг, ЮАР, 23 августа 2023 года URL: https://www.mid.ru/ru/foreign_policy/news/1901504/ (дата обращения: 08.09.2023).

4. Уфимская декларация// VII саммит.- 2015 URL: http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf (дата обращения: 10.09.2023).

5. Этеквинская декларация и Этеквинский план действий // V саммит.- 2013 URL: http://www.kremlin.ru/supplement/1430 (дата обращения: 08.09.2023).

6. Лозовицкая, Г. П. Безопасность детей и подростков в киберпространстве / Г. П. Лозовицкая // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы (к 20-летию образования Московского университета МВД России имени В.Я. Кикотя) : Сборник научных трудов Международного форума, Москва, 25 марта 2022 года / Сост. В.В. Бушуев. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. – С. 194.

7. Лозовицкая, Г. П. Искусственный интеллект: правовые проблемы использования / Г. П. Лозовицкая, Л. В. Маринкина // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года / Под общей редакцией И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020. – С. 517-521.