Манойло А.В., Лавринов Б.Б.

Основные принципы и направления формирования пространства коллективной информационной безопасности стран БРИКС: российский подход

Аннотация: Настоящая статья посвящена исследованию принципов, направлений, форм и методов формирования единого пространства коллективной безопасности стран БРИКС в информационной сфере. Цель создания такого пространства коллективной безопасности – совместное противодействие новым вызовам и угрозам в информационной сфере, таким как киберпреступность, информационный терроризм и экстремизм, операции информационной войны, с которыми каждая из входящих в БРИКС стран в отдельности на сегодня не справляется. Основанием для создания такого пространства и системы, обеспечивающей его информационную безопасность на уровне, отвечающего национальным интересам стран БРИКС, является общая для всех указанных стран потребность в противодействии транснациональной киберпреступности и в отражении операций информационной войны, организуемых зарубежными противниками и конкурентами БРИКС. Решение данной задачи автор видит в формировании системы наднациональных органов БРИКС, отвечающих за обеспечение информационной безопасности объединения в целом и за отражение операций информационной войны. В этом плане такая система органов может быть организована, используя опыт создания и… функционирования органов Европейского союза.

Манойло Андрей Викторович – доктор политических наук, профессор факультета политологии МГУ имени М.В. Ломоносова.

Лавринов Борис Борисович – аспирант кафедры российской политики факультета политологии МГУ имени М.В. Ломоносова.

1. Информационная безопасность. Понятие и ключевые тренды

Обеспечение информационной безопасности любого государства в современном мире находится в прямой зависимости от наличия высокоразвитой и конкурентоспособной информационно-коммуникативной инфраструктуры.

Информационно-коммуникативная инфраструктура государства

подразумевает под собой наличие двух составляющих: технологической и смысловой (содержательной).

Технологическая (кибер) составляющая национальной информационно-коммуникативной инфраструктуры представляет собой совокупность информационных систем, подсистем и центров, баз знаний и данных, систем связи, центров управления, средств и технологий сбора, хранения, обработки и передачи информации и т.д. Таким образом, кибер-безопасность государства подразумевает под собой наличие таких организационных мер и структур как: национальные системы спутниковой связи, навигации и вещания, национальная система платёжных карт, национальные базы данных и знаний, государственные системы защиты и блокировки информации, национальные поисковые системы и т.д. Следует отметить, что список требований, предоставляемых к высокоразвитым информационно-коммуникативным инфраструктурам с каждым годом становится всё более и более обширным.

Состояние информационно-коммуникативной инфраструктуры и информационной индустрии государства в реалиях глобального информационного общества является важнейшим условием успешности реализации внутренней политики. Однако процесс информатизации в разных государствах неравномерен, что приводит к существованию такого феномена как «цифровая асимметрия». «Цифровая асимметрия» заключается в неравномерности распределения информационных ресурсов между различными государствами и, как следствие, неравномерных возможностях использования глобального информационного пространства. В связи с этим борьба за информационные ресурсы и информационное пространство между государствами приобретает принципиально важное значение.

Не менее значимой для вопроса информационной безопасности является и смысловая (содержательная) сторона информационно-коммуникативной инфраструктуры государства. Если говорить упрощённо, она представляет собой тот посыл (контент), который транслирует государство в общество и/или международное сообщество посредством наличествующих у него информационно-коммуникативных ресурсов. Также к содержательной стороне обеспечения информационной безопасности относятся вопросы её концептуального и стратегического оформления и нормативно-правового регулирования.

Из системной сложности и разветвлённости информационно-коммуникативной инфраструктуры государства логически проистекает идея формирования единого пространства информационной безопасности в наднациональных рамках международных интегративных организаций с участием России (БРИКС, ЕАЭС), что, с одной стороны, позволит соединить самые передовые технологии стран-участниц, произвести обмен бесценным опытом в сфере обеспечения информационной безопасности, снизить ресурсные затраты и издержки каждой отдельной страны, а с другой стороны, может стать

рупором развития единого информационного пространства в рамках которого будут функционировать смыслы и ценности общие для государств объединения, будет производиться культурный и символический обмен между различными обществами, усилиться сотрудничество в различных областях экономики за счёт её высокой информатизации, станет возможно формирование, например, единой платёжной системы и в отдалённой перспективе – даже единого рынка товаров и услуг.

2. Актуальные вызовы и угрозы информационной безопасности РФ

1.Ослабление международного авторитета России за счёт вытеснения её с внешнего информационного рынка;

2.Формирование негативного имиджа России на международной арене;

3. Ослабление интеграционных процессов с участием России (БРИКС, СНГ, ЕАЭС);

4.сФормирование информационной зависимости российского общества, заключающейся в доминировании на внутреннем рынке и рынках стран-партнёров зарубежных систем спутниковой связи, навигации, вещания и платежей;

5. Информационное воздействие на российское общество и общества стран ЕАЭС, СНГ и БРИКС с целью формирования негативного образа России и соответствующих моделей политического поведения граждан данных стран в её отношении;

6. Усиление интеграционных процессов, связанных с противодействием России ряда государств на международной арене;

7. Формирование зависимости России от импорта высоких технологий;

8. Усиление информационного влияния на территории России, а также стран СНГ и ЕАЭС международных террористических организаций;

9.Разработка рядом государств концепций информационных и гибридных войн, направленных против России и её партнёров;

10. Потенциальная угроза вторжения ряда стран и террористических организаций в информационное пространство России и её партнёров, а также нарушение нормального функционирования национальных информационных и телекоммуникационных систем России, стран БРИКС, СНГ и ЕАЭС.

11. Угроза возрастания уровня кибер-преступности на территориях России и её партнёров;

12. Формирование новых угроз, связанных с феноменами «Интернета вещей» и технологиями Big Data, к которым Россия может быть технологически не готова.

3. Актуальное состояние информационно-коммуникативной инфраструктуры Бразилии

Бразилия озаботилась отстаиванием собственного информационного

суверенитета **в 2013 г.** после публикации доклада Э. Сноудена о слежке различных ведомств США за её гражданами в Интернете. **В апреле 2014 г. Парламент Бразилии утвердил так называемый «Билль Марко», более известный как «Интернет-конституция»**, основное содержание которого посвящено декларированию прав и свобод личности в интернет-пространстве, а также мерам и механизмам их соблюдения. В том же году Бразилия начала реализацию ряда мероприятий, направленных на собственное технологическое обеспечение интернет-коммуникаций в рамках своих национальных границ. Например, государственные служащие Бразилии отказались от использования американских поставщиков услуг электронной почты и перешли на бразильские.

В 2015 г. в Бразилии начата реализация крупномасштабного **проекта по прокладыванию интернет-кабеля из Европы в Бразилию по дну Атлантического океана в обход США**, в дальнейшем планируется также соединение Бразилии Африкой и Азией. **17 февраля 2017 г.** бразильское правительство заявило о необходимости создания **кибер-полиции**, ответственной за предотвращение кибер-преступлений (незаконное использование персональных данных, кибер-шпионаж, кибер-терроризм и т.д.)

Таким образом, в настоящий момент наибольшее внимание в области кибер-безопасности в Бразилии уделяется защите государственно значимых данных, важных инфраструктурных объектов, персональных и банковских данных. Особую значимость для Бразилии приобретает вопрос собственной создания информационно-коммуникативной инфраструктуры, независимой от США и американских IT-компаний. Однако по состоянию на 2017 г. в Бразилии существует ряд сложностей в реализации собственных IT-проектов, связанных с безусловным **лидерством американских компаний на внутреннем рынке IT**, технологическим отставанием от ведущих в области информационных технологий держав и недостаточной ресурсной обеспеченностью.

4. Актуальное состояние информационно-коммуникативной инфраструктуры Индии

На сегодняшний день **Индия** занимает одно из лидирующих мест в мире по числу кибер-преступлений, хакерских атак и распространения вредоносного ПО. Соответственно, вопрос формирования пространства информационной безопасности для данной страны является отнюдь не праздным.

В 2012 г. индийским правительством был утверждён пятилетний план «по повышению уровня информационной безопасности учреждений критически важной инфраструктуры на территории всей страны». В рамках данного плана предполагалось претворение в жизнь следующих мер: создание ведомства быстрого реагирования на кибер-угрозы, создание национальной операционной системы, полное обеспечение информационно-коммуникативной безопасности правительственных структур, создание

национальных баз данных и знаний, использование биометрических технологий для получения доступа гражданами к сети Интернет и осуществления финансовых онлайн-операций.

В 2013 г. индийское правительство предприняло ряд решительных мер по созданию национального пространства информационной безопасности: был создан **Национальный центр защиты критически важной инфраструктурной информации, учреждена полиция по кибер-безопасности**. **В 2014 г.** при канцелярии кабинета министров была учреждена **должность координатора по вопросам национальной кибер-безопасности**. Для индийского правительства деятельность в области построения национальной системы кибер-безопасности усложняется **фактическим нахождением Индии в состоянии открытой информационной войны с Пакистаном**.

В 2016 г. после информационной атаки пакистанской хакерской группировки «Легион» при Министерстве электроники и информационных технологий были созданы сразу несколько агентств**: Национальная организация технических исследований, Национальная разведывательная сеть и Национальный информационный совет**.

В феврале 2017 г. Команда при правительстве Индии по реагированию на чрезвычайные ситуации запустила проект «Cyber Swachha Kendra», рассчитанный на усиление мер мобильной безопасности. Декларируемыми целями проекта являются защита мобильных информационных систем и данных, а также информирование граждан по вопросам личной кибер-безопасности.

Таким образом, меры, предпринятые правительством Индии за последние 5 лет, существенным образом помогли снизить уровень внутренней кибер-преступности, однако, проблемы **кибер-шпионажа и кибер-терроризма** (в первую очередь со стороны Пакистана) остаются актуальными для Индии и по сей день. По данным **на 2017 г.** в **рамках Индекса Кибер Безопасности ООН Индия занимает 23 место**, существенно уступая России (10) по ряду параметров.

5. Актуальное состояние информационно-коммуникативной инфраструктуры Китая

Китай по праву считается одним из государств-лидеров по части технологий национальной информационной и кибер-защиты, направленных на контроль и регулирование интернет-пространства на своей территории. **С 1998 г. в рамках общего проекта «электронного правительства» в Китае существует 12 так называемых «золотых проектов», направленных на регулирование интернет-пространства.**

Наиболее известным из таковых проектов является **проект «Золотой**

щит», представляющий собой систему фильтрации содержимого интернета за счёт ограничения доступа к ряду ресурсов и страниц на территории КНР. Проект «Золотого щита» является примером обеспечения содержательной стороны пространства информационной безопасности, к запрещённым сайтам относятся: сайты с некорректной политической тематикой, сайты с критикой в адрес правительства, порнографические сайты, сайты, не удовлетворяющие требованиям китайского законодательства. На данный момент «Золотой щит» использует следующие методы фильтрации: Блокировка IP-адресов, фильтрация DNS-запросов и их переадресация, блокировка интернет-адресов (URL), фильтрация на этапе пересылки пакетов, блокировка соединений, осуществляемых через VPN.

Помимо блокировки нежелательных ресурсов и контента действующее законодательство КНР предусматривает следующие меры ограничений на использование интернета: ручное отслеживание контента в социальных сетях интернет-полицией, пользовательская цензура блоговых платформ.

В 2016 г. китайским парламентом был принят соответствующий закон, согласно которому в Китае планируется создание полицейских подразделений, которые будут заниматься обеспечением кибер-безопасности, планируется создание системы контроля за поставщиками ПО для значимых инфраструктурных объектов, а также усиление контроля за деятельностью иностранных компаний в Интернете, в частности, компании обязуются предоставлять ключи шифрования собственных данных, а провайдеры – хранить все пароли пользователей и также передавать их властям по первому требованию.

Борьба с кибер-терроризмом и кибер-шпионажем в Китае осуществляется за счёт деятельности десятого (сбор научно-технической информации) и одиннадцатого (радиоэлектронная разведка и компьютерная безопасность) бюро **министерства государственной безопасности КНР**, подчиняющегося КПК.

В **2000 г.** руководство **Народно-освободительной армии Китая** разработало **Программу модернизации средств информационной войны**. В рамках данной программы были запущены проекты модернизации радиоэлектронной разведки и контрразведки. Ещё в середине 90х-гг. КНР были введены в эксплуатацию 4 новых центра радиоразведки и Тихом Океане, а в 1999 г. на Кубе был развёрнут китайский центр радиоперехвата.

Таким образом, с точки зрения противодействия информационному влиянию и кибер-шпионажу Китай занимает одно из лидирующих мест в мире. Китайский опыт показывает, что предупредительные меры борьбы способны нивелировать угрозу вторжения контрагентов в пространство информационной безопасности и информационного суверенитета государства. Однако по данным **Индекса Кибер Безопасности 2017 г.** Китай располагается лишь на 32 месте, существенно уступая и Сингапуру (1), и США (2) и России (10), что во многом

обуславливается наличием в данном Индексе критерия безопасности персональных данных граждан.

6. Актуальное состояние информационно-коммуникативной инфраструктуры ЮАР

Меры, предпринимаемые правительством **ЮАР** в рамках обеспечения национальной информационной безопасности, можно условно разделить на несколько основных групп: технологическое и ресурсное обеспечение равного доступа всех граждан страны к информации, противодействие кибер-преступлениям, создание предупреждающих механизмов защиты от потенциальных информационных атак и применение биометрических технологий для осуществления финансовых операций частными лицами в Интернете.

В 2010 г. в ЮАР впервые были созданы специальные подразделения полиции по борьбе с кибер-преступлениями, деятельность которых направлена на предотвращение и отслеживание экономических кибер-преступлений и кибер-преступлений против личности и значимых государственных инфраструктурных объектов.

В конце 2016 г. правительством ЮАР был издан «Билль о киберпреступлениях и кибербезопасности», поставивший первоочередной задачей в рамках постепенной информатизации общества создание пространств общенациональной и личной информационной безопасности. Согласно данному Биллю в **2017 г. в ЮАР был создан Центр Кибербезопасности при Национальном Университете Йоханнесбурга при содействии правительства Республики**. Данный центр занимается подготовкой профессиональных кадров, созданием нормативно-правовых основ регулирования информационного пространства ЮАР, информационно-технической подготовкой деятельности правительственных органов в данной сфере, а также научными исследованиями по вопросам кибер и информационной безопасности.

6 сентября 2017 г. между Россией и ЮАР было подписано **Соглашение о сотрудничестве в области кибербезопасности**. На сегодняшний день, согласно Индексу Кибербезопасности, для ЮАР являются чрезвычайно актуальными проблемы экономических кибер-преступлений, технологической зависимости, недостаточности ресурсной обеспеченности и нормативно-правовой базы. Сотрудничество с Россий в данной области является явным доказательством существующего запроса в южноафриканском обществе на обеспечение информационной и кибер безопасности.

7. Перспективные направления деятельности для РФ в рамках создания пространства коллективной безопасности БРИКС

1. Сотрудничество в области IT- технологий с компаниями стран-

участниц БРИКС, реализация совместных проектов.

2. Создание единой системы предупредительных мер противодействия кибер-преступлениям, международному терроризму в Интернете и информационным атакам.

3. Создание программных документов в области обеспечения коллективной информационно-коммуникативной безопасности: концепции информационной безопасности, стратегий коллективного противодействия информационным и гибридным войнам, имиджевой стратегии и т.д.

4. Сотрудничество в области обмена информацией и обеспечения равного доступа к информации всех граждан членов-государств БРИКС.

5. Обеспечение возможностей сотрудничества между ведущими СМИ стран-участниц БРИКС.

6. Обеспечение доступа аудитории стран-участниц БРИКС к российским информационным ресурсам и телеканалам (1 канал, Russia Today и т.д.) на русском и национальных языках.

7. Создание возможностей приоритетного доступа РФ к информационному пространству стран-участниц БРИКС. Например, точечное проникновение российских ресурсов и компаний под «Золотой щит».

8. Создание ряда совместных инфраструктурных проектов. Например, единой платёжной системы стран-участниц БРИКС, единых систем поиска и навигации.

9. Проведение совместных информационных и имиджевых компаний странами-участницами БРИКС в рамках позиционирования на международной арене.

10. Создание единых медиа: агентств новостей, телеканалов, периодических изданий, информационных онлайн-ресурсов и т.д.

8. «Дорожная карта» создания пространства информационной безопасности БРИКС.

1. Создание рабочей группы по разработке организационной структуры и нормативно-правовой базы проекта коллективной информационной безопасности БРИКС;

2. Подписание Договора Сотрудничества в области коллективной информационной безопасности странами БРИКС;

3. Разработка на основании договора нормативных, организационных, концептуальных и стратегических оснований реализации проекта;

4. Создание инфраструктуры для обеспечения функционирования подразделений пространства информационной безопасности БРИКС;

5. Формирование организационной структуры коллективной информационной безопасности БРИКС и её подразделений;

6. Создание «кибербаз» БРИКС и территориальных структурных подразделений во всех станах-членах организации.

9. Организационная структура пространства коллективной информационной безопасности БРИКС.

1. Совет коллективной информационной безопасности БРИКС призван явиться центральным концептуальным и стратегическим органом. В состав совета следует включить высших должностных лиц, руководящих вопросами развития ИКТ и информационной безопасности в соответствующих странах- участницах объединения.

2. Центр обеспечения кибербезопасности БРИКС будет заниматься технологическим обеспечением единого киберпространства, стратегическим планированием операций, предупреждением кибератак и оперативным реагированием на них. В качестве одного из подразделений данного центра предлагается создание киберполиции БРИКС.

3. К основным сферам ведения Центра информационной политики и Коммуникаций БРИКС будут относиться вопросы совместных информационных и имиджевых кампаний, международного сотрудничества, внутренних коммуникаций и связей с общественностью.