М.М. Кучерявый

Роль России и евразийского региона в формировании глобального подхода к обеспечению международной информационной безопасности

Role of Russia and the Eurasian region in formation of a global approach to ensuring the international information security

Аннотация: Прозрачность государственных границ для информационных потоков ведет к возникновению принципиально новой ситуации, связанной с обеспечением национальной безопасности. Автор считает, что отсутствие комплексной всесторонней защищенности информационного пространства государства может привести к значительному ограничению его суверенитета и существенному ослаблению позиций страны на мировой арене. Анализируются принципы и методы обеспечения информационной безопасности и другие важнейшие аспекты, способные сыграть стабилизирующую роль в современной системе международных отношений.

Summary: Transparency of frontiers for information streams conducts to emergence of essentially new situation connected with ensuring of national security. The author of article offered the reader considers that lack of complex all-round security of information space of the state can lead to considerable restriction of its sovereignty, and essential weakening of the position of the country on the world scene. Principles and methods of ensuring information security and other major aspects, capable to play stabilizing role in modern system of the international relations are analyzed.

Ключевые слова: Россия; Евразийский регион; СНГ; международная информационная безопасность.

Keywords: Russia; Eurasian region; CIS; international information security.

Кучерявый Михаил Михайлович
Санкт-Петербург,
Российская Федерация
Руководитель Управления
Федеральной службы
по техническому и экспортному
контролю по Северо-Западному
федеральному округу,
кандидат политических наук
pikestaff@yandex.ru

Kucheryaviy Mikhail Mikhaylovich
St. Petersburg,
The Russian Federation
The chief of the department of
Federal service on technical and
export control,
candidate of political sciences
pikestaff@yandex.ru

Начало XXI века характеризуется высокой динамикой геополитических изменений глобального и регионального масштаба. Глубокий кризис мировой экономики, возникший в 2008 году и приход второй волны которого становится все более реальным в наши дни, оказывает негативное влияние на жизнедеятельность всего международного сообщества. В этой ситуации усиливается неопределенность перспектив развития геополитических процессов, создаются условия для кардинальной трансформации всего существующего миропорядка.

В комплексе социально-политических проблем, стоящих перед Россией, важнейшее место занимает задача обеспечения безопасности страны. Одним из условий процветания нации является способность государства предупредить и сдержать агрес-



сию, а в случае необходимости защитить интересы общества и личности. Среди концептуальных вопросов обеспечения безопасности России ключевое место занимает необходимость достижения баланса между выявленными угрозами и степенью защищенности государства [12]. Реалиями международной жизни является возникновение новых очагов напряженности и обострение старых конфликтов в разных частях мира. Вместе с тем, отличительной чертой современных войн и вооруженных конфликтов стала их информационная составляющая, которая проявляется в виде противоборства в информационной сфере [6]. В данной связи все большее значение приобретает обеспечение информационной безопасности российского государства.

Под информационной безопасностью понимают состояние защищенности информационной среды. В данной связи защита от информационной агрессии представляет собой деятельность по противодействию информационной агрессии, направленной на достижение политических целей, которые агрессор стремится достигнуть как с помощью военных, так и пропагандистских средств.

В настоящее время США развернули глобальную борьбу за общественное сознание мирового сообщества. Эта борьба ведется на основе координации деятельности всех государственных и коммерческих структур, с применением во всемирном масштабе самых современных информационных технологий. В то же время глобальному расширению и качественному преобразованию информационного противоборства способствовало формирование единого мирового информационного пространства.

В наши дни мировые державы развернули информационное противоборство, которое приобрело геостратегический характер. Цель такого противоборства – достижение превосходства в мировом информационном пространстве. Данное превосходство планируется использовать в борьбе за изменение глобального баланса сил и сложившегося мирового порядка. В настоящее время наиболее развитые страны располагают мощными информационными ресурсами, которые при их успешном применении могут сыграть важную роль в достижении глобальных политических целей, повлиять на развитие международных процессов в различных регионах мира. Сегодня информационные войны представляют собой «игру без правил», так как сейчас не существует общепризнанных международно-правовых норм и правил его ведения.

Стало очевидным, что прозрачность государственных границ для информационных потоков ведет к возникновению принципиально новой ситуации для обеспечения национальной безопасности. Отсутствие комплексной всесторонней защищенности информационного пространства государства может привести к значительному ограничению его суверенитета и существенному ослаблению позиций страны на мировой арене.

Первый опыт ведения информационного противоборства был приобретен в войне в зоне Персидского залива в 1991 году. Тогда многонациональные силы, используя методы радиоэлектронного и огневого противодействия, осуществили блокирование практически всей информационной, в том числе и военной системы Ирака. Этот успех не только позволил осмыслить роль информационного противоборства, но и заставил задуматься над тем, как выйти из подобного положения, если такое противоборство будет навязано им самим.

В США были проведены аналитические исследования и эксперименты под руководством Агентства информационной безопасности Министерства обороны, которые показали, что степень уязвимости компьютерных систем и баз данных военного ведомства США достаточно высока. Проникнуть в мозговой центр Пентагона оказывается несложно, так как он имеет множество различных выходов в другие информационные системы как внутри государства, так и за его пределами.

В настоящее время можно достаточно легко нарушить работу информационных сетей индустриально развитого государства через каналы Интернета. Здесь в качестве примера могут служить мощные запланированные атаки компьютерных хакеров на сайты ряда крупных американских компаний или правительственные сайты Эстонии сразу после демонтажа памятника «Воина-освободителя». Было продемонстрировано хакерское превосходство над профессионалами, обеспечивающими электронную безопасность авторитетных сайтов. Следует обратить внимание, что никакого взлома серверов не было, система безопасности нигде не нарушалась, однако в США это впервые оценили как «кибертерроризм». Значение сетей Интернета в развитых странах уже сейчас настолько велико, что малейшее посягательство на их неприкосновенность расценивается как жизненная угроза безопасности страны [10]. В составе военно-воздушных сил США даже было образовано новое киберкомандование, где будут создаваться, тренироваться и снаряжаться силы для проведения длительных глобальных операций в киберпространстве и посредством киберпространства, полностью интегрированных с воздушными и космическими операциями [11].

Доступность глобальной компьютерной сети позволяет передавать необходимую информацию в любой регион мира и выполнять многие задачи, связанные с информационным противоборством. Не исключено, что в рамках информационного противоборства самостоятельное развитие может получить кибернетическая борьба, в ходе которой будут наноситься мощные информационные удары по интегрированным компьютерным системам противника. Может осуществляться информационное вторжение с целью нарушить системы его жизнеобеспечения, электро-, газо-, водоснабжение, нарушение системы связи, движения транспорта, срыв финансовых операций и т.п.

В качестве одного из ключевых аспектов противостояния в рассматриваемой сфере выступает информационная война. Под ней понимается «противоборство между государствами в информационном пространстве с целью нанести ущерб информационным системам, процессам и ресурсам, критически важным структурам (информационно-техническая война), подрыва политической и социальной систем, а также массированной психологической обработки личного состава войск и населения с целью дестабилизировать общество и государство (информационно-психологическая война)» [1].

При этом информационная война рассматривается не как обособленные действия, а как интеграция всех форм и способов вооруженной борьбы, при которой происходит значительное сокращение привлекаемых сил и средств за счет повышения информационных возможностей.

Ее суть заключается в том, что войска достигают информационного превосходства, под которым понимается как поступление информации в большем количестве, так и более высокая степень доступа к ней более мелких звеньев системы и, как следствие, более глубокое понимание ситуации на поле боя. Это становится возможным в результате доступа географически разбросанных войск к единой информационной системе. При этом синхронизация их действий достигается уже не за счет централизованного управления, а за счет своевременной реакции этих войск на изменения обстановки.

Для лишения возможного противника заблаговременно накопленной информации, а также для минимизации наносимого в результате ведения разведки ущерба уже в мирное время должно осуществляться противодействие видовой и радиоэлектронной разведкам иностранных государств, которое ведется космическими и воздушными разведывательными системами и системами двойного назначения.

В 1992 году был принят Закон Российской Федерации «О безопасности». В соответствии с этим законом безопасность рассматривается как состояние защищенности



жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [4].

Термин «национальная безопасность» впервые использован в Федеральном законе «Об информации, информатизации и защите информации» 1995 года, а его определение дано в первом Послании Президента Российской Федерации Федеральному Собранию «О национальной безопасности» в 1996 году. В этом документе сказано: «Национальная безопасность понимается как состояние защищенности национальных интересов от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства».

Данное определение фактически идентично определению «безопасность» в Законе «О безопасности», поскольку совокупность жизненно важных интересов личности, общества, государства и составляет национальные интересы. К тому же основополагающий документ в этой области, впервые утвержденный Президентом Российской Федерации в 1997 году, а в новой редакции в 2000 году, называется Концепцией национальной безопасности Российской Федерации и ее структура полностью соответствует основным положениям Закона «О безопасности».

В соответствии с положениями существующей законодательной и нормативно-правовой базы определение понятия «национальная безопасность» выглядит следующим образом: национальная безопасность или безопасность нации есть защищенность жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внутренних и внешних угроз, обеспечивающая устойчивое поступательное развитие страны.

Поэтому закономерно определение и с ним можно согласиться, что «...безопасность – состояние защищённости от возможного нанесения ущерба, способность к сдерживанию или парированию опасных воздействий, а также к быстрой компенсации нанесённого ущерба. Безопасность означает сохранение системой стабильности, устойчивости и возможности саморазвития» [2].

Следует различать систему национальной безопасности и систему обеспечения национальной безопасности. Первая – это система взаимодействия интересов и угроз, а вторая – это функциональная система органов, сил, средств, различных организаций, призванных решать задачи по обеспечению национальной безопасности.

Необходимо отметить следующее. Широко используемая в исследованиях трактовка безопасности как защищенности достаточно обоснована, но следует иметь в виду, что защита – это лишь один из возможных, хотя и наиболее часто используемых, вариантов реагирования на угрозу. Безопасность всегда связана с защитой процесса реализации интересов, но характер интересов и процесс их реализации может быть наступательным или оборонительным. Это наглядно демонстрируют США, которые всегда наступательно продвигают и реализуют свои национальные интересы, а потому и деятельность по защите, охране этих интересов выглядит такой же активной и наступательной. Обеспечение безопасности является условием существования и развития личности, общества и государства, что и позволяет им сохранять накопленные духовные и материальные ценности. Критерием обеспечения безопасности (в самом общем смысле) можно считать определение пределов, рамок, границ политических, социальных, техногенных, природных явлений, превышение которых может нанести трудновосполнимый ущерб нации в настоящем и будущем.

Для того, чтобы дать определение информационной безопасности, необходимо уточнить классификационный признак деления национальной безопасности государства по видам.

Закон Российской Федерации «О безопасности» предусматривает деление национальной безопасности на следующие виды: государственную, экономическую, общественную, оборонную, информационную, эколо-

гическую и иные (ст. 13). Однако законодатели не дали ни строгого толкования принципов классификации по видам безопасности, ни определения этих понятий, что на практике привело к необоснованному дроблению родового понятия. В литературе и в средствах массовой информации можно встретить федеральную, конституционную, планетарную и т. д.

В качестве классификационных признаков должны быть выделены характер угроз и сферы жизнедеятельности. В зависимости от характера угроз, их источника, специфики можно выделить такие виды безопасности, как безопасность от угроз природного характера, безопасность от угроз антропогенного характера, безопасность от военных угроз, которые, в свою очередь, можно дробить на более мелкие виды безопасности от конкретных угроз. При этом под безопасностью от того или иного вида угроз понимается защищенность жизненно важных интересов государства от угроз данного вида.

В человеческом обществе жизненно важные интересы всех объектов безопасности подвергаются воздействию самых различных угроз, поэтому особую практическую значимость имеет подразделение видов безопасности по сферам или областям жизнедеятельности, в которых и проявляются эти угрозы. Именно по этому принципу классифицированы жизненно важные интересы, угрозы и направления обеспечения национальной безопасности в Концепции национальной безопасности Российской Федерации [5]. Наиболее обобщенно подобную классификацию можно ограничить выделением пяти видов безопасности, которые можно дробить на более мелкие виды безопасности по конкретным сферам жизнедеятельности. Это – социально-политическая, экономическая, военная, информационная и экологическая безопасность.

В качестве угроз в информационной сфере в рамках Концепции национальной безопасности России 2000 года рассматривается следующее: «Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним» [5].

На смену этому документу пришел новый, отражающий перемены, происходящие в международной системе и внутри страны. В 2009 году была принята Стратегия национальной безопасности России до 2020 года, которая отразила ключевые взгляды, в том числе на основные проблемы в информационной сфере: «Угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности» [13].

Довольно важным фактором было признано «…развитие общей гуманитарной и информационно-телекоммуникационной среды на пространстве государств–участников Содружества Независимых Государств и в сопредельных регионах» [13]. Информационные аспекты отмечены уже в каждой из сфер безопасности в качестве одних из ключевых.

В то же время на данный момент все еще действует Доктрина информационной безопасности 2000 года [3], оформленная в качестве надстройки вслед за принятием

базовой Концепции национальной безопасности, однако не получившая достаточной юридической силы. Дело в том, что Доктрина информационной безопасности, несмотря на развернутую программу действий по обеспечению безопасности страны в этой области, не получила возможности проведения ее в жизнь.

Наконец, в 2010 году вышел новый Федеральный Закон «О безопасности», который вновь если не расширил, то четко очертил вместе с другими сферами довольно четко и ясно и информационную область безопасности. Безусловно, эта законодательная инициатива была вызвана к жизни быстроменяющимися условиями, особенно внешнеполитического характера.

Для нашей страны очевидным направлением действий по обеспечению собственной информационной безопасности выступает выведение этого вопроса на международный уровень, где основу составляют наиболее востребованные в отечественной внешней политике международные структуры – Содружество Независимых Государств, Шанхайская организация сотрудничества и Организация Объединенных Наций.

Приоритет остается, естественно, за работой с ближайшими соседями на той территории, где уровень доверия максимально высок, ведь современная Россия достигла репутации весьма надежного исполнителя своих международных обязательств. Поэтому первые инициативы отрабатывались на странах СНГ, еще в 2006 году была принята Концепция формирования информационного пространства Содружества Независимых Государств, в которой недостаточно развернуто, но четко прописана необходимость коллективного обеспечения информационной безопасности [8]. Сам документ послужил лишь поводом к интенсификации работы в этом направлении на многостороннем уровне и подтолкнул к запуску следующего этапа.

Дальнейшие события привели к тому, что именно Евразийский регион и Российская Федерация выступили в качестве инициаторов перехода на новый уровень международного взаимодействия в области информационной безопасности. Через десять лет после запуска процесса по объединению усилий в области информационной политики в СНГ страны, увязывавшие свое участие в многосторонних межгосударственных институтах с повышением доверия в области границ, смогли подключить дополнительные ресурсы [7]. Все это выразилось в формировании в 2006 году Группы экспертов Шанхайской организации сотрудничества по международной информационной безопасности. Как и в случае с определением ключевых аспектов терроризма, ШОС в плане информационной безопасности задала тон глобальному сообществу [9]. С первых дней своей работы Группа экспертов привлекла внимание Генеральной Ассамблеи ООН. Этот шаг сблизил позиции по ключевым понятиям не только среди стран–членов ШОС, но и среди экспертов, представляющих отдаленные регионы.

Следующим этапом стало представление в 2010 году контактной группой из пятнадцати стран Генеральному секретарю ООН доклада, в котором впервые на столь высоком уровне говорилось о необходимости выработки общих подходов в борьбе с киберугрозами и признавалось, что угрозы эти могут исходить не только от преступников и террористов, но и от государств. В сентябре 2011 года этот этап дополнился новым шагом, выразившимся в обнародовании двух программных документов – «Правилах поведения в области обеспечения международной безопасности» и проекте конвенции ООН «Об обеспечении международной информационной безопасности».

Последнее заседание контактной группы прошло 8 июня 2012 года в Санкт-Петербурге, а этот год может стать завершающим для принятия нового международного документа, способного очертить основные категории (информационная война, информационная инфраструктура, информационное оружие, информационное пространство), принципы и методы обеспечения ин-

формационной безопасности и другие важнейшие аспекты, выработанные при непосредственном участии нашей страны и способные соизмерить и внести вклад в стабилизирующую роль в информационные аспекты современной системы международных отношений.

Использованная литература:

1. Война и мир в терминах и определениях. Под ред. Д.О. Рогозина. – М., 2004. – С. 75.

2. Война и мир в терминах и определениях. Под ред. Д.О. Рогозина. – М., 2004. – С. 20.

3. Доктрина информационной безопасности // Российская газета – [электронный ресурс]. – URL:www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm.

4. Закон Российской Федерации «О безопасности» // Ведомости Съезда народных депутатов и Верховного Совета Российской Федерации. – 1992. – № 15. – Ст. 769.

5. Концепция национальной безопасности Российской Федерации // Совет безопасности Российской Федерации. – 2000 г. – [электронный ресурс]. – URL: www.scrf.gov.ru/documents/1.html.

6. Косов Ю. В. Особенности геополитических процессов в Центральной Европе // Управленческое консультирование. − 2009. − № 3. − С. 91–97.

7. Косов Ю.В., Плотников В.А. На пути к новому партнерству в Евразии // Управленческое консультирование. – 2012.− № 1. − С. 223–226.

8. Косов Ю.В., Торопыгин А.В. Проблема безопасности государств – членов евразийского экономического сообщества // Управленческое консультирование. Актуальные проблемы государственного и муниципального управления. – 2005. − № 2. − С. 100–107.

9. Кучерявый М.М., Плотников В.А. Региональная модель формирования информационного общества (на примере Содружества Независимых Государств) // Евразийская интеграция: экономика, право, политика. – 2012. −№11.– С. 118–119.

10. Ноговицын А.А., Барвиненко В.В., Мушков Ю.И. Методика оценки и пути обеспечения военной безопасности государства // Вестн. Академии военных наук. – 2004. – № 1(6). – С. 115

11. Пентагон борется с виртуальными врагами – [электронный ресурс]. – URL: www.newsru.com/world/19sep2007/kiber.html.

12. Плотников В.А. Теоретико-концептуальные основы исследования международной безопасности в Азиатско-Тихоокеанском регионе // Известия Российского государственного педагогического университета им. А.И. Герцена: Аспирантские тетради. – 2008. − №27(61). − С. 202–205.

13. Стратегия национальной безопасности Российской Федерации до 2020 года // Президент России. – 2009. – 13 мая [электронный ресурс]. – URL: www.xn--d1abbgf6aiiy.xn--p1ai/ref_notes/424.

В человеческом обществе жизненно важные интересы всех объектов безопасности подвергаются воздействию самых различных угроз, поэтому особую практическую значимость имеет подразделение видов безопасности по сферам или областям жизнедеятельности, в которых и проявляются эти угрозы.