М. М. Кучерявый

РОЛЬ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ В СИСТЕМЕ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Проанализирована роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации, представлена характеристика двух основных векторов обеспечения информационной безопасности РФ, а именно — государственно-правового и технологического. Рассмотрен также феномен кибербезопасности, ее основные элементы и ее роль в системе обеспечения информационной безопасности на национальном и международном уровнях.

Ключевые слова: национальная безопасность, информационная безопасность Российской Федерации, информационное общество, кибербезопасность.

M. Kucheriavyi

The role of the information component in the system policy National security of the Russian Federation

In the following article is analyzed the role of the information component in the political system of ensuring the national security of the Russian Federation, is presented the characteristics of two key vectors of the information security of the Russian Federation, namely, state-legal and technological. The article also considers the phenomenon of cybersecurity, its key elements and its role in the system of information security at the national and international levels.

Keywords: national security, information security of the Russian Federation, information society, cybersecurity.

Роль информационной составляющей в системе национальной безопасности в начале XXI века значительно возросла, и этот процесс продолжается и в настоящее время. Стремительное развитие и широкое распространение современных информационных технологий происходит не только в сфере национальной безопасности, но и в смежных с ней областях, которые имеют принципиальное значение для обеспечения безопасности современного государства.

Особое значение имеет информационная компонента в средствах обеспечения национальной безопасности, и ее удельный вес в этом процессе будет возрастать и далее, по крайней мере, в среднесрочной перспективе. Значительная часть сил обеспечения национальной безопасности также ориентирована на решение стратегических задач, непосредственно или косвенным образом связанных с обеспечением информационной безопасности. Для управления и координации действий указанных сил и использования названных средств в информационной области в нашей стране проводится соответствующая политика.

«Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере» [2].

В структуре политики информационной безопасности мы считаем целесообразным выделить два основных направления — государственно-правовое и технологическое.

Государственно-правовое направление связано с функционированием государственных органов власти и с состоянием законодательной и нормативно-правовой базы, а также с качеством «человеческого фактора» и потенциала, с развитием общественных отношений. В «Доктрине информационной безопасности Российской Федерации» сформулированы основные принципы, направления и задачи государственной политики обеспечения информационной безопасности Российской Федерации. Они поставлены перед федеральными органами государственной власти, перед органами государственной власти субъектов федерации, общественными объединениями. В указанном документе значительное внимание уделяется гуманитарному направлению политики обеспечения национальной безопасности, реализации роли человеческого фактора в этом процессе. В частности, в Доктрине подчеркивается: «Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации… правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере» [2].

Федеральные органы государственной власти и органы государственной власти субъектов Российской Федерации, при решении возникающих в информационной сфере конфликтов должны неукоснительно руководствоваться указанными принципами и иными законодательными нормативными и правовыми актами, регулирующими отношения в сфере информационной безопасности. Важнейшей задачей государства в области информационной безопасности является обеспечение гарантий конституционных прав и свобод человека и гражданина на доступ к информации и обеспечение полноценных возможностей для деятельности в информационной сфере.

Аналогичная правовая практика существует и во многих зарубежных странах. В законодательных и нормативных документах ведущих государств современного мира информационная безопасность определяется в качестве реальной возможности информационной системы проявлять в должной степени устойчивость к аварийным ситуациям и противозаконным враждебным действиям, которые в состоянии ограничить или закрыть доступ к хранимой или транслируемой информации, а также нарушить ее сохранность и конфиденциальность.

Как показывает анализ зарубежного опыта правового обеспечения информационной безопасности, около 100 государств приняли законы о праве на информацию. Устойчивая тенденция на принятие национальных законов, гарантирующих доступ к информации о деятельности органов власти, отмечается с начала 60-х годов. В последние 20 лет такие законы были приняты в таких странах, как Франция, Греция, Дания, Голландия, Бельгия, Португалия, Испания, Финляндия и Италия. Законы о доступе граждан к правительственной информации приняты

в США, Канаде, Австралии и Новой Зеландии. В ряде стран Европы, таких, как Нидерланды, Испания, Португалия, Австрия, Венгрия, Эстония, Бельгия и Румыния, право граждан на доступ к официальной информации закреплено конституционно. Во Франции, Греции и Италии эти права закреплены в законах. Совершенствование законодательства в данной сфере продолжается в Великобритании, Германии, Эстонии, Молдове, Польше и в ряде других государств. Законодательное ограничение прав на доступ к правительственной информации установлено, например, в Швеции и Финляндии [1, с. 46].

Интересен для нашей страны опыт Европейского Союза по созданию системы правового регулирования телекоммуникации и защиты информации. В рамках этой системы принят комплекс соответствующих правовых актов, направленных на обеспечение информационной безопасности. В частности, было введено понятие «сетевая и информационная безопасность» (СИБ) и сформулированы концептуальные основы европейской политики по ее обеспечению, приняты директивы Европейской комиссии о частной жизни и электронных коммуникациях, об охранении данных.

Наряду с принятием нормативно правовых актов в ЕС проводится работа по институционализации сферы информационной безопасности. Так, учрежден институциональный контрольный механизм за соблюдением прав граждан на частную жизнь при обработке персональных данных институтами и органами Евросоюза в составе Европейского контролера по защите данных и инспекторов по защите данных. В контексте системы мер по борьбе с угрозами СИБ организовано Европейское агентство сетевой и информационной безопасности.

Приняты ЕС и документы принципиального стратегического характера, в частности, «Стратегия безопасности информационного общества “Диалог, партнерство и расширение возможностей”». Этот документ содержит обзор современного состояния угроз безопасности информационного общества и определяет дополнительные меры по обеспечению СИБ. К документам подобного рода следует также отнести акт «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости», который содержит инициативу по защите важнейшей информационной инфраструктуры. В последнее время в ЕС запущены несколько важных инновационных проектов в сфере противодействия киберпреступности [8, с. 77].

Однако в условиях развития информационного общества в нашей стране, в процессе информатизации глобальных масштабов становится все более очевидным, что обеспечить информационную безопасность путем деятельности органов государственной власти, правоохранительных структур и развития законодательной и нормативно-правовой базы достаточно затруднительно. Полностью не решает эту проблему даже применение инновационных технических средств.

В современном информационном обществе имеет место обусловленность всех основных видов индивидуальной и общественной деятельности от информационно-коммуникационных технологий. От этих технологий зависит информационное обеспечение государственной деятельности, деловой активности, сфер образования культуры и т. д. Таким образом, информационный контент превратился в важный и ценный компонент функционирования всех основных субъектов общества: личности, социальных и экономических институтов, государства. Когда имеющую большое значение информацию не удается должным образом охранить от несанкционированного доступа, возникают проблемы с обеспечением безопасности на личном, общественном или государственном уровне.

В связи с рассмотренной выше проблемой специалисты обращают внимание на

необходимость формирования соответствующей современным реалиям информационного общества культуры информационной безопасности. Например, А. А. Малюк по данному поводу пишет: «Государственные органы, предприятия, организации, индивидуальные владельцы и пользователи ИТ-индустрии должны знать о факторах, угрожающих информационной безопасности, и о возможных превентивных действиях, должны осознавать свою ответственность и принимать меры для повышения безопасности информационных технологий. С этой целью должна быть сформирована культура информационной безопасности, которая является составной частью культуры общества» [4, с. 33].

В современном мире прилагаются значительные усилия для формирования глобальной культуры кибербезопасности. Это свидетельствует о том, что обеспечение информационной безопасности превратилось в актуальную глобальную проблему наших дней. Данный процесс следует рассматривать в одном ряду с проблемами сохранения и развития культуры и предотвращения войн и вооруженных конфликтов, обеспечения экономической и экологической, демографической и продовольственной, энергетической и сырьевой безопасности в планетарном масштабе.

Основным дипломатическим полем для разработки подходов к формированию глобальной культуры кибербезопасности стали ведущие международные организации. Такая ситуация объясняется следующими причинами. Во-первых, это связано с тем, что в современном глобальном информационном обществе все больше становится трансграничных соединений, связывающих пользователей в разных странах, иногда находящихся на различных континентах и расположенных на значительных расстояниях друг от друга. Во-вторых, поиски решения проблемы глобальной культуры информационной безопасности требуют переговоров с большим числом участников — субъектов международных отношений и международного права. Подобного рода форумы многосторонней дипломатии наиболее оптимально, как показывает опыт, проводить в рамках международных организаций. В-третьих, на повестке дня, как мы можем предположить, — создание нового института международного публичного права — права информационной безопасности. Как известно, международное право формируется в наше время, прежде всего, ООН и некоторыми другими авторитетными международными организациями.

Организация Объединенных Наций одна из первых проявила большой интерес к рассматриваемой проблеме. С одной стороны, культура глобальной безопасности имеет большое значение для обеспечения безопасности всего международного сообщества. С другой стороны, ООН всегда проявляла пристальное глубокое внимание к вопросам развития информационного обмена и информационных технологий. Например, еще в 1971 году Генеральная Ассамблея ООН приняла резолюцию «Свобода информации; права человека и научно-технический прогресс». Дважды в 2000 и 2001 году этот авторитетный форум рассматривал вопросы и принимал резолюции на тему «Борьба с преступным использованием информационных технологий».

Особый интерес вызывают резолюции Генассамблеи ООН по проблемам формирования культуры информационной безопасности. Первая из них «Создание глобальной культуры кибербезопасности» была принята 20 декабря 2002 года. Эксперты и дипломаты ООН констатировали: «Стремительное развитие информационной технологии изменило то, как государственные органы, предприятия, другие организации и индивидуальные пользователи должны подходить к кибербезопасности» [5]. В «Приложении» к этому документу сформулированы «Элементы для создания глобальной культуры кибербезопасности». По мнению авторов данного документа, глобальная

культура кибербезопасности будет требовать от всех участников учета следующих девяти взаимодополняющих элементов.

1) *Осведомленность.* Участники должны быть осведомлены о необходимости безопасности информационных систем и сетей и о том, что они могут сделать для повышения безопасности.

2) *Ответственность.* Участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения.

3) *Реагирование.* Участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и вводить процедуры, предусматривающие оперативное и эффективное сотрудничество в деле предупреждения таких инцидентов, их обнаружения и реагирования на них. Это может предполагать трансграничный информационный обмен и сотрудничество.

4) *Этика.* Поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим.

5) *Демократия.* Безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный поток информации, конфиденциальность информации и коммуникации, надлежащую защиту информации личного характера, открытость и гласность.

6) *Оценка риска.* Все участники должны выполнять периодическую оценку риска, которая: позволяет выявлять угрозы и факторы уязвимости; имеет достаточно широкую базу, чтобы охватить такие ключевые внутренние и внешние факторы, как технология, физические и человеческие факторы, применяемая методика и услуги третьих лиц, сказывающиеся на безопасности; дает возможность определить допустимую степень риска; помогает выбрать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации.

7) *Проектирование и внедрение средств обеспечения безопасности.* Участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей.

8) *Управление обеспечением безопасности.* Участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций.

9) *Переоценка.* Участники должны подвергать вопросы безопасности информационных систем и сетей обзору и повторной оценке и вносить надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости [5].

Почти через десять лет Генассамблея ООН вновь вернулась к обсуждаемой проблеме и приняла новую резолюцию, в которой, в частности, дано описание «Инструмента добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур». В рекомендациях, содержащихся в документе, сделан акцент на защиту, в первую очередь, систем государственного управления, а также на просветительскую работу по распространению знаний об информационной сфере и подготовке специалистов-профессионалов для этой сферы. Так, одна из рекомендаций, изложенная

в вышеуказанном «Инструменте добровольной самооценки», ориентирует государства — члены Организации Объединенных Наций на подготовку и реализацию «плана кибербезопасности». Этот план предназначен «для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур» [6].

Международный союз электросвязи (МСЭ), который является специализированным учреждением ООН в области электросвязи и информационно-коммуникационных технологий, также активно подключился к работе по формированию культуры информационной безопасности. Эксперты МСЭ констатируют: «С учетом того, что персональные компьютеры становятся все более мощными, что происходит конвергенция технологий, что все шире распространяется применение информационно-коммуникационных систем и что растет число соединений через государственные границы, все, кто разрабатывает, владеет, управляет, обслуживает и использует информационные сети, должны осознавать проблемы кибербезопасности и принимать соответствующие их функциям меры для защиты сетей. Органы государственного управления должны играть ведущую роль в создании культуры кибербезопасности и в поддержке мер, принимаемых другими участниками»[3].

Соединенные Штаты Америки являются государством, которое во второй половине прошлого века создало наиболее благоприятные условия для развития в этой стране информационно-коммуникационных технологий и стало одной из первых стран, где эти технологии широко используются во всех сферах общественной жизни. США уделяют большое внимание политике информационной безопасности, активно развивая как государственно-правовое, так и технологическое направление указанной сферы. Однако, как отмечают некоторые эксперты, огромный прогресс в развитии информационно-коммуникационных технологий привел к тому, что их развитие стало опережать формирование соответствующей нормативно-правовой базы. В настоящее время государственная власть США прилагает значительные усилия на преодоление этого разрыва.

Данный опыт развития политики информационной безопасности в заокеанской державе, вероятно, может быть учтен и при формировании политики информационной безопасности в нашей стране. Российские исследователи уделяют достаточно большое внимание анализу американского опыта реализации политики обеспечения информационной безопасности [9, с. 95].

Однако в последнее время политика информационной безопасности США оказалась серьезно скомпрометирована разоблачениями некоторых сотрудников американских спецслужб, прежде всего, Э. Сноудена. Достоянием всеобщей гласности оказались обстоятельства, которые неопровержимо свидетельствовали о том, что американские правящие круги при проведении политики информационной безопасности полностью пренебрегали стратегическими интересами в сфере кибербезопасности других государств.

«Сноуден предал гласности информацию о секретной программе электронной слежки под кодовым названием «PRISM». И, надо подчеркнуть, что речь идёт, в том числе, о слежке за европейскими пользователями интернет-компаний и социальных сетей. АНБ является главным оператором программы, распределяя полученную информацию (по сферам интересов) между ЦРУ, ФБР, Управлением по борьбе с наркотиками и другими спецслужбами. Сноуден раскрыл далеко не все секреты, которыми владеет, но и то, что прозвучало, в Латинской Америке, например, было воспринято с крайней

тревогой. Если империя позволяет себе нагло шпионить даже за своими союзниками по НАТО, то на какие же действия она способна в странах к югу от Рио-Гранде (город в штате Техас, США), которые считает своим «задним двором»?» [9].

В сложившихся условиях в глобальном информационном пространстве, когда в силу политики США возникли серьезные проблемы с обеспечением кибербезопасности у многих других стран, Российская Федерация должна найти адекватный ответ на эти глобальные вызовы. Для Российской Федерации является необходимым реализовать долгосрочную технологическую политику в информационной сфере. Целью такой политики должно быть создание информационно-коммуникационной инфраструктуры, в которую входили бы собственные информационные магистрали, включающие систему серверов, созданных и расположенных на территории России и управляемых российскими компаниями. Российскими должны быть все компоненты указанной инфраструктуры, начиная от процессоров и операционных систем и заканчивая конкретными программными продуктами.

В «Государственной программе Российской Федерации “Информационное общество (2011–2020 годы)”» особое внимание уделено тому, что в современном глобальном информационном обществе отставание в развитии информационно-коммуникационных технологий и киберпространства представляет угрозу не только обеспечению информационной безопасности, но и всей системе поддержания национальной безопасности. Это означает, что недостаточно эффективная политика информационной безопасности становится слабым звеном, существенно ослабляющим и всю общегосударственную политику национальной безопасности. Индустриально развитые государства современного мира в настоящее время на основе инновационных информационно-коммуникационных технологий приступили к качественному преобразованию всех основных сфер общественной жизнедеятельности — от экономики до здравоохранения и т. п.

На данное обстоятельство особо обращается внимание в вышеназванной государственной программе. Так, в данном документе подчеркнуто, что «одним из вызовов, на который должна ответить Российская Федерация, является переход развитых стран к формированию новой технологической базы экономических систем, основанной на использовании новейших достижений в области информатики, в том числе в здравоохранении и в других сферах. Ответ на этот вызов — инновационный сценарий, направленный на формирование новой экономики, или экономики знаний и высоких технологий, в число ведущих отраслей которой входят отрасли связи и информационных технологий. В отношении отрасли информационных технологий определены такие цели, как повышение качества жизни граждан, развитие экономической, социально-политической и культурной сфер жизни общества, а также совершенствование системы государственного управления» [7].

Для достижения этих целей необходимо, во-первых, чтобы технологическое направление политики информационной безопасности было ориентировано на формирование современной информационно-телекоммуникационной инфраструктуры, обеспечение высокого уровня ее доступности, предоставление на ее основе качественных услуг. Следствием такой технологической политики должно оказаться обеспечение конкурентоспособности и технологического развития российских информационных технологий как на внутреннем, так и на мировом рынках и киберпространствах.

Во-вторых, политика, направленная на всемерное развитие информационной сферы, при всей ее важности, не должна стать самоцелью. Успешная реализация такой политики должна привести к повышению качества образования, медицинского обслуживания, социальной защиты населения, к

развитию культуры и средств массовой информации на основе информационных технологий.

В-третьих, важным результатом политики обеспечения информационной безопасности, которого необходимо достичь в процессе реализации «Государственной программы Российской Федерации “Информационное общество (2011–2020 годы)”», следует рассматривать повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и коммерческих организаций с органами государственной власти.

В-четвертых, необходимо осуществить в рамках политики информационной безопасности как важной составной части политики обеспечения национальной безопасности комплекс специальных мер. Эти меры должны быть направлены на противодействие использованию информационных технологий в целях угрозы национальным интересам России, включая обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры и информационных и телекоммуникационных систем. Такой подход следует рассматривать как обеспечение суверенитета нашей страны над ее информационным пространством.

Для достижения последней из указанных целей в рамках «Государственной программы» предусмотрена особая подпрограмма «Безопасность в информационном обществе». «Мероприятия этой подпрограммы обеспечивают решение задачи предупреждения угроз, возникающих в информационном обществе, посредством выполнения функции государственного контроля (надзора) в сфере реализации программы, создания средств защиты информации, мониторинга угроз, регулярной оценки защищенности компонентов инфраструктуры, ликвидации неблагоприятных последствий нарушений ее защиты, своевременной модернизации систем защиты компонентов инфраструктуры»[7].

Итак, анализ основных элементов, необходимых для формирования культуры информационной безопасности, показывает, что в них достаточно ярко выражен политический аспект. Прежде всего, речь идет о политических ценностях демократического общества, а также о характеристиках политического управления, таких, как политика обеспечения безопасности, ответственность, оценка рисков. В данной связи можно утверждать, во-первых, что культура информационной безопасности тесно соприкасается с политической культурой российского общества и будет в перспективе оказывать определенное влияние на развитие последней. Во-вторых, необходимо, чтобы процесс формирования культуры кибербезопасности занял должное место в информационной составляющей политики национальной безопасности Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. *Асланов Р. М.* Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество. 2012. № 2 (86). С. 46.
2. Доктрина информационной безопасности Российской Федерации. Гл. Ш. Ст. 8 [Электронный ресурс]// URL: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM
3. Доклад Международного союза электросвязи «Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности». Женева.: МСЭ, 2010 [Электронный ресурс]// URL: http://www. itu. int/dms_pub/itu-d/opb/stg/D-STG-SG01. 22-2010-PDF-R. pdf
4. *Малик А. А.* Формирование культуры информационной безопасности общества //Педагогика. 2009. № 3. Март. 2009. С. 33.
5. Резолюция, принятая Генеральной Ассамблеей. № 57/239. Создание глобальной культуры кибербезопасности. 20 декабря 2002 года. [Электронный ресурс]// URL:http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement.

6. Резолюция, принятая Генеральной Ассамблеей. № 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур. 21 декабря 2009 года. [Электронный ресурс]// URL:http://daccess-dds ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement
7. Распоряжение Правительства РФ от 20.10.2010 N 1815-р (ред. от 15.08.2012) «О государственной программе Российской Федерации “Информационное общество (2011–2020 годы)”». Гл. 2 [Электронный ресурс]// URL: www.consultant.ru Дата сохранения: 04.05.2013.
8. *Смирнов А. А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза. М.: ЮНИТИ — ДАНА: Закон и право. 2012. С. 77–110.
9. *Шариков П. А.* Эволюция государственной стратегии в сфере информационной безопасности // США — Канада. Экономика, политика, культура. 2009. 3 12. С. 95–108.

REFERENCES

1. *Aslanov R. M.* Zarubezhnyj opyt pravovogo regulirovanija obespechenija informatsionnoj bezopasnosti // Politika i obshchestvo. 2012. № 2 (86). S. 46.
2. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii. Gl. Sh. St. 8 [Elektronnyj resurs]// URL: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM.
3. Doklad Mezhdunarodnogo sojuza elektrosvjazi “Zashchishchennost’ setej informatsii i svjazi: peredovoj opyt po sozdaniju kul’tury kiberbezopasnosti”. Zheneva.: MSE, 2010 [Elektronnyj resurs]// URL: http://www. itu. int/dms_pub/itu-d/opb/stg/D-STG-SG01. 22-2010-PDF-R. pdf
4. *Malik A. A.* Formirovanie kul’tury informatsionnoj bezopasnosti obshchestva //Pedagogika. 2009. № 3. Mart. 2009. S. 33.
5. Rezoljutsija, prinjataja General’noj Assambleej. № 57/239. Sozdanie global’noj kul’tury kiberbezopasnosti. 20 dekabrja 2002 goda [Elektronnyj resurs]// URL:http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement.
6. Rezoljutsija, prinjataja General’noj Assambleej. № 64/211. Sozdanie global’noj kul’tury kiberbezopasnosti i otsenka natsional’nyh usilij po zashchite vazhnejshih informacionnyh infrastruktur. 21 dekabrja 2009 goda [Elektronnyj resurs]// URL:http://daccess-dds ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement
7. Rasporjazhenie Pravitel’stva RF ot 20.10.2010 N 1815-r (red. ot 15.08.2012) «O gosudarstvennoj programme Rossijskoj Federacii “Informatsionnoe obshchestvo (2011–2020 gody)”». Gl. 2 [elektronnyj resurs]// URL: www. consultant. ru Data sohranenija: 04. 05. 2013.
8. *Smirnov A. A.* Obespechenie informatsionnoj bezopasnosti v uslovijah virtualizatsii obshchestva. Opyt Evropejskogo Sojuza. M.: JuNITI — DANA: Zakon i pravo. 2012. S. 77–110.
9. *Sharikov P. A.* Jevoljutsija gosudarstvennoj strategii v sfere informatsinnoj bezopasnosti // SShA — Kanada. Ekonomika, politika, kul’tura. 2009. 3 12. S. 95–108.

М. В. Невзоров

СБОР ИНФОРМАЦИИ ПО ЭТНОПОЛИТИЧЕСКИМ КОНФЛИКТАМ: НЕДОСТАТКИ БАЗ ДАННЫХ И ПОИСК РЕШЕНИЙ

Представлен результат сравнения основных зарубежных проектов по сбору информации о конфликтах. Отмечаются недостатки баз данных: 1) факты собираются преимущественно о вооруженных столкновениях; 2) эмпирические факты не учитывают информацию о восприятии актора в конфликтной ситуации. Автор предполагает, что устранить данные недостатки может единая теория конфликта, которая логически