УДК 34

Особенности системы информационной безопасности как элемента международной безопасности в современном мире

Пелевина Екатерина Сергеевна

Аспирант,

Северо-западный институт управления,

Российская академия народного хозяйства и государственной службы

при Президенте Российской Федерации,

199178, Российская Федерация, Санкт-Петербург, Средний пр. В.О., 57/43;

e-mail: pelevinakate@mail.ru

Аннотация

В статье раскрываются особенности и интерпретации понятия «информационная безопасность» в контексте проблематики обеспечения международной и национальной безопасности в современном мире. Осуществлена попытка исследования проблематики путем выявления ключевых факторов, влияющих на процессы экономической и глобальной безопасности в историческом контексте и в разрезе важнейших правовых, национальных и международных документов, регулирующих отношения в этой сфере. С политико-правовых позиций выявлена проблематика в обеспечении информационной безопасности в мире и на уровне отдельных государств, в том числе России. В завершении исследования сделан вывод о том, что стремительное развитие информационных и интернет-технологий является вызовом для всего мирового сообщества и требуют принятия мер по регулированию рынка, в частности, путем стандартизации процессов.

Для цитирования в научных исследованиях

Пелевина Е.С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. Том 6. № 1А. С. 194-205.

Ключевые слова

Интернет, информационная безопасность, международные угрозы, глобальная безопасность, политика, международная безопасность.

Введение

На сегодняшний день информационная безопасность считается одним из важнейших компонентов национальной безопасности. Значимость последней постепенно возрастает во всех сферах общественной жизни, в том числе и в политической. При этом становится очевидным, что в информационном обществе информация представлена, с одной стороны, предметом массового потребления, а с другой – мощным экономическим ресурсом. При этом создание идеальной системы информационной безопасности может зависеть от того, кто и как будет ею управлять.

Сегодня все чаще высказываются опасения о том, что ключевым сдерживающим фактором внедрения информационной безопасности в области экономики и бизнеса является неравномерное развитие информационной сферы. Отсюда следует, что развитие информационного общества в России является одной из важнейших задач повышения эффективности управления информационной безопасностью. При этом важно отметить, что информационное общество связано с высоким уровнем развития телекоммуникационных и информационных технологий, а также их интенсивным использованием бизнесом, гражданами и органами государственной власти.

Кроме того, международный опыт свидетельствует о том, что информационные и телекоммуникационные технологии уже являются локомотивом социально-экономического развития большинства стран мира, а обеспечение гарантированного свободного доступа граждан к информации представляет одну из важнейших задач государства.

Международная информационная безопасность

В современных условиях информационная сфера жизни международного сообщества представлена в виде динамично развивающейся системы самоорганизации различных социальных институтов, которую нельзя подчинить исключительно позитивному праву одного государства. Социальные коммуникативные системы и институты ставят перед собой цель выработать морально-нравственные установки и сформировать представления людей о необходимых моделях поведения в обществе; в итоге социальной коммуникации появляются новые аспекты модернизации социальной организации общества и развития права [Кириленко, 2016, 312].

Проблема информационной безопасности тесно связана с понятиями «международная безопасность» и «экономическая глобализация». Так, ключевой потребностью системы государства является необходимость обеспечения условий, которые необходимы для ее функционирования и развития. Стремительное распространение оружия массового уничтожения ставят мировое сообщество перед необходимостью сохранения и обеспечения мира. Система международного права при этом нормативно закрепила потребность в мире как глобальный основной интерес и возложила на государства юридическую обязанность по поддержанию идеи мира между различными государствами.

В научной и правовой среде международная безопасность представлена в виде такого состояния межгосударственных отношений, которое способно отвечать объективному интересу каждого государства, и, кроме того, не противоречить глобальному интересу, который нормативно закреплен в современном международном праве. Вместе с тем необходимость обеспечения исполнения государствами возложенных на них юридических обязанностей по поддержанию мира, основанных на неуклонном соблюдении ими основополагающих принципов и норм международного права, имеет целью защиту и реализацию субъективных внутригосударственных прав на их индивидуальную безопасность, включая право на существование, равноправное функционирование и развитие в межгосударственных отношениях [Базилевский, 1983, 13].

Под международной информационной безопасностью, согласно терминологии ООН, понимается защищенность глобальной информационной системы от террористических, преступных и военно-политических угроз. В 2003 году Россия в документе «Основы государственной политики в области международной информационной безопасности до 2020 года» также в качестве международных угроз обозначила опасность вмешательства во внутренние дела суверенного государства посредством информационно-коммуникационных технологий (ИКТ). Такой тип угроз опасен возможностью нарушения общественной стабильности, а также разжигания межэтнической и межнациональной розни.

Кроме этого, необходимо отметить, что относительно терминологии нет единства мнений в понимании термина «международная информационная безопасность». Чаще всего она понимается как столкновение национальных интересов государств, однако в целом вопрос терминологии остается дискуссионным. Россия придерживается широкого понимания термина «международная информационная безопасность», являющегося собирательным различных технических аспектов, включая безопасность информационных сетей и систем, а также манипулирование информацией, ее распространение путем глобальных информационных сетей и информационного воздействия. При этом страны Запада и прежде всего США являются сторонниками узкого подхода, понимая под международной информационной безопасностью только технические аспекты и кибербезопасность.

В современном мире серьезную угрозу национальной безопасности представляют различные формы терроризма. Международным терроризмом создана открытая кампания в целях дестабилизации ситуации уже не только в отдельных странах, но и группах стран и во всем мире в целом.

Взаимодействие государств при решении вопросов международной информационной безопасности

Другим серьезным вызовом, вставшим перед современным мировым сообществом, является «экономическая глобализация», или глобализация мировой экономики. Стремительная интернационализация хозяйства охватила практически одновременно весь мир, и для

крупнейших компаний развитых стран суверенитет иных государств уже стал играть роль тормоза. Однако западные державы и их союзники воздерживаются от применения «новейших» приоритетов «поствестфальской» системы к самим себе.

Для США и их союзников основополагающие парадигмы Вестфальской системы являются незыблемыми, что особенно ярко проявляется в реакции США на события 9 сентября, повлекшие за собой всемерное укрепление суверенитета США и почти полное игнорирование суверенитета Афганистана. При этом складывается достаточно сложная геостратегическая обстановка, сопровождаемая отсутствием защиты со стороны подписанной в 1990 году Парижской хартии для новой Европы, рассматриваемой в качестве новой системы безопасности. Доминирование после распада СССР «атлантической», а затем и американской однополярности резко изменяет картину мира, привязывая всю перспективу безопасности к единовластию супердержавы.

Особое значение при этом начинают играть новые образования БРИКС, ШОС и ОДКБ, деятельность которых, по мнению инициаторов, должна быть направлена на восстановление равновесия в современном мире. В современных условиях международная безопасность обеспечивается основной универсальной организацией – ООН, а также ОБСЕ, в состав которых входят 56 государств и 11 стран, которые имеют статус партнеров по международному сотрудничеству. При этом эксперты отмечают, что ООН сегодня уже не является главным инструментом мира и международной безопасности и заметно теряет авторитет. ОБСЕ также не может взять на себя данные функции, поскольку на настоящий момент не имеет полномочий, которые были бы сопоставимы с полномочиями Совета Безопасности ООН [Андреев, 2011, 56].

Отдельные аспекты проблематики информационной безопасности связаны с распространением новых информационно-коммуникационных технологий, влияющих на политические и другие аспекты современных международных отношений. Обсуждение данной проблематики, поднятой еще на конференции «Информационное сообщество и развитие», проходившей в Мидранде (ЮАР) 13-15 мая 1996 года, привело к принятию в 1998 году на 53 сессии Генеральной Ассамблеи ООН Резолюции 53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Данная резолюция впервые на самом высоком международном уровне признала возможность негативных последствий распространения и использования информационных технологий и средств. В связи с этим также была выражена озабоченность, что такие технологии и средства могут использоваться в целях, несовместимых с обеспечением международной безопасности и стабильности. Позже подобные резолюции были приняты Генеральной ассамблеей ООН на протяжении нескольких лет.

Далее проблема управления Интернетом и его роли в системе международной безопасности фигурирует в качестве важнейшего направления международной информационной политики и межгосударственного сотрудничества. В частности, во время женевского этапа

Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS) 12 декабря 2003 года принимается декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии». Данный документ зафиксировал, что Интернет является публичным ресурсом глобального масштаба, а управление его использованием – одни из ключевых вопросов повестки дня информационного общества.

На международном уровне контроль за интернет-пространством сегодня уже требует многостороннего диалога государств, а также прозрачной и демократической полемики при участии органов государственного управления, бизнеса и субъектов гражданского общества, включая международные организации. Такая система управления направлена на справедливое распределение ресурсов, открывающее доступ для всех, а также на гарантирование стабильного и защищенного функционирования Интернета с учетом многоязычия. Кроме того, в документе отмечается, что управление пользования Интернетом требует участия всех заинтересованных сторон, а также соответствующих межправительственных и международных организаций [Декларация принципов…, www].

Таким образом, Декларация принципов, а также принятый вместе с ней План действий потребовали учреждения рабочей группы по вопросам управления использованием сети Интернет в пределах открытого и всеобъемлющего процесса, который должен обеспечивать механизм активного участия органов государственного управления, бизнеса и субъектов гражданского общества. Это также касается и развивающихся, и развитых стран, системы международных организаций и форумов, целью которых является изучение вопроса об управлении использованием Интернет [План действий, www].

В качестве результатов работы первого этапа WSIS в сентябре 2004 года учреждается Рабочая группа по управлению Интернетом (Working Group on Internet Governance). Ключевая задача, поставленная перед группой, состоит в необходимости изучения и внесения к 2005 году соответствующих предложений по управлению Интернетом. Предмет деятельности Группы состоит в необходимости выработки рабочего определения управления Интернетом; выявлении вопросов государственной политики в данной сфере; формировании единого понимания роли и области ответственности органов государственного управления международных организаций, а бизнеса и субъектов гражданского общества стран [About WGIG, www].

В качестве результата деятельности Группы можно назвать подготовку в июне 2005 года отчета ко второму этапу WSIS, который подтвердил необходимость участия различных заинтересованных сторон в системе управления Интернетом. Речь идет о правительствах, бизнесе, субъектах гражданского общества, а также международных организациях. В рамках деятельности Рабочей группы сформировано рабочее определение управления использования Интернета, суть которого состоит в разработке и применении правительствами, бизнесом и субъектами гражданского общества общих принципов, правил, норм и процедур принятия решений и программ, формирующих необходимые условия для развития и использования Интернета.

Кроме того, особо стоит отметить выделение в документе четырех аспектов государственной политики, имеющих отношение к управлению Интернетом и создающих рамку исследования проблематики информационной безопасности:

– инфраструктура и управления важнейшими интернет-ресурсами;

– применение Интернета, а также спам, сетевая безопасность и киберпреступность;

– иные вопросы, связанные с деятельностью организаций сферы управления Интернетом (к примеру, вопросы прав интеллектуальной собственности или международной торговли);

– различные аспекты развития управления Интернетом, в частности, создание потенциала в развивающихся странах [Отчет рабочей группы…, www].

Кроме вышеуказанных, стоит отметить проблему управления ключевыми Интернет-ресурсами, суть которой состоит в необходимости создания центра управления, работа которого будет основана на деятельности единого централизованного механизма распределения ресурсов. Среди таких ресурсов стоит выделить IP-адреса – сетевые адреса, присваиваемые любому работающем в Интернете устройству, а также доменные имена. При этом важно, что информационное взаимодействие в Интернете требует однозначного определения интернет-узла ввиду его уникальности в масштабах сети.

Современные теоретические подходы к международным аспектам информационной безопасности

Разобравшись с понятием и правовой основой международной информационной безопасности стоит обратить особое внимание также на современные теоретические подходы к международным аспектам информационной безопасности с позиции политологических и международно-политических исследований.

Так, либеральная методология основана на подходах к содержанию понятия «информационная безопасность», а также эмпирических данных, отстаивающих вульгарно-нигилистический вектор, в рамках которого игнорируется сущность данной проблематики, а также допускается ее предвзятая интерпретация.

В качестве примера данного подхода можно привести полемику вокруг текста «Доктрины информационной безопасности», которая разгорелась в СМИ после того, как данный документ был представлен на суд широкой публике, которая тут же подключилась к ее обсуждению вместе с экспертным сообществом ученых. Опубликованные на данную тему материалы ставили под сомнение необходимость исследования проблематики информационной безопасности в целом, включая обвинения в адрес Совета Безопасности РФ в некомпетентности, навязывании обществу цензуры, а также ограничения свободы демократических средств массовой коммуникации.

В некоторых материалах также говорится о смирительном характере содержания Доктрины информационной безопасности и включенных в нее идей, а также распространении других

инсинуаций в отношении составителей и структур исполнительной власти, разработавших этот документ. Обобщенным выводом из обсуждения проблемы информационной безопасности, основанной на позициях либеральной идеологии, становится утверждение автора действующего до настоящего времени закона о СМИ профессора М. Федотова о необходимости «обезвредить доктрину информационной безопасности» [Цит. по: Лебедев, www].

Некоторые исследователи связывают проблематику обеспечения информационной безопасности государства с необходимостью возврата к практике цензуры СМИ и введения некоторых ограничений на свободу информации. Данная позиция, однако, противоречит нормам Конституции Российской Федерации, а также является дополнительным аргументом сторонников либерально-нигилистического подхода понимания международной информационной безопасности. При этом этап становления концепции информационной безопасности является логичным отражением накопленного политического опыта, обусловливающего поиск средств защиты от угроз национальной безопасности.

Положительный аспект дискуссии о смысловых характеристиках концепции информационной безопасности состоит в формировании научных представлений о сущности информационных угроз, которые характерны для реалий информационного общества, связанных с представлениями практиков холодной войны и идеологическим противоборством двух систем.

В данном контексте плодотворность изменений политического дискурса в российской политологии проявляется в процессе эффективной разработки концепции информационной безопасности, а также обогащении понятийного аппарата теории международных отношений. Особенно наглядно это проявляется в том, что производным от концепции информационной безопасности становится понятие «международная информационная безопасность», прочно утвердившееся в рабочем языке современной дипломатии и теории международных отношений.

Особое значение здесь приобретает тот факт, что Россия является первым государством, инициировавшим появление в современном мире новой угрозы национальной и международной безопасности, связанной с глобальным развитием информационно-коммуникационных технологий.

В 1998 году РФ выступило с инициативой подписания на уровне президентов России и США заявления, регулирующего комплекс проблем международной информационной безопасности. Позиция российской стороны была основана на констатации наличия в мире нового качественного потенциала развития человечества, появившегося в результате глобальной информационно-технологической революции. Без принятия таких превентивных мер данный потенциал может стать не только источником угроз стратегического характера, но также и основанием для появления новых технологий ведения вооруженных конфликтов, что в конечном счете может противоречить интересам поддержания мира и стратегической стабильности на всей Земле.

Таким образом, концептуальные подходы, сформировавшие понятие «международная информационная безопасность», находят свое отражение в тексте Совместного заявления об общих вызовах безопасности в начале XXI века, которое было подписанно президентами России и США 2 сентября 1998 года. Данное заявление способствовало конституированию вопросов международной информационной безопасности в качестве объекта теории международных отношений.

Большое значение для формирования системы международной информационной безопасности и закрепления информационной безопасности как части системы международной безопасности имеет стандартизация требований и характеристик защищенных информационных комплексов, которая нашла отражение в Системе международных и национальных стандартов безопасности информации, включающей более сотни различных документов. В качестве примера можно привести стандарт ISO 15408, известный как Common Criteria.

Данный стандарт обеспечивает единые правила, используемые при разработке функций безопасности информационных технологий, а также для приобретения коммерческих продуктов с такими же свойствами. Ключевое направление оценки – угрозы, которые могут проявляться при злоумышленных действиях человека, и угрозы, вызванные другими факторами. Важным здесь является и создание специализированных требований для коммерческой кредитно-финансовой сферы, учитывая тот факт, что существовавшие до этого отечественные и зарубежные документы были привязаны к условиям правительственной или военной системы, а значит имели отношение к секретной информации, представлявшей государственную тайну.

Выпуск и внедрение стандарта за рубежом сопряжено с разработкой новой, стандартизуемой архитектуры, направленной на обеспечение информационной безопасности вычислительных систем, т. е. на создание технических и программных средств ЭВМ, которые бы отвечали Общим критериям. К примеру, международная организация Open Group, объединяющая более 200 ведущих фирм – производителей вычислительной техники и телекоммуникаций со всего мира, выпустила новую архитектуру безопасности информации для коммерческих автоматизированных систем с учетом указанных критериев.

Заключение

Таким образом, можно сделать вывод, что за последние годы сетевой рынок сопровождается фрагментированным влиянием на формирование стандартов. Стремительное распространение Интернета и обретение им характерных черт потребительского и коммерческого рынка приводит к необходимости поиска путей влияния на стандартизацию путем усиления конкурентной борьбы.

Библиография

1. Андреев Ю.В. Проблемы суверенитета и международная безопасность // Власть. 2011. № 1. С. 34-35.
2. Базилевский Б.Н. Международно-правовые аспекты региональной безопасности: автореферат дис. …канд. юрид. наук. М., 1983. 23 с.
3. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии»: документ WSIS-03/GENEVA/DOC/4-R от 12.12.2003. URL: http://goo.gl/EOXB6c
4. Дзиньпин Си. Си Цзиньпин призвал страны БРИКС прикладывать больше усилий. URL: http://ftimes.ru/economy/5948-si-czinpin-prizval-strany-briks-prikladyvat-bolshe-usilij/
5. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Рос. Федерации 09.09.2000 № Пр-1895. URL: http://www.consultant.ru/document/cons_doc_LAW_28679/
6. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН № 53/70. URL: http://goo.gl/YzdrVG
7. Кириленко В.П. Международное право и информационная безопасность государства. СПб.: СПбГИКиТ, 2016. 396 с
8. Крутских А.В. Война или мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности:сб. статей. М.: МЦНМО, 2004. 208 с.
9. Лавров: судьбы мира не могут определяться одной страной. URL: http://tass.ru/politika/2204220
10. Лебедев А. Концепция информационной безопасности будет обезврежена. URL: http://kommersant.ru/doc/330807
11. Мазитов Р.Р. Информационная безопасность Российской Федерации на современном этапе // Российская юстиция. 2009. № 11. С. 4-7.
12. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года: Утверждены Президентом Рос. Федерации 24.07.2013 № Пр-1753. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/
13. Отчет рабочей группы по управлению использованием Интернет: документ WSIS-II/PC-3/DOC/5-R от 03.08.2005. URL: https://goo.gl/kqdrqq
14. Пилипенко В.Ф. Безопасность: теория, парадигма, концепция, культура. М.: ПЕР СЭ-Пресс, 2005. 192 с.
15. План действий: документ WSIS-03/GENEVA/DOC/5-R от 12.12.2003. URL: http://goo.gl/XQE2eh

16. Противостоять угрозам терроризма и экстремизма страны БРИКС будут все вместе. URL: http://www.yoki.ru/news/news/09-07-2015/441929-0/
17. Селиванов А.И. Координация систем научного обеспечения стратегического управления стран БРИКС: задачи и перспективы. URL: http://www.lawinrussia.ru/node/359017
18. Шестюк В.П. (ред.) Научные и методологические проблемы информационной безопасности: сб. статей. М.: МЦНМО, 2004. 208 с.
19. About WGIG (Working Group on Internet Governance). URL: http://goo.gl/ffBbIw

Features of information security system as an element of international security in the modern world

Ekaterina S. Pelevina
Postgraduate student,
North-West Institute of Management,
Russian Presidential Academy of National Economy and Public Administration,
199178, 57/43 Srednii pr. V.O., Saint Petersburg, Russian Federation;
e-mail: pelevinakate@mail.ru

Abstract

The article describes the characteristics and interpretations of the term "information security" in the context of the problems of ensuring international and national security in the modern world. The attempt is made to study the problem by identifying key factors that affect the processes of economic and global security in the historical context and in the context of important legal, national and international documents, regulating relations in this sphere. The problems of ensuring information security in the world and at the level of individual states, including Russia, are detected from political and legal positions. Finally, the conclusion is drawn that the rapid development of information and Internet technologies is a challenge for the entire international community and requires taking of measures to regulate the market, particularly through standardization of processes.

For citation

Pelevina E.S. (2017) Osobennosti sistemy informatsionnoi bezopasnosti kak elementa mezhdunarodnoi bezopasnosti v sovremennom mire [Features of information security system as an element of international security in the modern world]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 6 (1A), pp. 194-205.

Keywords

Internet, information security, international threats, global security, politics, international security.

References

1. *About WGIG (Working Group on Internet Governance)*. Available at: http://goo.gl/ffBbIw [Accessed 11/12/16].
2. Andreev Yu.V. (2011) Problemy suvereniteta i mezhdunarodnaya bezopasnost' [The issues of sovereignty and international security]. *Vlast'* [Power], 1, pp. 34-35.
3. Bazilevskii B.N. (1983) *Mezhdunarodno-pravovye aspekty regional'noi bezopasnosti: avtoreferat dis. ...kand. yurid. nauk* [International legal aspects of regional security. Doct. Diss. Abstract]. Moscow.
4. *Deklaratsiya printsipov "Postroenie informatsionnogo obshchestva – global'naya zadacha v novom tysyacheletii": dokument WSIS-03/GENEVA/DOC/4-R ot 12.12.2003* [Declaration of Principles "Building the Information Society: a global challenge in the new Millennium": document WSIS-03/GENEVA/DOC/4-R from December 12, 2003]. Available at: http://goo.gl/EOXB6c [Accessed 11/12/16].
5. *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii: utverzhdena Prezidentom Ros. Federatsii 09.09.2000 № Pr-1895* [The information security doctrine of the Russian Federation: approved by the President of the Russian Federation on September 9, 2000 No. Pr-1895]. Available at: http://www.consultant.ru/document/cons_doc_LAW_28679/ [Accessed 11/12/16].
6. *Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoi bezopasnosti: Rezolyutsiya General'noi Assamblei OON № 53/70* [Achievements in the field of informatization and telecommunications in the context of international security: Resolution of the UN General Assembly No. 53/70]. Available at: http://goo.gl/YzdrVG [Accessed 11/12/16].
7. *Dzin'pin Si. Si Tszin'pin prizval strany BRIKS prikladyvat' bol'she usilii* [Xi Jinping has called on BRICS countries to make more efforts]. Available at: http://ftimes.ru/economy/5948-si-czin-pin-prizval-strany-briks-prikladyvat-bolshe-usilij/ [Accessed 11/12/16].
8. Kirilenko V.P. (2016) *Mezhdunarodnoe pravo i informatsionnaya bezopasnost' gosudarstva* [International law and information security of the state]. St. Petersburg: St. Petersburg State Institute of Film and Television.
9. Krutskikh A.V. (2004) Voina ili mir: mezhdunarodnye aspekty informatsionnoi bezopasnosti [War or peace: international aspects of information security]. *Proc. "Nauchnye i metodologicheskie problemy informatsionnoi bezopasnosti"* [Scientific and methodological problems of information security]. Moscow: Moscow Centre for Continuous Mathematical Education.
10. *Lavrov: sud'by mira ne mogut opredelyat'sya odnoi stranoi* [Lavrov: the fate of the world can not be defined by one country]. Available at: http://tass.ru/politika/2204220 [Accessed 11/12/16].

11. Lebedev A. *Kontseptsiya informatsionnoi bezopasnosti budet obezvrezhena* [The concept of information security will be defused]. Available at: http://kommersant.ru/doc/330807 [Accessed 11/12/16].
12. Mazitov R.R. (2009) Informatsionnaya bezopasnost' Rossiiskoi Federatsii na sovremennom etape [Information security of the Russian Federation at the present stage]. *Rossiiskaya yustitsiya* [Russian justice], 11, pp. 4-7.
13. *Osnovy gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti na period do 2020 goda: Utverzhdeny Prezidentom Ros. Federatsii 24.07.2013 № Pr-1753* [The foundations of state policy of the Russian Federation in the field of international information security for the period up to 2020: approved by the President of the Russian Federation on July 24, 2013 No. Pr-1753]. Available at: http://www.consultant.ru/document/cons_doc_LAW_178634/ [Accessed 11/12/16].
14. *Otchet rabochei gruppy po upravleniyu ispol'zovaniem Internet: dokument WSIS-II/PC-3/DOC/5-R ot 03.08.2005* [Report of the working group on Internet use management: document WSIS-II/PC-3/DOC/5-R dated August 3, 2005]. Available at: https://goo.gl/kqdrqq [Accessed 11/12/16].
15. Pilipenko V.F. (2005) *Bezopasnost': teoriya, paradigma, kontseptsiya, kul'tura* [Security: theory, paradigm, concept, culture]. Moscow: PER SE-Press Publ.
16. *Plan deistvii: dokument WSIS-03/GENEVA/DOC/5-R ot 12.12.2003* [Action plan: document WSIS-03/GENEVA/DOC/5-R dated December 12, 2003]. Available at: http://goo.gl/XQE2eh [Accessed 11/12/16].
17. *Protivostoyat' ugrozam terrorizma i ekstremizma strany BRIKS budut vse vmeste* [The BRICS countries will counter the threats of terrorism and extremism together]. Available at: http://www.yoki.ru/news/news/09-07-2015/441929-0/ [Accessed 11/12/16].
18. Selivanov A.I. *Koordinatsiya sistem nauchnogo obespecheniya strategicheskogo upravleniya stran BRIKS: zadachi i perspektivy* [Coordination of systems of scientific support for strategic management in BRICS countries: challenges and prospects]. Available at: http://www.lawinrussia.ru/node/359017 [Accessed 11/12/16].
19. Shestyuk V.P. (ed.) (2004) *Nauchnye i metodologicheskie problemy informatsionnoi bezopasnosti: sb. statei* [Scientific and methodological problems of information security: collection of articles]. Moscow: Moscow Centre for Continuous Mathematical Education.