УДК 323.22/.28

Проблемы реализации государственной политики России в сфере информационной безопасности

Фролов Николай Владимирович

Аспирант,

кафедра политологии,

Московский государственный технический университет им. Н.Э. Баумана,

105005, Российская Федерация, Москва, 2-я Бауманская ул., 5/1;

e-mail: nikolay.mgtu@gmail.com

Аннотация

Вопросы обеспечения информационной безопасности и проведения единой государственной политики в данной сфере становятся все более актуальными. Предметом дискуссий по-прежнему является определение содержания таких основополагающих понятий, как «государственная информационная политика», «государственная политика в сфере информационной безопасности», их соотношения между собой, а также с государственной политикой в области обеспечения национальной безопасности. В результате анализа действующего законодательства, а также различных научных подходов автором обоснована позиция, согласно которой государственная политика в сфере информационной безопасности должна реализовываться как часть государственной информационной политики и государственной политики в области обеспечения национальной безопасности, являясь связующим звеном между ними. Проводится анализ основных тенденций реализации государственной политики России в сфере информационной безопасности, а также проблем такой реализации. Автор обосновывает вывод о том, что основной и наиболее актуальной проблемой в данной сфере является проблема разработки и реализации концепции информационного противоборства.

Для цитирования в научных исследованиях

Фролов Н.В. Проблемы реализации государственной политики России в сфере информационной безопасности // Теории и проблемы политических исследований. 2016. № 4. С. 84-96.

Ключевые слова

Государственная информационная политика, национальная безопасность, информационная безопасность, государственная политика в сфере информационной безопасности, защита информации.

Введение

Развитию общества в настоящее время сопутствует процесс информатизации. Вместе с тем, данный процесс, который приобрел глобальный, общемировой характер, создает новые угрозы безопасности личности, общества и государства.

В последние годы были внесены существенные изменения в законодательство Российской Федерации, направленные на защиту национальных интересов страны в сфере информационной безопасности. Особое внимание при этом было уделено проблемам воздействия информации на общественное сознание [Куликов, 2010, 277-278]. Вооруженные конфликты на Украине, а также на территории ряда арабских государств, происходящие начиная с конца 2013 года, являются явным примером того, какие пагубные последствия может иметь использование и распространение информации в средствах массовой информации, в том числе в сети Интернет. Практика информационных войн в современный период стала одним из основных способов достижения ведущими мировыми державами своих целей.

Важную роль в выявлении существующих тенденций и проблем реализации государственной политики в сфере информационной безопасности играет уяснение характера взаимосвязи государственной информационной политики, государственной политики в сфере информационной безопасности и государственной политики в области обеспечения национальной безопасности.

Информационная функция государства и её реализация в информационной политике страны

Государственная информационная политика связана с реализацией одной из функций государства, которая выделяется рядом ученых [Ермошина, 2010, 52; Просвирнин, 2002, 31-32], – информационной функции. Данная функция государства существовала на всех этапах развития общества. Однако в связи с достижениями научно-технического прогресса, в результате которых появились информационно-телекоммуникационные технологии, использование которых создало основу для формирования мирового информационного общества, роль информации существенно возросла. Это, в свою очередь, привело к повышению роли государства в регулировании процессов информатизации общества.

Несмотря на то, что на необходимость формулирования и реализации государственной информационной политики России указано в ряде нормативных правовых актов[1], до сих пор определение данного понятия на законодательном уровне не закреплено. Концепция государственной информационной политики Российской Федерации, одобренная на засе-

1 Например, Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895); Стратегия развития информационного общества в Российской Федерации (утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212).

дании Комитета Государственной Думы по информационной политике и связи 15 октября 1998 г. и на заседании Постоянной палаты по государственной информационной политике Политического консультативного совета при Президенте Российской Федерации 21 декабря 1998 г. (далее – Концепция государственной информационной политики России), определяет государственную информационную политику Российской Федерации как «совокупность целей, отражающих национальные интересы России в информационной сфере, стратегических направлений их достижения (задач) и систему мер, их реализующих»[2].

Данное определение носит достаточно общий характер, не раскрывает круг субъектов, осуществляющих государственную информационную политику, не позволяет установить соотношение понятия «государственная информационная политика» с понятиями «государственная политика в сфере информационной безопасности» и «государственная политика в области обеспечения национальной безопасности».

Примечательно, что в числе целей, задач, принципов государственной информационной политики в Концепции государственной информационной политики России ни слова не говорится об информационной безопасности. Вместе с тем, в данной Концепции предусмотрено, что решение основных задач такой политики должно осуществляться посредством различных форм воздействия на объекты информационной сферы, в том числе системы обеспечения информационной безопасности. При этом указывается на то, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности. Одновременно определено, что одним из основных направлений государственной информационной политики в данной области является тесное взаимодействие мероприятий государственной информационной политики с мероприятиями, проводимыми в рамках государственной политики обеспечения информационной безопасности.

В свою очередь, Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895 (далее – Доктрина информационной безопасности России), содержит в себе положения, указывающие на то, что государственная информационная политика России должна осуществляться в рамках государственной политики России в сфере информационной безопасности. В частности, в данной Доктрине указывается на то, государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации формулирует и реализует государственную информационную политику России, а первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются разработка

2 Концепция государственной информационной политики Российской Федерации (Одобрена на заседании Комитета Государственной Думы по информационной политике и связи 15 октября 1998 г. и на заседании Постоянной палаты по государственной информационной политике Политического консультативного совета при Президенте Российской Федерации 21 декабря 1998 г.). [Электронный ресурс]. – Режим доступа: URL http://library.zntu.edu.ua/zakon/98ru-gip.html

и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики.

Противоречивость обозначенных формулировок не позволяет однозначно установить соотношение между государственной информационной политикой и государственной политикой в сфере информационной безопасности в России. Однако, по мнению автора, они должны соотноситься как общее с частным.

Проблемы международной информационной безопасности

Рассмотрим основные противоречия (конфликты) в информационной сфере, которые существуют в современном мире и требуют разрешения со стороны государства.

1. С одной стороны, становление информационного общества предъявляет новые требования к государству по обеспечению информационных прав граждан, прежде всего в части обеспечения доступности информации. В частности, возрастают масштабы использования информационно-телекоммуникационных сетей, в том числе сети Интернет, с помощью которых органы государственной власти и местного самоуправления не только доводят до граждан информацию о своей деятельности, но и оказывают государственные и муниципальные услуги, отправляется документация, производятся платежи и т. п. С другой стороны, встает вопрос о том, что государство, осуществляя меры, направленные на обеспечение доступа своих граждан к информации, обязано обеспечить защиту других их прав и законных интересов, в частности, права на неприкосновенность частной жизни, а также защиту интересов общества и самого государства, так как отсутствие государственного регулирования процессов передачи информации может нанести непоправимый вред интересам личности, общества и государства. В данном случае возникает дилемма доступности и безопасности информации, разрешение которой находится в зоне ответственности государства [Козориз, 2012, 121]. Достигнуть баланса интересов в этом вопросе можно только путем реализации комплексной государственной политики в информационной сфере. Формирование и реализация государственной информационной политики без учета требований, направленных на обеспечение информационной безопасности, может привести к тяжелым последствиям, вплоть до утраты государственного суверенитета. В то же время государственная политика в сфере информационной безопасности, направленная на обеспечение безопасности национальных интересов, не может проводиться без учета необходимости соблюдения конституционных прав граждан на получение информации, в частности, такая политика не должна предусматривать введение необоснованных ограничений на сбор, хранение, использование и распространение информации, деятельность средств массовой информации и т. п. Поэтому представляется, что государственная политика в сфере информационной безопасности должна реализовываться в рамках государственной информационной политики, имеющей более широкий спектр объек-

тов воздействия. Здесь же отметим, что одновременно государственная политика в сфере информационной безопасности является одним из направлений осуществления государственной политики в области обеспечения национальной безопасности. Данный вывод согласуется с положениями, содержащимися в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 (далее – Стратегия национальной безопасности России), согласно которым национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

С учетом изложенного представляется, что государственная политика в сфере информационной безопасности является неотъемлемой составляющей частью государственной информационной политики и государственной политики в области обеспечения национальной безопасности, представляя собой связующее звено между ними.

2. С одной стороны, идет развитие глобализации и глобальных процессов, а с другой – увеличение числа различных субъектов на мировой арене и их суверенизация [Пастухова, 2006, 130]. Процесс глобализации позволяет ускорять процессы внедрения новых информационных технологий, способствует развитию международного информационного обмена и имеет ряд иных позитивных последствий, позволяющих обеспечить доступность информации. Однако в условиях глобализации контроль информационных потоков со стороны государства становится затруднителен, что, в свою очередь, создает угрозу государственному суверенитету и территориальной целостности страны. В частности, отсутствие государственного регулирования, в том числе путем введения ограничений и запретов в области сбора, использования, хранения и распространения информации, может привести к распространению информации, создающей угрозу национальным интересам, нарушению конституционных прав граждан, совершению киберпреступлений и т. п. Как правильно отмечает Н.Н. Куняев, «развитие глобального информационного пространства диктует новые потребности правового и организационного регулирования в информационной сфере, связанные с обеспечением защиты государства и его граждан от посягательств со стороны других стран или террористических организаций» [Куняев, 2008, 40].

С учетом изложенного представляется, что государственная информационная политика должна носить комплексный характер. Именно в рамках такой политики следует реализовывать государственную политику в сфере информационной безопасности. В противном случае маловероятно, что необходимый баланс между доступностью и безопасностью информации будет достигнут.

Проведенный анализ реализации государственной политики в сфере информационной безопасности на современном этапе применительно к России позволяет выделить следующие основные тенденции:

1. Совершенствование нормативной правовой базы реализации государственной политики в сфере информационной безопасности с уклоном в сторону установления дополнительных требований, ограничений и запретов в отношении лиц, осуществляющих сбор, хранение, использование и распространение информации, особенно с использованием глобальной сети Интернет. Подобная расстановка акцентов, с одной стороны, позволяет обеспечить защиту информации от несанкционированного доступа, устранить существующие правовые пробелы, а также предотвратить совершение правонарушений, в том числе в сфере компьютерной информации. Включение такого рода положений в законодательство позволяет осуществлять противодействие угрозам национальной безопасности, в частности, когда посредством сети Интернет распространяются материалы, содержащие публичные призывы к осуществлению террористической деятельности или публично оправдывающие терроризм, другие экстремистские материалы. С другой стороны, подобного рода ограничительная практика не должна приводить к ущемлению других конституционных прав и свобод граждан, в том числе свободы мысли и слова, права на получение информации. Отсутствие баланса в данном вопросе может привести к созданию условий для подрыва конституционных основ России, которая является демократическим правовым государством.

2. Усиление роли международного сотрудничества в сфере информационной безопасности. За последние годы во внешней политике России произошли изменения, связанные с привлечением к диалогу по вопросам сотрудничества в сфере международной информационной безопасности новых стратегических партнеров, в частности, Бразилии и Кубы[3]. При этом и взаимодействие в рамках Союзного Государства, СНГ, Шанхайской организации сотрудничества, Организации Договора о коллективной безопасности продолжает развиваться. В частности, расширяется круг вопросов, по которым такое сотрудничество осуществляется, проводится работа по унификации законодательства стран-участниц данных организаций в сфере информационной безопасности.

3. Программный подход при реализации государственной политики в сфере информационной безопасности, который позволяет обеспечить комплексность и наибольшую эффективность в деятельности государственных структур, ответственных за проведение такой политики.

4. Возрастание значимости угроз информационной безопасности России, носящих внешний характер, таких как манипулирование информацией (дезинформация, сокрытие или искажение информации), блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории. Источниками

3 Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Гаване 11 июля 2014 года); Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (Заключено в г. Москве 14 мая 2010 года).

таких угроз исходя из положений, содержащихся в Доктрине информационной безопасности России, считаются, в том числе:

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Здесь необходимо отметить, что в России государственная политика в сфере информационной безопасности направлена только на предотвращение данных угроз, то есть носит оборонительный характер.

5. Повышение роли сети Интернет в реализации государственной политики в сфере информационной безопасности, так как в настоящее время посредством данной сети обеспечивается право граждан на доступ к информации о деятельности органов государственной власти, передаются сведения, содержащие персональные данные, в том числе в процессе оказания государственных и муниципальных услуг, а также совершаются другие действия, которые подразумевают необходимость адекватной защиты и мониторинга обращающейся в сети Интернет информации. Также с каждым днем растет риск возникновения угроз информационной безопасности России, источником которых являются действия, совершаемые в сети Интернет, в том числе в процессе ведения информационных войн.

6. Повышение внимания к вопросу о необходимости разработки, создания и внедрения отечественных информационно-телекоммуникационных технологий с целью снижения зависимости России от импорта иностранной техники, посредством которой совершается информационный обмен.

7. Рост киберпреступности, являющийся неизбежным следствием процессов информатизации и формирования информационного общества.

Дальнейшее совершенствование государственной политики в сфере информационной безопасности требует решения ряда проблем, основные из которых, по мнению автора, можно сгруппировать следующим образом:

1. Проблемы, связанные с отсутствием правового регулирования отношений в сфере информационной безопасности либо недостаточностью и (или) неэффективностью такого регулирования.

К данной группе проблем относится отсутствие в настоящее время закрепленных в нормативных правовых актах дефиниций таких ключевых понятий, как «информационная безопасность» и «государственная политика в сфере информационной безопасности».

В связи с выполнением целого ряда задач, содержащихся в Доктрине информационной безопасности России, требуется ее актуализация. Отсутствие четко сформулированных приоритетов реализации государственной политики в сфере информационной безопасности и их несогласованность со Стратегией национальной безопасности России и Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 года, будут являться препятствием на пути эффективного обеспечения информационной безопасности в стране.

Кроме того, развитие информационных технологий требует постоянного мониторинга и совершенствования законодательства во избежание возникновения угроз национальным интересам в результате их использования. Так, в настоящее время одной из наиболее важных проблем является отсутствие правовой регламентации использования в деятельности органов государственной власти «облачных» технологий. В настоящее время отечественное оборудование, обеспечивающее их безопасное использование, практически не применяется, а задействование импортного оборудования в данном случае может привести к несанкционированному доступу к персональным и иным данным, в том числе со стороны спецслужб иностранных государств [Терещенко, 2014, 130].

2. Проблемы, связанные с отсутствием должной координации деятельности различных государственных структур, направленной на реализацию государственной политики в сфере информационной безопасности.

Ряд ученых высказывает точку зрения о необходимости создания государственного органа, в полномочия которого входит координация деятельности иных государственных органов, осуществляющих деятельность в сфере информационной безопасности. В частности, А.Б. Губарев предлагает создать государственный орган, специально уполномоченный на принятие мер по предотвращению и минимизации последствий угроз информационной агрессии, который в своей деятельности будет опираться на существующие уже государственные учреждения, и в его компетенцию будет входить координация их работы в информационной сфере [Губарев, 2005, 140-147]. Вместе с тем, такая координация может осуществляться и уже существующими органами, например, Советом Безопасности Российской Федерации. В частности, Совет Безопасности Российской Федерации выполняет такую функцию, как анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности, о социально-политической и об экономической ситуации в стране, о соблюдении прав и свобод человека и гражданина. Более того, с учетом анализа функций в области обеспечения информационной безопасности уже существующих федеральных государственных органов и особенностей выполнения ими данных функций (в частности, в связи с имеющимися ограничениями на распростра-

нение находящейся в их распоряжении информации) можно поставить под сомнение саму возможность выполнения какой-либо вновь созданной структурой координирующей роли в отношении таких органов.

3. Проблемы борьбы с киберпреступностью, которая приобрела глобальный характер. На современном этапе очевидно, что эффективная борьба с совершением преступлений в сфере компьютерной информации возможна только на основе объединения усилий всего международного сообщества, так как подобные преступления носят внетерриториальный характер и совершаются с использованием информационно-телекоммуникационных технологий, а следовательно, касаются всех государств. В настоящее время сотрудничество по данному вопросу осуществляется Россией только со странами-участницами СНГ на основании Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 1 июня 2001 года).

4. Проблемы, связанные с зависимостью России от информационных технологий, импортируемых из-за рубежа. Как отмечается учеными, «наблюдаются негативные тенденции в создании отечественных средств информатизации, уменьшаются финансовые возможности потенциальных потребителей этих средств и государственная поддержка основных направлений работ» [Просвирнин, 2002, 34].

5. Проблемы, связанные с противодействием информационной агрессии со стороны иностранных государств. Представляется, что на современном этапе данная группа проблем является наиболее актуальной и требует принятия решительных мер со стороны государства по их устранению.

В частности, применение информационного оружия, в том числе в процессе ведения информационных войн, стало распространенной практикой в современном мире и одним из основных инструментов проведения своих интересов ведущими мировыми державами, в том числе США. При этом одним из основных объектов воздействия в данном случае становится сознание людей. В связи с этим ряд ученых стали выделять такую разновидность информационной безопасности как информационно-психологическая безопасность, под которой понимается основанное на балансе интересов личности, общества и государства состояние защищенности психологии личности и социальных общностей от осуществляемого при обороте вредоносной информации психологического манипулирования, а также иного негативного воздействия на нравственно-психологическое здоровье и развитие [Рыдченко, 2009, 28-29].

Информационная политика России

В отличие от ряда государств, ведущих агрессивную информационную политику, приводящую зачастую к вооруженным конфликтам и подрывающую мировую безопасность,

Россия в информационных войнах занимает оборонительную позицию. Какой-либо концепции деятельности государственных структур в условиях информационной войны в России не существует. Как результат, наша страна зачастую оказывается проигравшей в такого рода противоборствах. Несмотря на то, что ряд ученых, в частности, Е.В. Старостина, Д.Б. Фролов [Старостина, Фролов, 2005], А.Б. Губарев [Губарев, 2005], Е.А. Соловьева [Соловьева, 2011], предпринимали попытки изучения таких явлений, как «информационные войны» и «информационное противоборство», данная тематика не просто продолжает оставаться актуальной, но и требует переосмысления с учетом изменившегося значения данных явлений на современном этапе.

Заключение

В настоящее время определение понятия «информационная война» в российском законодательстве отсутствует. В то же время, межправительственные соглашения России и таких стран, как Куба, Беларусь, государства-члены Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности[4], предусматривают, что под информационной войной понимается противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Примечательно, что соответствующие соглашения с Республикой Беларусь и Кубой были заключены в конце 2013 года и середине 2014 года соответственно. Это лишний раз подчеркивает осознание актуальности данного вопроса на современном этапе и необходимости поиска новых международных партнеров для решения обозначенной проблемы.

Формирование научно обоснованной концепции информационного противоборства, участником которого является Россия, в настоящее время является приоритетным направлением реализации государственной политики России в сфере информационной безопасности. Такая концепция должна учитывать необходимость консолидации усилий не только традиционных, но и новых международных партнеров России в области обеспечения международной информационной безопасности.

4 Например, Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Москве 25 декабря 2013 года); Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Екатеринбурге 16 июня 2009 года).

Библиография

1. Губарев А.Б. Информационные войны как объект политологического исследования: дис. … канд. полит. наук. Уссурийск, 2005. 170 с.
2. Ермошина Р.А. Совершенствование механизма реализации Российским государством информационной функции // Юридический мир. 2010. № 12. С. 50-53.
3. Козориз Н.Л. Информация: дилемма безопасности и доступности // Право в Вооруженных Силах – Военно-правовое обозрение. 2012. № 12. С. 119-122.
4. Куликов Е.М. Распространение слухов как угроза информационной безопасности России // Общество и право. 2010. № 4. С. 276-279.
5. Куняев Н.Н. Информационная безопасность как объект правового регулирования в Российской Федерации // Юридический мир. 2008. № 2. С. 38-40.
6. Пастухова Н.Б. Государственный суверенитет в эпоху глобализации // Журнал российского права. 2006. № 5. С. 130-141.
7. Просвирнин Ю.Г. Информационная функция государства // Журнал российского права. 2002. № 3. С. 29-35.
8. Рыдченко К.Д. Понятие, сущность и содержание информационно-психологической безопасности // Административное право и процесс. 2009. № 4. С. 28-29.
9. Соловьева Е.А. Информационное противоборство в сети Интернет: политологический анализ: дис. … канд. полит. наук. Пятигорск, 2011. 215 с.
10. Старостина Е.В., Фролов Д.Б. Информационные войны: проблемы терминологии // Адвокат. 2005. № 1.
11. Терещенко Л.К. Безопасность информации при использовании облачных сервисов органами государственной власти // Право. Журнал Высшей школы экономики. 2014. № 1. С. 129-139.

The issues of the implementation of the Russian information security state policy

Nilolai V. Frolov
Postgraduate,
Department of political science,
Bauman Moscow State Technical University,
105005, 5/1 2-ya Baumanskaya st., Moscow, Russian Federation;
e-mail: nikolay.mgtu@gmail.com

Abstract

The article deals with the implementation issues of the Russian information security state policy. The issues of providing information security and realization of the state policy in this sphere are becoming more relevant. The subject of discussion is still the definitions of such fundamental concepts as "state information policy", "state policy in the sphere of information security", their relation to each other, as well as to state policy in the sphere of providing national security. Analysing the existing legislation, as well as various scientific approaches, the author proves that the state policy in the sphere of information security should be implemented as a part of the state information policy and state policy in the field of national security, working as a link between them. The main trends of the realization of the Russian state policy in the sphere of information security are analyzed, as well as the problems of its implementation. The author justifies the conclusion that the main and most urgent problem in this sphere is the issue of the development and implementation of information warfare concept. Such concept has to consider need of consolidation of efforts not only traditional, but also new international partners of Russia in the field of ensuring the international information security.

For citation

Frolov N.V. (2016) Problemy realizatsii gosudarstvennoi politiki Rossii v sfere informatsionnoi bezopasnosti [The issues of the implementation of the Russian information security state policy]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 4, pp. 84-96

Keywords

State information policy, national security, information security, state policy in the field of information security, information protection.

References

1. Ermoshina R.A. (2010) Sovershenstvovanie mekhanizma realizatsii Rossiiskim gosudarstvom informatsionnoi funktsii [Improvement of mechanism of realization of informational function by the Russian state]. *Yuridicheskii mir* [Juridical world], 12, pp. 50-53.
2. Gubarev A.B. (2005) *Informatsionnye voiny kak ob"ekt politologicheskogo issledovaniya. Dokt. Diss.* [Information wars as an object of political science research. Doct. Diss.] Ussuriysk.
3. Kozoriz N.L. (2012) Informatsiya: dilemma bezopasnosti i dostupnosti [Information: security dilemma and availability]. *Pravo v Vooruzhennykh Silakh – Voenno-pravovoe obozrenie* [Law in the Armed Forces – Military-legal review], 12, pp. 119-122.

4. Kulikov E.M. (2010) Rasprostranenie slukhov kak ugroza informatsionnoi bezopasnosti Rossii [Distribution of rumours as threat Information security of Russia]. *Obshchestvo i pravo* [Society and law], 4, pp. 276-279.
5. Kunyaev N.N. (2008) Informatsionnaya bezopasnost' kak ob"ekt pravovogo regulirovaniya v Rossiiskoi Federatsii [Information security as an object of legal regulation in the Russian Federation]. *Yuridicheskii mir* [Juridical world], 2, pp. 38-40.
6. Pastukhova N.B. (2006) Gosudarstvennyi suverenitet v epokhu globalizatsii [State sovereignty in the era of globalization]. *Zhurnal rossiiskogo prava* [Journal of Russian law], 5, pp. 130-141.
7. Prosvirnin Yu.G. (2002) Informatsionnaya funktsiya gosudarstva [Information function of the state]. *Zhurnal rossiiskogo prava* [Journal of Russian law], 3, pp. 29-35.
8. Rydchenko K.D. (2009) Ponyatie, sushchnost' i soderzhanie informatsionno-psikhologicheskoi bezopasnosti [Concept, Essence and Contents of Informational-Psychology Security]. *Administrativnoe pravo i protsess* [Administrative law and procedure], 4, pp. 28-29.
9. Solov'eva E.A. (2011) *Informatsionnoe protivoborstvo v seti Internet: politologicheskii analiz. Dokt. Diss.* [Information warfare on the Internet: political analysis. Doct. Diss.]. Pyatigorsk.
10. Starostina E.V., Frolov D.B. (2005) Informatsionnye voiny: problemy terminologii [Information war: terminology problems]. *Advokat* [Lawyer], 1.
11. Tereshchenko L.K. (2014) Bezopasnost' informatsii pri ispol'zovanii oblachnykh servisov organami gosudarstvennoi vlasti [Information Security and the Application of Cloud Services by State Bodies]. *Pravo. Zhurnal vysshei shkoly ekonomiki* [Law. Journal of the Higher School of Economics], 1, pp. 129-139.