ПРОБЛЕМЫ ПРАВОВОЙ ПОЛИТИКИ ЗА РУБЕЖОМ

И.Н. Сопилко*

НАУЧНЫЕ ОСНОВЫ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Аннотация. *Основным назначением политики кибербезопасности в обществе является сохранение самобытности наций, государств, создание реальных и действенных механизмов обеспечения информационных прав и свобод человека в киберпространстве, предотвращения манипулирования массовым сознанием. Особенности исследования научной позиции в отношении политики кибербезопасности состоит в том, что онтологически концепция политики кибербезопасности является следствием парадигмального понимания мультивекторности развития информационного общества и его многоальтернативности, невозможности заранее определить направления развития и соответственно четко урегулировать нормами права широкий спектр информационных правоотношений. Гносеологически концепция политики кибербезопасности помогает операционализировать междисциплинарную методологию к ее формированию и применить ее с соответствующим добавлением адекватного методологического инструментария по развитию эффективного механизма политики кибербезопасности с учетом современных тенденций как относительно генезиса новых киберугроз, так и междисциплинаризации наук. Аксиологически концепция политики кибербезопасности в случае ее легитимации должна выступить ценностью, которую сам по себе несет документ такого концептуального уровня. Современное мироздание и формирование цифрового универсума вне контекста политики кибербезопасности невозможны.*

Ключевые слова: *юриспруденция, законодательство, кибербезопасность, киберугроза, киберпространство, информация, правоотношения, политика, концепция, оптимизация.*

Современный уровень глобализации все меньше и меньше вызывает восторженные возгласы, особенно в среде исследователей информационной тематики. Все больше начинает появляться аналитических работ, в которых авторы системно подходят к изучению вопросов глобализации, а также ее воздействия на сферу информационной безопасности. В этой связи стоит отметить, что современное информационное общество вследствие неурегулированности нормами права информационных отношений столкнулось с новыми угрозами. Хотя данные угрозы многие исследователи относят к сугубо информационным, по своим последствиям они носят многовекторный характер, а стало быть, воз-

© Сопилко Ирина Николаевна

* Кандидат юридических наук, Директор Юридического института Национального авиационного университета

sopilko_i@ukr.net

03680, Украина, Киев, проспект Космонавта, корп. 1, каб. 446.

действуют на всю сферу общественных отношений. Именно поэтому встает необходимость разработки новых алгоритмов управления данными отношениями, формирования комплексных институтов права. Решение данной задачи возможно в рамках реализации более глобальной задачи — разработки научных основ политики кибербезопасности.

Многие исследователи описывают положительные моменты как формирования информационного общества, так и необходимости разработки информационного права как общего регулятора информационных отношений[1]. Другая группа ученых сосредоточивает внимание на обеспечении информационной безопасности, реализации отдельных положений государственной информационной политики[2]. Однако надо заметить, что в данных работах не учитываются современные тенденции развития киберпространства, основное внимание уделено лишь вопросам систематизации информационного законодательства и развития различных институтов информационного права.

Авторы трактуют информационное общество исходя из аксиоматических положений информациологической парадигмы. Причем содержание информационного общества раскрывается в соответствии с тем, какую отрасль науки представляет исследователь. Но еще в прошлом столетии Р. Акофф справедливо отмечал: «По существу, имеются просто проблемы, а различные прилагательные — юридический, экономический, психологический, демографический и т.п. описывают всего лишь различные подходы к их изучению»[3].

Такое положение вещей привело к полному хаосу как в информационном праве, так и в исследованиях по кибербезопасности, которые не могут даже представить парадигмальной концепции государственной информационной политики, не говоря уже о выработке концептуальных научных основ политики кибербезопасности.

В России уровень исследований в данной сфере также является недостаточным ни для эффективного правового регулирования, ни для реализации поставленных Президентом РФ задач по формированию эффективного государства. Так, модно назвать учебник «Информационная политика»[4] и монографию В.Н. Лопатина, в которой были заложены основы системного понимания информационной составляющей государственной политики[5]. В отдельных работах освещаются лишь некоторые вопросы формирования данной политики, однако без выхода на стратегический, системный уровень[6]. Как справедливо подчеркивал Б.В. Ахлибининский, «любая система обладает обязательным свойством целостности»[7]. Потому говорить о сформиро-

[1] Беляков К.І. Інформаційне право: аналіз термінологічно-понятійного апарату // Науковий вісник Київського національного університету внутрішніх справ. 2007. Вип. 3. С. 67–79; Бєляков К.І. «Інформаційна» аксіоматика у праві: проблеми формування // Науковий вісник Юрид. академії МВС України. 2004. № 3. С. 263–268; Гурковський В.І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика). К., 2010.

[2] Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. Харків, 2000; Баскаков В.Ю. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2011. № 24. С. 263–269; Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції. К., 2006; Ліпкан В., Максименко Ю. Націобезпекознавство: проблеми формування категорійно-понятійного апарату // Підприємництво, господарство і право. 2011. № 8. С. 7–11; Ліпкан В.А. та ін. Інформаційна безпека України. К., 2004; Ліпкан В.А. Систематизація інформаційного законодавства України. К., 2012; Марущак А.І. Правові основи захисту інформації з обмеженим доступом. К., 2007; Гевлич В. Державна політика України у сфері захисту персональних даних: міжнародно-правовий аспект // Право України. 2006. № 1. С. 9–15; Кормич Б.А. Інформаційна безпека: організаційно-правові основи. К., 2004; Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К., 2007; Цимбалюк В.С. Основи інформаційного права України / за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К., 2004.

[3] Райветт П., Акофф Р. Исследование операций. М., 1966. С. 40.

[4] Информационная политика / под общ. ред. В.Д. Попова. М., 2003.

[5] Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб., 2000.

[6] Берестова Т.Ф. Государственная информационная политика – инструмент обеспечения единства информационного пространства // Науч. и техн. б-ки. 2006. № 8. С. 15–28; Коновченко С.В., Киселев А.Г. Информационная политика в России. М., 2004; Нестерчук И.В. Информационная политика государства и ее роль в формировании политической культуры студенчества в условиях глобализации: автореф. дис. ... канд. полит. наук. М., 2002; Корконосов И. Проблемы формирования единого информационного ресурса в интересах обеспечения законодательного и исполнительного органов власти субъектов РФ // Государственная информация и демократизация общества: Материалы Междунар. конф. (15–16 мая 2000 г.). СПб., 2001. С. 36–46; Нисневич Ю.А. Информационная политика как комплексная проблема актуализации государственного управления // Библиотека в эпоху перемен: дайджест (по публикациям 1998 года). М., 1999. С. 14–23.

[7] Ахлибинский Б.В. Информация и система. Л., 1969. С. 150–151.

ванной парадигме информационной политики, а тем более политики кибербезопасности, не представляется возможным.

Проведенный анализ библиографических источников в каталогах РГБ дает возможность сформулировать важный вывод: в большинстве научных исследований информационная политика рассматривается в контексте библиотечного дела[8]. Более того, анализ основополагающих документов в сфере национальной безопасности, в том числе информационной, дает возможность заключить о значительном законодательном потенциале в данной сфере: в 2000 г. принята Доктрина информационной безопасности России; в 2008 г. — Стратегия развития информационного общества РФ; в этом же году утверждены Приоритетные проблемы научных исследований в области обеспечения информационной безопасности РФ.

Что же касается непосредственно информационной политики, то она представлена как составляющая гуманитарной политики в контексте реализации в других государствах национальных интересов России, идентификации источников угроз государству.

В Украине ситуацию можно охарактеризовать несколько по-иному. Так, в Национальном институте стратегических исследований проводятся системные исследования не только проблем информационной безопасности, но и затронутых в статье проблем[9]. Данный подход позволяет выходить на принятие государственных решений не с позиций субъективизма, а с учетом научных исследований и национальных интересов. Необходимо доработать и принять Информационный кодекс Украины. Он должен стать логичным шагом после принятия Концепции государственной информационной политики, солидное место в котором займут вопросы кибербезопасности. Данные документы должны быть пронизаны общей идеологией, их основное содержание должно заключаться в том, чтобы в условиях современного мира обеспечить Украине надежный уровень процветания и развития в угрожающем ее информационному суверенитету киберпространстве.

Онтологически концепция политики кибербезопасности является следствием парадигмального понимания мультивекторности развития информационного общества и его многоальтернативности, невозможности заранее определить направления развития и соответственно четко урегулировать нормами права широкий спектр информационных отношений. Императивный дуализм парадигмальности относительно необходимости четкого государственного регулирования и имманентности многоальтернативности развития информационного общества в результате трансформации глобализационных процессов является исходным положением данной концепции. В ней должны быть отражены принципы видения развития государства в современных условиях, сохранения его ведущей и определяющей роли в общественных процессах, в том числе и с учетом антропологических идей, в частности формирования разумного баланса концепций человекоцентризма и государствоцентризма, которые в Украине исследуются достаточно глубоко в рамках научных школ теории права и государства, а также философии права.

Гносеологически концепция политики кибербезопасности помогает операционализировать междисциплинарную методологию к ее формированию, применить ее с соответствующим добавлением адекватного методологического инструментария по развитию эффективного механизма политики кибербезопасности с учетом современных тенденций как относительно генезиса новых киберугроз, так и междисциплинаризации наук. В современных условиях ученые должны специализироваться не по отдельным наукам, а по отдельным проблемам. В Украине ведется значительная работа по формированию науки информационного права, выделению отдельной специальности и формированию высококвалифицированных кадров. В то же время данная работа проводится лишь с учетом традиций правовых наук, несколько игнорируются уже существующие наработки в сфере международных отношений, в частности по специальности «Международная инфор-

---

[8] Дубов Д. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка // URL: <http://www.niss.gov.ua/articles/294> (последнее посещение – 18 марта 2013 г.); Монтвилофф В. Национальная информационная политика: руководство по формулированию, одобрению, реализации и функционированию национальной информационной политики. М., 2009. С. 6–28; Федоров В. Культурная и информационная политика государства: взгляд из библиотеки // Библиотековедение. 2005. № 1. С. 17–22; Информационная политика, информационные поводы, PR в музейной деятельности // Музей. 2008. № 8. С. 12–18; Багрова И.Ю. Национальная информационная политика: цели, содержание и механизм реализации (аналитический обзор) // Рос. гос. б-ка. Информкультура. 1994. Вып. 2. С. 18–47; Багрова И.Ю. Информационная политика: оперативность, точность, полнота // Библиотекарь. 1990. № 10. С. 11.

[9] США вводят тотальный контроль в Интернете // URL: <http://ukrlife.net/ssha-vvodyat-totalnyiy-kontrol-v-internete> (последнее посещение – 18 марта 2013 г.).

мация». Это является свидетельством того, что научные исследования концептуально лишены творческого потенциала и креатива для своего развития. Изначальное создание границ рамками и методологией одной науки (юридической, международных отношений, экономической и т.д.) фактически приводит к тому, что системная проблема рассматривается фрагментарно не в силу узости самого ученого, а в силу ограниченности методологического потенциала науки, в рамках которой он исследует системный феномен.

Одним из выходов из ситуации считается дальнейшее развитие информациологии, основы которой были заложены И.И. Юзвишиным. Актуальными, на мой взгляд, может быть развитие таких направлений:

1) информационная акмеология;
2) информационная этика;
3) информационная политика;
4) политика кибербезопасности.

Главным атрибутом современной информациологии должно стать системное видение информационного общества, а главное — роли государства в его эффективном развитии, в том числе с помощью управленческих, правовых и иных механизмов.

Аксиологически концепция политики кибербезопасности в случае ее легитимации должна выступить ценностью, которую сам по себе несет документ такого концептуального уровня. Современное мироздание и формирование цифрового универсума вне контекста политики кибербезопасности невозможны, равно как и развитие эффективного государства вне политики кибербезопасности и информационного общества. Следовательно, значение этой политики является в ее способности сформировать основные ценности, ради которых собственно и должна осуществляться данная политика. Смысловой статус концепции также играет ведущую роль в формировании как ориентиров всей государственной политики, так и информационного законодательства.

Следует признать, что даже сама постановка вопроса о формировании научных основ политики кибербезопасности является новаторской по своему содержанию; в рамках правовых наук данную тему никто раньше не поднимал. И хотя сама проблематика уже становится объектом научного анализа отдельных исследователей, в частности Национального института стратегических исследований, отдельно и акцентированно проблемы формирования и определения именно правового содержания данной концепции не анализируются.

Особенностью киберпространства является сложность его правового определения, описания отношений между субъектами. Именно поэтому только в США акт киберугроз и кибератаки рассматриваются как акты объявления войны. Причем на уровне законодательства данный вопрос не урегулирован и решается в рамках руководства Агентства по национальной безопасности.

Следует признать конструктивным опыт работы в США негосударственных компаний. В частности, в феврале 2013 г. американская компания Mandiant, которая осуществляет свою деятельность в сфере кибербезопасности, представила неопровержимые доказательства осуществления кибершпионажа секретным подразделением 61398 китайской армии. В частности, установлено место нахождения этой группы, а также ее связи с должностными лицами китайской армии, что подчеркивает поддержку государством актов кибершпионажа.

У Президента США находится на рассмотрении законопроект относительно признания актов кибершпионажа актами агрессии, со всеми вытекающими отсюда последствиями, вплоть до применения обычных вооружений.

В других государствах данные вопросы также не находят должного решения. Например, в ЕС не принято никаких документов, в которых была бы четко выписана процедура выявления кибератак, осуществлена их классификация по определенным критериям на соответствующие уровни угроз как информационному обществу, так и киберпространству, сетям, критической инфраструктуре.

Более того, вряд ли в таких условиях можно четко отделить кибервойны от кибератак, операций киберподразделений специальных служб иностранных государств и самостоятельной деятельности хакеров, в том числе с целью диверсии и инспирирования конфликтов, подобно ботам в форумах, которые пытаются поссорить между собой форумчан.

В мире в целом формируются соответствующие подразделения кибербезопасности. В соответствии с официальными они существуют в США (U.S. Cyber Command), Великобритании (Cyber Security Operations Centre), Германии (Internet Crime Unit, Federal Office for Information Security), Австралии (The Cyber security operations centre), Индии.

Приведенные факты подтверждают необходимость активизации прежде всего правовых исследований в данной сфере, которая сейчас является наименее урегулированной нормами права, хотя объективно представляет серьезную угрозу как безопасности го-

сударства, так и безопасности конкретного человека.

Нельзя не отметить и то, что государство может ввести ограничительные режимы использования киберпространства. Так, в Китае существуют определенные ограничения на пользование фейсбуком, в КНДР вообще такой сервис, как Google, запрещен. В США, которые презюмируют себя эталоном демократии, в том числе и в сфере информационных отношений, было принято законодательство о контроле в Интернете, выделяются средства на прослушивание в Интернете и слежения за людьми[10].

Фактически информационное общество принесло обманчивые плоды радости от доступа к безграничным массивам информации лишь на первых порах. Когда люди уже не представляют свою жизнь без Интернета и цифровых технологий, а информационное общество стало очевидным фактом, наступило время расплаты — лишение информационных свобод человека, манипулирование его сознанием. Примером может служить иск европейских государств к Googl с требованием выплаты 1 млрд дол. за нарушения информационных прав граждан ЕС. Речь идет в частности, о персональных данных, которые сервис собирает и использует по своему усмотрению, фактически формируя информационную надгосударственную империю.

Именно поэтому основным назначением политики кибербезопасности является сохранение самобытности наций, государств, создание реальных и действенных механизмов обеспечения информационных прав и свобод человека в киберпространстве, предотвращения манипулирования массовым сознанием и ввода ограничительных правовых и информационных режимов.

В Европе многие ученые ведут неправедную научную войну с самой эффективной политической организацией — государством. Упадок сил государственных институтов приведет к институциональной несостоятельности в эффективной защите прав и свобод человека в киберпространстве, сопряженной с провалами в государственной киберполитике, что может привести к потере государственности.

Государственная политика кибербезопасности (ГПКБ) формируется и реализуется в условиях, когда в современном мире нивелируется различие между национальным и глобальным киберпространством, растет число жертв от атак хакеров и масштабность противоправной деятельности в киберпространстве, наблюдается устойчивая тенденция к появлению новых видов киберугроз, а само киберпространство начинает использоваться для формирования в сознании людей алгоритмов управления современной цивилизацией, а также трансформируется в поле будущих войн и сражений.

Малоэффективность информационного законодательства предопределяет и неэффективность как международно-правового механизма, так и вообще сотрудничества в сфере реализации политики кибербезопасности в широком смысле.

Государственная политика кибербезопасности должна:

1) вытекать из требований Конституции Украины, положений Концепции государственной информационной политики, Стратегии национальной безопасности Украины, Доктрины информационной безопасности Украины, теории и опыта информационной борьбы, причем как внутреннего, так и зарубежного;

2) способствовать развенчанию мифологизации относительно безальтернативно позитивного восприятия информационного общества, формировать правильное и адекватное понимание опасности от неконтролируемого развития информационного общества;

3) способствовать выявлению фальсификаций трактовки положений государственной политики и формировать направления противодействия им;

4) обеспечивать формирование единого подхода на всех уровнях государства к осуществлению политики кибербезопасности; в рамках данной политики должны быть выработаны цели, функции, принципы и методы деятельности по формированию и реализации политики кибербезопасности;

5) сформировать основы для определения направлений создания общегосударственной системы кибербезопасности;

6) заложить фундамент для опережающего предупреждения киберугроз, формирования правовой базы по регулированию информационных отношений;

7) формировать культуру кибербезопасности и соответствующего ей сознания;

8) укрепить уровень кибербезопасности.

Очевидно, поставленная проблема требует дальнейшего детального изучения, от ее реального решения будет зависеть дальнейшая судьба государства.

[10] Нестерчук И.В. Информационная политика государства и ее роль в формировании политической культуры студенчества в условиях глобализации: автореф. дис. ... канд. полит. наук. М., 2002.

Библиография:

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. — Харків, 2000.
2. Ахлибинский Б.В. Информация и система. — Л., 1969.
3. Багрова И.Ю. Информационная политика: оперативность, точность, полнота // Библиотекарь. — 1990. — № 10.
4. Багрова И.Ю. Национальная информационная политика: цели, содержание и механизм реализации (аналитический обзор) // Рос. гос. б-ка. Информкультура. — 1994. — Вып. 2.
5. Баскаков В.Ю. Захист інформації з обмеженим доступом в умовах боротьби з організованою злочинністю // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2011.— № 24.
6. Берестова Т.Ф. Государственная информационная политика — инструмент обеспечения единства информационного пространства // Науч. и техн. б-ки. — 2006. — № 8.
7. Бєляков К.І. «Інформаційна» аксіоматика у праві: проблеми формування // Науковий вісник Юрид. академії МВС України. — 2004. — № 3.
8. Бєляков К.І. Інформаційне право: аналіз термінологічно-понятійного апарату // Науковий вісник Київського національного університету внутрішніх справ. — 2007. — Вип. 3.
9. Гевлич В. Державна політика України у сфері захисту персональних даних: міжнародно-правовий аспект // Право України. — 2006. — № 1.
10. Гурковський В.І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика). — К., 2010.
11. Дубов Д. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка // URL: <http://www.niss.gov.ua/articles/294> (последнее посещение — 18 марта 2013 г.).
12. Информационная политика / под общ. ред. В.Д. Попова. — М., 2003.
13. Информационная политика, информационные поводы, PR в музейной деятельности // Музей. — 2008. — № 8.
14. Коновченко С.В., Киселев А.Г. Информационная политика в России. — М., 2004.
15. Корконосов И. Проблемы формирования единого информационного ресурса в интересах обеспечения законодательного и исполнительного органов власти субъектов РФ // Государственная информация и демократизация общества: Материалы Междунар. конф. (15–16 мая 2000). — СПб., 2001.
16. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. — К., 2004.
17. Ліпкан В., Максименко Ю. Націобезпекознавство: проблеми формування категорійно-понятійного апарату // Підприємництво, господарство і право. — 2011. — № 8.
18. Ліпкан В.А. Систематизація інформаційного законодавства України. — К., 2012.
19. Ліпкан В.А. та ін. Інформаційна безпека України. — К., 2004.
20. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції. — К., 2006.
21. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. — СПб., 2000.
22. Марущак А.І. Правові основи захисту інформації з обмеженим доступом. — К., 2007.
23. Монтвилофф В. Национальная информационная политика: руководство по формулированию, одобрению, реализации и функционированию национальной информационной политики. — М., 2009.
24. Нестерчук И.В. Информационная политика государства и ее роль в формировании политической культуры студенчества в условиях глобализации: автореф. дис. ... канд. полит. наук. — М., 2002.
25. Нисневич Ю.А. Информационная политика как комплексная проблема актуализации государственного управления // Библиотека в эпоху перемен: дайджест (по публикациям 1998 года). — М., 1999.
26. Райветт П., Акофф Р. Исследование операций. — М., 1966.
27. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. — К., 2007.
28. США вводят тотальный контроль в Интернете // URL: <http://ukrlife.net/ssha-vvodyat-totalnyiy-kontrol-v-internete> (последнее посещение — 18 марта 2013 г.).
29. Федоров В. Культурная и информационная политика государства: взгляд из библиотеки // Библиотековедение. — 2005. — № 1.
30. Цимбалюк В.С. Основи інформаційного права України / За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. — К., 2004.

References (transliteration):

1. Belyakov K.I. Informatsiyne pravo: analiz terminologichno-ponyatiynogo aparatu // Naukoviy visnik Kiïvs'kogo natsional'nogo universitetu vnutrishnikh sprav. — 2007. — Vip. 3.
2. Belyakov K.I. «Informatsiyna» aksiomatika u pravi: problemi formuvannya // Naukoviy visnik Yurid. akademiï MVS Ukraïni. — 2004. — № 3.
3. Gurkovs'kiy V.I. Derzhavne upravlinnya rozbudovoyu informatsiynogo suspil'stva v Ukraïni (istoriya, teoriya, praktika). — K., 2010.
4. Aristova I.V. Derzhavna informatsiyna politika: organizatsiyno-pravovi aspekti. — Kharkiv, 2000.
5. Baskakov V. Yu. Zakhist informatsiï z obmezhenim dostupom v umovakh borot'bi z organizovanoyu zlochinnistyu // Borot'ba z organizovanoyu zlochinnistyu i koruptsiєyu (teoriya i praktika). — 2011. — № 24.
6. Lipkan V.A., Maksimenko Yu.Є., Zhelikhovs'kiy V.M. Informatsiyna bezpeka Ukraïni v umovakh єvrointegratsiï. — K., 2006.
7. Lipkan V., Maksimenko Yu. Natsiobezpekoznavstvo: problemi formuvannya kategoriyno-ponyatiynogo aparatu // Pidpriєmnitstvo, gospodarstvo i pravo. — 2011. — № 8.
8. Lipkan V.A. ta in. Informatsiyna bezpeka Ukraïni. — K., 2004.
9. Lipkan V.A. Sistematizatsiya informatsiynogo zakonodavstva Ukraïni. — K., 2012.
10. Marushchak A.I. Pravovi osnovi zakhistu informatsiï z obmezhenim dostupom. — K., 2007.
11. Gevlich V. Derzhavna politika Ukraïni u sferi zakhistu personal'nikh danikh: mizhnarodno-pravoviy aspekt // Pravo Ukraïni. — 2006. — № 1.
12. Kormich B.A. Informatsiyna bezpeka: organizatsiyno-pravovi osnovi. — K., 2004.
13. Sidak V.S. Zabezpechennya informatsiynoï bezpeki v kraïnakh NATO ta ЄS. — K., 2007.
14. Tsimbalyuk V.S. Osnovi informatsiynogo prava Ukraïni / Za red. M.Ya. Shvetsya, R.A. Kalyuzhnogo ta P.V. Mel'nika. — K., 2004.
15. Rayvett P., Akoff R. Issledovanie operatsiy. — M., 1966.
16. Informatsionnaya politika / pod obshch. red. V.D. Popova. — M., 2003.
17. Lopatin V.N. Informatsionnaya bezopasnost' Rossii: Chelovek. Obshchestvo. Gosudarstvo. — SPb., 2000.
18. Berestova T.F. Gosudarstvennaya informatsionnaya politika — instrument obespecheniya edinstva informatsionnogo prostranstva // Nauch. i tekhn. b-ki. — 2006. — № 8.
19. Konovchenko S.V., Kiselev A.G. Informatsionnaya politika v Rossii. — M., 2004.
20. Nesterchuk I.V. Informatsionnaya politika gosudarstva i ee rol' v formirovanii politicheskoy kul'tury studenchestva v usloviyakh globalizatsii: Avtoref. dis. ... kand. polit. nauk. — M., 2002.
21. Korkonosov I. Problemy formirovaniya edinogo informatsionnogo resursa v interesakh obespecheniya zakonodatel'nogo i ispolnitel'nogo organov vlasti sub'ektov RF // Gosudarstvennaya informatsiya i demokratizatsiya obshchestva: Materialy Mezhdunar. konf. (15–16 maya 2000). — SPb., 2001.
22. Nisnevich Yu.A. Informatsionnaya politika kak kompleksnaya problema aktualizatsii gosudarstvennogo upravleniya // Biblioteka v epokhu peremen: Daydzhest (po publikatsiyam 1998 goda). — M., 1999.
23. Akhlibinskiy B.V. Informatsiya i sistema. — L., 1969.
24. Dubov D. Suchasni trendi kiberbezpekovoï politiki: visnovki dlya Ukraïni. Analitichna zapiska // URL: <http://www.niss.gov.ua/articles/294> (poslednee poseshchenie — 18 marta 2013 g.).
25. Montviloff V. Natsional'naya informatsionnaya politika: rukovodstvo po formulirovaniyu, odobreniyu, realizatsii i funktsionirovaniyu natsional'noy informatsionnoy politiki. — M., 2009.
26. Fedorov V. Kul'turnaya i informatsionnaya politika gosudarstva: vzglyad iz biblioteki // Bibliotekovedenie. — 2005. — № 1.
27. Informatsionnaya politika, informatsionnye povody, PR v muzeynoy deyatel'nosti // Muzey. — 2008. — № 8.
28. Bagrova I.Yu. Natsional'naya informatsionnaya politika: tseli, soderzhanie i mekhanizm realizatsii (analiticheskiy obzor) // Ros. gos. b-ka. Informkul'tura. — 1994. — Vyp. 2.
29. Bagrova I.Yu. Informatsionnaya politika: operativnost', tochnost', polnota // Bibliotekar'. — 1990. — № 10.
30. SShA vvodyat total'nyy kontrol' v Internete // <http://ukrlife.net/ssha-vvodyat-totalnyiy-kontrol-v-internete> (poslednee poseshchenie — 18 marta 2013 g.).

Материал получен редакцией 25 марта 2013 г.