ISSN 2524-2369 (Print)
ISSN 2524-2377 (Online)
УДК 349
https: //doi.org/10.29235/2524-2369-2019-64-2-220-226

Поступила в редакцию 12.02.2019
Received 12.02.2019

В. Ю. Арчаков, О. С. Макаров, А. Л. Баньковский

Государственный секретариат Совета Безопасности Республики Беларусь, Минск, Беларусь

О КОНЦЕПТУАЛЬНЫХ ВЗГЛЯДАХ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ В АСПЕКТЕ СОВРЕМЕННОГО ОБЩЕСТВЕННОГО РАЗВИТИЯ

Аннотация. В данной статье разработчики Концепции информационной безопасности Республики Беларусь рассматривают ее положения как важные элементы в основах дальнейшего становления и укрепления суверенного белорусского государства. В силу новизны отношений, возникающих в информационной сфере, она подвержена повышенной уязвимости от рисков, вызовов и угроз, которые транспортируются во все иные сферы общественной жизни. Проблема обеспечения информационной безопасности становится важнейшим вопросом реализации сбалансированных интересов личности, общества и государства. Обеспечение информационной безопасности превращается в самостоятельную область функционирования общества и в единой системе общегосударственной деятельности направлено на поступательное социально-экономическое развитие Беларуси.

Ключевые слова: информационная безопасность, информационная сфера, концептуальные подходы, государственная деятельность, общественное развитие, риски, вызовы, угрозы

Для цитирования. Арчаков, В. Ю. О концептуальных взглядах на информационную безопасность Республики Беларусь в аспекте современного общественного развития / В. Ю. Арчаков, О. С. Макаров, А. Л. Баньковский // Вес. Нац. акад. навук Беларусі. Сер. гуманіт. навук. – 2019. – Т. 64, № 2. – С. 220–226. https: //doi.org/10.29235/2524-2369-2019-64-2-220-226

V. Yu. Archakov, O. S. Makarov, A. L. Bankowski

State Secretary of the Security Council of Republic of Belarus, Minsk, Belarus

ON CONCEPTUAL VIEWS ON INFORMATION SECURITY OF THE REPUBLIC OF BELARUS IN THE ASPECT OF MODERN SOCIAL DEVELOPMENT

Abstract. In this article the authors of the Information Security Concept of the Republic of Belarus regard its provisions as important elements in the bases for the further formation and strengthening of the sovereign Belarusian state. Due to the novelty of relations arising in the information sphere, it is exposed to increased vulnerability to risks, challenges and threats that are transported to all other spheres of public life. The problem of information security ensuring is becoming one of the most important issues in the realization of balanced interests of individual, society and the state. Ensuring information security is becoming an independent area of the functioning of society and, in a single system of nation-wide activity, is aimed at the progressive socio-economic development of Belarus.

Keywords: information security, information sphere, conceptual approaches, state activities, social development, risks, challenges, threats

For citation. Archakov V. Yu., Makarov O. S., Bankowski A. L. On conceptual views on information security of the Republic of Belarus in the aspect of modern social development // *Vestsi Natsyianal'nai akademii navuk Belarusi. Seryia humanitarnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Humanitarian series,* 2019, vol. 64, no. 2, pp. 220–226 (in Russian). https: //doi.org/10.29235/2524-2369-2019-64-2-220-226

Введение. Необходимость утверждения концептуальных подходов к пониманию феномена информационной безопасности и обеспечению ее безопасности в Беларуси уже давно обсуждалась в научных и экспертных кругах [1–5]. По сложившемуся мнению, отсутствие в течение длительного времени таких общепринятых взглядов на безопасность информационной сферы в нашей достаточно развитой стране и продвинутом информационном обществе свидетельствует о ее определенном отставании от объективных глобальных и региональных тенденций.

В марте 2019 года Советом Безопасности страны утверждена Концепция информационной безопасности Республики Беларусь [6]. Согласно своему основному предназначению Концепция конкретизирует и обобщает официальные взгляды на сущность информационной безопасности как

состояния защищенности информационной сферы, актуализирует стратегические приоритеты в области обеспечения информационной безопасности, создает дополнительную методологическую основу для их комплексной практической реализации.

При этом Концепция по своей сути является документом, ориентированным в первую очередь на приоритеты развития, задает параметры деятельности по обеспечению информационной безопасности через описание перспективных моделей и конфигураций защищенного состояния информационной сферы.

Развитие как политическая предустановка. Принятая Концепция информационной безопасности, являясь по своему предназначению общественно-политическим, программным, декларативным актом, синтезирует целый ряд положений и взглядов, позиционирующих Беларусь как стабильно и последовательно развивающееся государство, нацеленное на суверенное созидательное развитие, самостоятельное, мирное и равноправное существование в международном сообществе. Одновременно задаются и соответствующие установки, определяющие роль и место общегосударственной деятельности по обеспечению информационной безопасности в дальнейшем укреплении Беларуси как сравнительно молодого суверенного государства.

В качестве доминанты через структуру и содержание Концепции отчетливо проводится мысль о том, что подходы к обеспечению безопасности в информационной сфере исходят прежде всего из социально-экономических интересов, т. е. не существуют первично, обособленно или противоположно по отношению к ним, а напротив, формируются исключительно в русле продвижения Беларуси к качественно новым этапам своего развития. Именно поэтому нынешняя Концепция основывается не только на базовой Концепции национальной безопасности Республики Беларусь, определяющей в обобщенном виде основные национальные интересы, угрозы в информационной сфере, их источники и направления нейтрализации [7, п. 14, 27, 34, 42, 54], но и на стратегических документах в области информатизации, развития цифровой экономики, информационного общества, науки и технологий, защиты интеллектуальной собственности[1]. Концепция поддерживает и продолжает общегосударственную линию на развитие информационного общества и «цифровую» трансформацию, т. е. является своевременным шагом системы обеспечения национальной безопасности по реализации новейших социально-экономических трендов в жизнедеятельности страны.

В Концепции особенно отмечается значение безопасного развития не только Беларуси как государства, но и каждого человека, общества, негосударственного сектора, научного, образовательного, идеологического потенциала. Получает новое звучание тема государственно-частного партнерства как одно из непременных условий устойчивого мирового развития. В данной области оно коснется всевозможных вопросов – от поддержки отечественных производителей средств защиты информации и обновления механизмов выявления угроз до внедрения современных образовательных, профессиональных стандартов и повышения компьютерной грамотности населения.

Наряду с этим в Концепции подчеркивается значение и роль личности, важность соблюдения интересов граждан, их конституционных и иных основополагающих прав, свобод, возможностей, что рассчитано на всё более конструктивное и эффективное вовлечение общества и каждого человека в процесс обеспечения и осознанного поддержания безопасности непрерывно формирующейся информационной сферы.

В свою очередь, именно через развитие информационной сферы главным образом обеспечивается ее безопасность, и об этом прямо говорится в Концепции [6, раздел III].

Защищенность конституционных основ. В Концепции отражаются самые современные вызовы и угрозы, которые формируются в информационной сфере, проистекают из нее и представляют опасность для конституционных основ суверенных государств, их поступательного развития по избранному пути и повседневной жизнедеятельности. Речь идет прежде всего о манипуляциях массовым сознанием, дискредитации традиционных идеалов и ценностей, размывании

[1] Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы, одобрена Президиумом Совета Министров Республики Беларусь (протокол от 3 ноября 2015 г. № 26); Государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы, утверждена Постановлением Совета Министров Республики Беларусь от 23.03.2016 г. № 235; Стратегия Республики Беларусь в сфере интеллектуальной собственности на 2012–2020 годы, утверждена Постановлением Совета Министров Республики Беларусь от 02.03.2012 г. № 205 и др. // Эталон – Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

национального менталитета, нарушении устойчивости информационных инфраструктур, «цифровой» зависимости и т. д.

Для более структурированного понимания этих вызовов и угроз, характерных именно для нынешней эпохи, изложению основных целей и направлений государственной политики обеспечения информационной безопасности предшествует краткое описание состояния и развития информационной сферы. В этом описании выделены гуманитарный и технологический аспекты информационной сферы, что соответствует общепринятым научно-теоретическим и практическим подходам и, кроме того, изначально предопределяет соответствующие предметы защиты: в последующих разделах гуманитарный аспект корреспондируется с обеспечением безопасности информационного пространства (сферы смыслов), технологический – с защитой инфраструктуры и информационных ресурсов.

Мировое развитие, как и продвижение Беларуси к качественно новым жизненным укладам, в ближайшей перспективе будет неизбежно проходить в достаточно сложных условиях глобальной конфронтации, а поэтому особое значение приобретает защита государствами своих национальных интересов, и особенно это касается стран, не претендующих на глобальное либо региональное лидерство. С учетом этого в Концепции впервые применено такое целеполагающее понятие, как «информационный суверенитет», указывающее на незыблемость этой конституционной основы (как решающее условие безопасного развития государства) и выражающееся в неприемлемости навязывания Беларуси каких бы то ни было гуманитарных либо технологических стандартов и приоритетов.

Одновременно с этим через введение принципа информационного нейтралитета разъясняется, что Беларусь исключает возможность каких-либо инициатив со своей стороны по вмешательству в информационную сферу других государств, и тем самым подчеркивается непричастность нашей страны к любым информационным и кибервойнам, акциям, операциям сейчас и в перспективе. Помимо выражения собственной позиции, это означает, что такого же подхода Беларусь ожидает от других государств. К тому же и в Конституции Республики Беларусь [8, ст. 6], и в Концепции национальной безопасности четко указывается ориентированность нашей страны на нейтральный статус [7, ст. 18].

Необходимо, тем не менее, подчеркнуть, что Концепция все же остается документом, нацеленным на обеспечение безопасности. Поэтому при всей ее спокойной и созидательной тональности ясно указывается на готовность Беларуси защищать национальные интересы в информационной сфере, отстаивать информационный суверенитет, всесторонне реагировать на риски, вызовы и угрозы, в том числе в кризисных и иных обостренных условиях, с применением специальных сил и средств.

Международное измерение. В Концепции подчеркивается вовлеченность суверенной Беларуси в глобальные и региональные процессы развития и безопасности, приверженность лучшим мировым и международным практикам, демонстрируется приемлемость различных норм и стандартов. Наряду с очевидным и объективным превалированием в Концепции собственных национальных подходов к проблемам информационной безопасности, духа и буквы международных актов, заключенных в этой сфере нашей страной в рамках СНГ, ОДКБ, Союзного государства Беларуси и России[1], в ней также упоминаются тематические Резолюции Генассамблеи

[1] Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 года; Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 года; Положение о сотрудничестве государств – членов ОДКБ в сфере обеспечения информационной безопасности, утверждено Решением Совета коллективной безопасности от 10 декабря 2010 года; Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 года, ратифицированный Законом Республики Беларусь от 15 июля 2015 года № 292-З; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года; Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности от 10 октября 2008 года; Модельный закон «Об информации, информатизации и информационной безопасности» – постановление МПА СНГ от 28 января 2014 года № 41-15; Модельный закон «О праве на доступ к информации» – постановление МПА СНГ от 17 апреля 2004 года; Модельный закон «О международном информационном обмене» – постановление МПА СНГ от 26 марта 2002 года № 19-7; Модельный закон «О персональных данных» – постановление МПА СНГ от 16 октября 1999 года и др. // Эталон – Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

ООН[1], рекомендации ОБСЕ (причем в Концепции фактически имплементированы отдельные положения документов ОБСЕ в сфере борьбы с кибертерроризмом[2]), некоторые конкретные европейские концепты[3], отдельные тезисы из иных общемировых документов[4].

В проекте Концепции уделено внимание и конкретным угрозам, проистекающим из информационной сферы, дискуссии вокруг которых в глобальном измерении формируют различные, в том числе диаметрально противоположные стратегические подходы государств к обеспечению своих национальных интересов. Например, заявляется о поддержке установления и регулирования всеобщих правил поведения в информационной сфере – то, чего на сегодняшний день достичь не удается. В данном случае речь идет не только и не столько о борьбе с киберпреступностью, в области которой существуют хоть какие-то договоренности[5], а именно о поведении, т. е. действиях, которые на государственном уровне могут не расцениваться как неправильные или недопустимые по отношению к другим странам, однако нарушают их интересы или понимание безопасности собственной информационной сферы (преднамеренные дезинформационные, провокационные или им подобные деструктивные воздействия на массовое сознание, вмешательство в функционирование национальных информационных инфраструктур).

Выражается позиция в отношении неоднозначного на международном уровне понимания того, что кибератаки с территории одного государства в отношении информационных объектов другой страны ни при каких обстоятельствах не должны бездоказательно приравниваться к вооруженному нападению и не могут служить поводом для ответных военных действий. Такого же мнения придерживается большинство стран мира, однако в западных теориях и исследованиях периодически озвучивается возможность реагировать на кибератаки именно с помощью военной силы. Изложенный подход не только выражает обеспокоенность Беларуси явными спекуляциями развитых стран на своем военном преимуществе и появлением у них возможности чрезмерно вольно трактовать происхождение кибератак, но и в целом обозначает нацеленность нашей страны на цивилизованное разрешение проблем и противоречий в информационной сфере.

Немаловажно, что с принятием Концепции у Беларуси появился дополнительный и вполне весомый повод для выдвижения собственных инициатив в сфере обеспечения международной информационной безопасности, нацеленных на безопасное развитие общества. Причем в ближайшем будущем, видимо, не следует рассчитывать на общее глобальное понимание и согласование правовых норм в сфере информационной безопасности. В этих условиях Республике Беларусь необходимо целенаправленно и последовательно выстраивать жизнеспособную систему междуна-

[1] К ним, в частности, относятся резолюции Генеральной ассамблеи ООН 57/239 «Создание глобальной культуры кибербезопасности» (2003), 58/199 «Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур» (2004), 64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» (2010), 65/141 «Использование информационно-коммуникационных технологий в целях развития» (2011) [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/development/ict/res.shtml. – Дата доступа: 04.02.2019.

[2] Решение № 3/04 Совета Министров ОБСЕ «Борьба с использованием Интернета в террористических целях» (MC.DEC/3/04/Corr.l) от 7 декабря 2004 года, Решение № 7/06 Совета Министров ОБСЕ «Противодействие использованию Интернета в террористических целях» (MC.DEC/7/06/Corr.l) от 5 декабря 2006 года, решение № 1063 «Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом» от 7 декабря 2012 года [Электронный ресурс]. – Режим доступа: https://www.osce.org/ru/resources/csce-osce-key-documents /. – Дата доступа: 04.02.2019.

[3] Например, Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) (подраздел «Защита персональных данных») [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/. – Дата доступа: 04.02.2019.

[4] Например, из Глобальной программы кибербезопасности Международного союза электросвязи (Подраздел 19. Обусловленность мер) [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. – Дата доступа: 04.02.2019. Положения Концепции также созвучны с известным Докладом группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2015) [Электронный ресурс]. – Режим доступа: https://www.un.org/disarmament/ru/. – Дата доступа: 04.02.2019.

[5] Имеются в виду упомянутые выше Соглашение государств – участников СНГ и конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. № 185 («Будапештская конвенция») [Электронный ресурс]. – Режим доступа: http://mvd.gov.by/main.aspx?guid=4603. – Дата доступа: 04.02.2019.

родной информационной безопасности вокруг себя, в том числе на основе собственных и узнаваемых авторитетных принципов.

Продвижение к моделям защищенности. Как уже упоминалось выше, в Концепции обстоятельно описываются основные предметы защиты – информационно-психологическая компонента информационной сферы, информационная инфраструктура, информационные ресурсы, и обеспечение их безопасности напрямую связано в первую очередь с развитием самих этих компонентов, а не только с «оборонительными» мерами.

Например, констатируется важность эффективной работы СМИ, конкурентоспособность которых необходимо неуклонно повышать, в том числе за счет важных для них государственно-правовых механизмов. Указывается на необходимость дальнейшей активизации присутствия государства в интернет-пространстве. Введение в практический оборот понятия деструктивного информационно-психологического воздействия на массовое общественное сознание[1] позволяет осознанно и предметно подходить к вопросу противодействия проявлениям и элементам «гибридных» и информационных войн, «операций на основе социальных эффектов», «цветных» революций, информационного терроризма и других видов противоборств в сфере смыслов[2]. А именно, проводить научные исследования и публичные дискуссии на данную тему, дополнительно обусловливать необходимость защитных мер, придавать углубленный смысл информационной и идеологической работе, при необходимости корректировать государственную информационную политику и конкретизировать задачи субъектам реагирования на риски и вызовы в информационной сфере. Обозначается актуальный вопрос о необходимости более настойчивого формирования исторической политики и ее системного использования как важнейшего атрибута суверенного государства в обеспечении национальной безопасности и общественного развития в целом. Обращается внимание на важность общественного контроля за распространением в информационном пространстве незаконной и недостоверной информации, и за рубежом эта практика давно и достаточно эффективно используется[3].

Рассматривая технологический аспект обеспечения информационной безопасности, в новой Концепции будет впервые официально применен термин «кибербезопасность», и это новшество автоматически определяет ориентирование государства на принятые и уже устоявшиеся в мире основные стандарты, подходы, формы и способы противодействия компьютерным инцидентам, компьютерным преступлениям и иным воздействиям на информационно-коммуникационную инфраструктуру. Дальнейшим практическим шагом в развитии института кибербезопасности будет имплементация этого понятия в национальное законодательство, что окончательно определит точки его соприкосновения с правовыми нормами и подходами других стран и иных субъектов международных отношений.

Придается дополнительный импульс деятельности по защите критически важных объектов информатизации (КВОИ), которая уже регламентирована законодательством, однако пока не приобрела однозначно системный характер[4]. Причем КВОИ – это, как правило, те автоматизирован-

[1] Ранее это понятие упоминалось (но не определялось) только в Концепции национальной безопасности как одна из основных потенциальных либо реально существующих угроз национальной безопасности и указывалось в Рекомендациях по сближению и гармонизации законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности / Постановление Парламентской Ассамблеи ОДКБ от 27 ноября 2014 года № 7–6 [Электронный ресурс]. – Режим доступа: http://www.paodkb.ru/upload/iblock/c07/rekomendatsii-po-sblizhen.-igarmoniz.-natsion.-zak_va-gos._chlenov-odkb-v-sfere-obesp.-inf._kommunik.-bezop.pdf. – Дата доступа: 04.02.2019.

[2] Рассмотрение информационно-психологической компоненты в качестве одной из проблем обеспечения информационной безопасности соответствует так называемому «евразийскому» подходу, применяемому в России, иных постсоветских странах, Китае, ОДКБ, ШОС и др. Для «европейской» модели более характерно замалчивание вопросов регулирования содержания информационного пространства и трактовка информационной безопасности в основном как защищенность информационной инфраструктуры.

[3] К примеру, российское общественное объединение «Лига безопасного Интернета» с 2011 года в постоянном режиме осуществляет мониторинг глобальной сети, и в целях обнаружения опасного контента привлекаются тысячи добровольцев по всей стране (так называемая «кибердружина»). Эффективность мониторинга достигается массовостью специалистов и тем, что сбор, обработка (определение признаков состава преступления, градация по видам преступлений), сопровождение уголовных и административных процессов, архивация информации осуществляются единым программно-аппаратным комплексом.

[4] Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» // Эталон – Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

ные системы, с помощью которых осуществляется управление важнейшими элементами социально-экономической инфраструктуры. Принципиальным является указание на то, что киберустойчивость КВОИ достигается главным образом за счет их безопасного проектирования и эксплуатации, и это нацелено на побуждение владельцев соответствующих объектов и систем изначально внедрять средства защиты и правильно ими пользоваться, нежели полагаться на то, что «ничего не произойдет» или рассчитывать на устранение проблем по мере их возникновения.

В части обеспечения безопасности информационных ресурсов в Концепции органично сочетаются интересы повышения открытости и привлекательности экономики страны с необходимостью защиты государственных секретов, причем даются конкретные посылы к обоснованному «облегчению» защитных действий в пользу интересов развития. Например, говорится о принципе соразмерности затрат на обеспечение защиты госсекретов с возможным вредом (ущербом) от их разглашения, недопущении излишнего усложнения режимных требований, нацеленность государства на общее сокращение объема секретов.

Заключение. Процедура концептуализации, как известно, является первым и крайне необходимым этапом, обеспечивающим введение так называемого распознающего фактора по отношению к имеющемуся объему разноплановых данных, что позволяет приступить к разработке стратегий и выходить на прогнозирование конкретных ситуаций.

В данном случае конкретизация и утверждение Концепцией информационной безопасности основ государственной политики и направлений деятельности по защите информационной сферы, а также приоритетность в них темы общественного развития нацеливает государственные инструменты последовательно и неуклонно совершенствовать свою практическую деятельность в данной области, исходя из интересов конструктивных, созидательных социально-экономических процессов. К тому же концептуальное закрепление моделей и форм позволяет не остерегаться каких-либо внезапных смещений в подходах и принципах, т. е. оно должно придать этой деятельности дополнительную устойчивость.

В целом же принятие Концепции позволит обеспечить дальнейшее целенаправленное совершенствование национального законодательства, перевести обеспечение информационной безопасности в более упорядоченную, регламентированную и ответственную деятельность, повысить ее эффективность за счет решения главных задач, вовлечения в это максимально широкого круга субъектов, улучшения их взаимодействия и усиления роли международно-правовых механизмов в интересах дальнейшего продвижения Беларуси к новым укладам общественного развития.

Список использованных источников

1. Систематизация и кодификация информационного законодательства / Ин-т государства и права Рос. акад. наук ; [сост. и ред. А. А. Антопольский]. – М. : Канон-Плюс, 2015. – 214 с.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры : учебник для студентов высш. учеб. заведений / под ред. Т. А. Поляковой, А. А. Стрельцова. – М. : Юрайт, 2016. – 325 с.

3. Арчаков, В. Ю. Теоретическое обоснование необходимости разработки концепции информационной безопасности Республики Беларусь / В. Ю. Арчаков, О. С. Макаров // Наука и инновации. – 2018. – № 10. – С. 14–19.

4. Макаров, О. С. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь / О. С. Макаров, А. Л. Баньковский // Право.by. – 2018. – № 5 (55). – С. 91–96.

5. Арчаков, В. Ю. Выступление на VIII Международной встрече высоких представителей, курирующих вопросы безопасности / В. Ю. Арчаков // VIII Международная встреча высоких представителей, курирующих вопросы безопасности, Тверская область, 23–25 мая 2017 г. – М., 2017. – С. 89–93.

6. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

7. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 окт. 2010 г., № 575 // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

8. Конституция Республики Беларусь 1994 года [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г. и 17 окт. 2004 г. // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

References

1. Antopol'skii A. A. (ed.) *Systematization and codification of information legislation*. Moscow, Kanon-Plyus Publ., 2015. 214 p. (in Russian).

2. Polyakova T. A., Strel'tsov A. A. *Organizational and legal support of information securit*y. Moscow, Yurait Publ., 2016. 325 p. (in Russian).

3. Archakov V. Yu., Makarov O. S. Theoretical substantiation of the need to develop an information security concept for the Republic of Belarus. *Nauka i innovatsii = The Science and Innovations*, 2018, no. 10, pp. 14–19 (in Russian).

4. Makarov O. S., Ban'kovskii A. L. Conceptual directions of legal regulation in the field of information security of the Republic of Belarus. *Pravo.by*, 2018, no. 5 (55), pp. 91–96 (in Russian).

5. Archakov V. Yu. Speech at the VIII International Meeting of High Representatives responsible for Security. *VIII Mezhdunarodnaya vstrecha vysokikh predstavitelei, kuriruyushchikh voprosy bezopasnosti, Tverskaya oblast', 23–25 maya 2017 g.* [VIII International Meeting of High Representatives in charge of security issues, Tver region, May 23–25, 2017]. Moscow, 2017, pp. 89–93 (in Russian).

6. About the Information Security Concept of the Republic of Belarus: Resolution of the Security Council of the Republic of Belarus, 18 March, 2019, no. 1. *Etalon. Legislation of the Republic of Belarus.* Minsk, 2019

7. On approval of the National Security Concept of the Republic of Belarus: Decree of the President of the Republic of Belarus, October 9, 2010, no. 575. *Etalon. Legislation of the Republic of Belarus.* Minsk, 2019 (in Russian).

8. Constitution of the Republic of Belarus 1994: with amendments and additions adopted in the republican referendums on November 24, 1996 and October 17, 2004. *Etalon. Legislation of the Republic of Belarus.* Minsk, 2019 (in Russian).

Информация об авторах

Арчаков Владимир Юрьевич – заместитель Государственного секретаря Совета Безопасности Республики Беларусь (ул. Карла Маркса, 38, 220016, Минск, Республика Беларусь). E-mail: iau@sssc.gov.by

Макаров Олег Сергеевич – доктор юридических наук, доцент, директор Белорусского института стратегических исследований (пр. Победителей, 7, 220004, Минск, Республика Беларусь).

Баньковский Алексей Леонидович – кандидат юридических наук, начальник информационно-аналитического управления Государственного секретариата Совета Безопасности Республики Беларусь (ул. Карла Маркса, 38, 220016, Минск, Республика Беларусь). E-mail: iau@sssc.gov.by

Information about the authors

Vladimir Yu. Archakov – Deputy State Secretary of the Security Council of the Republic of Belarus (38 Karla Marksa Str., Minsk 220016, Belarus). E-mail: iau@sssc.gov.by

Oleg S. Makarov – D. Sc. (Law), Associate Professor, Director of the Belarusian Institute of Strategic Researches (7 Pobeditelej Ave., Minsk 220004, Belarus).

Aleksej L. Bankowski – Ph. D. (Law), Head of Information and Analytical Department of the State Secretariat of the Security Council of the Republic of Belarus (38 Karla Marksa Str., Minsk 220016, Belarus). E-mail: iau@sssc.gov.by