

Доверие и безопасность в информационном обществе

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ: НОВОЕ ПРЕДСТАВЛЕНИЕ О СТРУКТУРЕ И СОДЕРЖАНИИ КОМПЛЕКСНОЙ ПРОБЛЕМЫ

Колин Константин Константинович

Доктор технических наук, профессор

Федеральный исследовательский центр «Информатика и управление» РАН, Институт проблем информатики

г. Москва, Российская Федерация

kolinkk@mail.ru

Аннотация

Проведен анализ структуры и содержания проблемы обеспечения информационной безопасности страны, представленной в Концепции информационной безопасности Республики Беларусь. Показан высокий научно-методологический уровень разработки этой актуальной и комплексной проблемы, а также необходимость ее дальнейшего изучения специалистами в данной области, учеными и преподавателями университетов. Сформулирован ряд существенных замечаний и рекомендаций по содержанию текста Концепции и показаны некоторые важные результаты, полученные в данной области российскими учеными.

Ключевые слова

информационная безопасность, информационная сфера, гуманитарные проблемы, интеллектуальная безопасность, русский язык, живучесть информационных систем.

Введение

В марте 2019 г. в жизни белорусского общества произошло важное событие: Советом Безопасности этой страны была утверждена Концепция информационной безопасности Республики Беларусь [1]. Анализ содержания этого документа показал, что он подготовлен на достаточно высоком научно-методологическом уровне и содержит ряд новых концептуальных положений, связанных с определением структуры и содержания этой актуальной, комплексной и многоаспектной проблемы. Поэтому текст Концепции, безусловно, представляет интерес не только для государственных и общественно-политических деятелей, но также и для научных работников академических институтов системных аналитиков, преподавателей и аспирантов ВУЗов, изучающих современную проблематику и методологию решения проблем обеспечения информационной безопасности.

Краткий анализ наиболее важных положений этой Концепции и является основной целью настоящей работы.

1 Новые представления о структуре проблемы информационной безопасности

Содержание текста рассматриваемой Концепции, для удобства его дальнейшего анализа, представлено в Таблице 1. Текст состоит из семи разделов, в каждом из которых имеется от двух до пяти глав, посвященных определенному аспекту проблемы.

Первое, что бросается в глаза при знакомстве с этим документом, это системность и логическая стройность изложения материалов по различным аспектам рассматриваемой в нем достаточно сложной и комплексной проблемы. При этом, некоторые положения Концепции являются новыми, и на уровне доктринальных документов такого уровня они рассматриваются впервые.

© Колин К.К., 2020. Производство и хостинг журнала «Информационное общество» осуществляется Институтом развития информационного общества.

Данная статья распространяется на условиях международной лицензии Creative Commons «Атрибуция — Некоммерческое использование — На тех же условиях» Всемирная 4.0 (Creative Commons Attribution – NonCommercial - ShareAlike 4.0 International; CC BY-NC-SA 4.0). См. <https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.ru>

Вторая особенность Концепции – это значительное внимание, которое уделяется в ней гуманитарным аспектам проблемы информационной безопасности. В аналогичных документах других стран, включая Россию, этим аспектам уделяется существенно меньшее внимание, в то время как, по оценкам ряда специалистов, именно гуманитарные аспекты проблемы информационной безопасности в последние годы становятся доминирующими [2], и в будущем эта тенденция будет только нарастать [3].

Таблица 1. Структура Концепции информационной безопасности Республики Беларусь

№ п/п	Разделы Концепции	Краткое содержание разделов
1	Общие положения	Мировое значение информационной сферы. Актуальность и значение Концепции. Предмет, цели и задачи Концепции, ее связь с другими доктринальными документами страны.
2	Состояние и развитие информационной сферы в Белоруссии	Гуманитарный аспект информационной сферы. Технологический аспект информационной сферы.
3	Государственная политика обеспечения информационной безопасности	Цели и направления государственной политики. Информационный суверенитет. Информационный нейтралитет. Государственное реагирование на риски, вызовы и угрозы.
4	Безопасность информационного пространства как условие развития суверенного демократического социального государства	Обусловленность мер и основные направления безопасности в информационном пространстве. Сохранение традиционных устоев и ценностей. Информационное обеспечение и сопровождение государственной политики. Безопасность массовой информации.
5	Обеспечение безопасности информационной инфраструктуры	Обусловленность мер и основные направления безопасности информационной инфраструктуры. Безопасность национального сегмента Интернет. Киберустойчивость критически важных объектов и государственных информационных систем. Киберпреступность.
6	Обеспечение безопасности информационных ресурсов	Обусловленность мер и основные направления безопасности информационных ресурсов. Защита государственной и служебной тайны. Безопасность персональных данных и государственных информационных ресурсов.
7	Механизмы реализации Концепции	Нормативно-правовые аспекты. Государственно-частное партнерство. Участие в международных соглашениях.

2 Мировое значение информационной сферы общества и процессов становления информационного общества

Содержание этих вопросов раскрывается в первом разделе текста Концепции, где сформулированы ее цель и задачи, показана связь с другими доктринальными документами страны. Здесь указано, что сегодня информационная сфера приобретает ключевое значение для человека, общества и государства, оказывает всеобъемлющее влияние на экономические, политические и социальные процессы в странах и регионах.

Нам представляется, что эта оценка является очень важной и адекватной современной мировой ситуации, основным тенденциям ее дальнейшего развития. Она ориентирует общество и органы государственной власти страны на необходимость позиционирования проблем

информационного развития и обеспечения информационной безопасности в качестве приоритетных в государственной политике и социальной практике. В этом разделе прямо указано, что «формируемое в глобальном масштабе информационное общество представляет собой новый этап развития цивилизации с преобладанием знаний и информации, воздействием информационных технологий на все сферы человеческой деятельности».

Таким образом, речь идет не о становлении цифровой экономики, о которой сегодня так много говорят и пишут [4], не о развитии Четвертой промышленной революции, согласно представлениям Клауса Шваба [5], а о принципиально новом этапе развития цивилизации, который в России уже давно изучается и получил название информационной цивилизации [6].

Данное положение Концепции является чрезвычайно важным не только в научно-методологическом, но и в практическом плане, так как оно ориентирует общество на цивилизационный характер происходящих в нем процессов цифровой трансформации, а также на их конечную цель – перехода на качественно более высокую ступень цивилизационного развития. А ведь еще Рене Декарт, один из пионеров в развитии методологии науки, утверждал, что правильно называть то или иное явление, значит правильно понимать его сущность.

Нам представляется, что такой, существенно более широкий подход к определению современного процесса информационного развития общества и обусловил то повышенное внимание к гуманитарным аспектам проблемы информационной безопасности, которое мы видим в данной Концепции.

3 Комплексный подход к проблеме и новая терминология

В данной Концепции информационная безопасность страны определяется как «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере». При этом, приоритетными являются интересы личности и общества. В ней также указано, что Концепция обеспечивает комплексный подход к проблеме информационной безопасности и создает методологическую базу для ее решения. С этой целью в тексте документа приведены определения основных терминов, используемых в данной области. Некоторые из них являются новыми и ранее в этой области не использовались. В их числе такие термины как «информационный суверенитет», «информационный нейтралитет», «суверенитет данных», «киберинцидент», «киберустойчивость».

Введение этих терминов обусловлено тем, что проблемная область информационной безопасности в последние годы быстро расширяется и требует формирования нового терминологического аппарата.

4 Гуманитарные аспекты информационной сферы и задачи обеспечения информационной безопасности

Анализу гуманитарных аспектов информационной сферы и связанным с ними задачам обеспечения информационной безопасности Республики Беларусь в Концепции посвящена отдельная Глава 4. В ней показано, что быстрое развитие мирового и национального пространства и его открытость для активной работы иностранных СМИ и использования интернет-ресурсов гражданами Белоруссии выдвигают проблему повышения качества национального контента. Это необходимо для повышения доверия населения страны к официальной информации и обеспечения баланса интересов личности, общества и государства.

Постановка этой проблемы в рамках Концепции информационной безопасности представляется весьма своевременной и стратегически важной в современных условиях нарастания противоборства в информационной сфере. Ведь именно доверие к органам государственной власти и государственным СМИ являются сегодня необходимым условием обеспечения социальной стабильности общества и снижения риска возникновения в нем социальных потрясений [7].

Для выполнения этого условия в обществе должна осуществляться государственная информационная политика, направленная на повышение открытости планов и действий органов государственной власти, а также на повышение социальной ответственности средств массовой информации, в особенности, телевидения [8].

5 Технологические аспекты информационной сферы: глубокая цифровизация общества

В качестве основных направлений информатизации в Республике Беларусь, в Концепции информационной безопасности определены следующие:

- развитие эффективной и прозрачной системы государственного управления, в которой обеспечиваются быстрые, удобные и безопасные коммуникации между государством, бизнесом и гражданами;
- модернизация национальной информационной инфраструктуры;
- внедрение ИКТ в реальном секторе экономики и социальной сфере;
- укрепление отрасли информационных технологий.

Здесь отмечается, что цифровая трансформация экономики является важнейшей составляющей процесса формирования в стране информационного общества и одним из главных направлений развития Республики Беларусь. С этой целью в ближайшие десятилетия *все отрасли, рынки и сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели*. При этом получают развитие технологии, основанные на системах искусственного интеллекта, использования нейронных сетей, распределенных вычислений и блокчейн-технологий.

Таким образом, из анализа содержания данного раздела Концепции мы видим, что развитие цифровой экономики рассматривается в ней не как самоцель, а лишь как одно из направлений построения в стране *информационного общества*. К аналогичному пониманию этого процесса приходят сегодня и в России. Так, например, в Указе Президента РФ о национальных целях России на период до 2030 года [9], в качестве одной из пяти таких целей, определено не развитие цифровой экономики, а *цифровая трансформация общества*. И это вполне логично, так как понятие цифровой трансформации общества является существенно более широким и охватывает не только экономическую сферу, но также и многие другие сферы жизнедеятельности российского общества [10].

6 Государственная политика обеспечения информационной безопасности

Анализу гуманитарных аспектов информационной сферы и связанным с ними задачам обеспечения информационной безопасности Республики Беларусь в Концепции посвящена отдельная Глава 4. В ней показано, что быстрое развитие мирового и национального пространства и его открытость для активной работы иностранных СМИ и использования интернет-ресурсов гражданами Белоруссии выдвигают проблему *повышения качества национального контента*. Это необходимо для повышения доверия населения страны к официальной информации и обеспечения баланса интересов личности, общества и государства.

Постановка этой проблемы в рамках Концепции информационной безопасности представляется весьма своевременной и стратегически важной в современных условиях нарастания противоборства в информационной сфере. Ведь именно доверие к органам государственной власти и государственным СМИ являются сегодня необходимым условием обеспечения социальной стабильности общества и снижения риска возникновения в нем социальных потрясений [7].

Для выполнения этого условия в обществе должна осуществляться государственная информационная политика, направленная на повышение открытости планов и действий органов государственной власти, а также на повышение социальной ответственности средств массовой информации, в особенности, телевидения [8].

7 Геополитические аспекты информационной безопасности

В Концепции введено новое понятие – *информационный суверенитет*. Его содержание определяется как «неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность».

Отмечается, что информационный суверенитет достигается, прежде всего, путем формирования такой системы правового регулирования отношений в информационной сфере, которая обеспечивает безопасное устойчивое развитие, социальную справедливость и согласие. С

этой целью в обществе «воспитывается и стимулируется критическое отношение к проявлениям неуважения национальных устоев, традиций и нарушения норм морали и права в информационной сфере, нетерпимость к дезинформации, информационным манипуляциям и иным неявным информационно-психологическим воздействиям».

Как видим, и здесь гуманитарные методы обеспечения информационной безопасности рассматриваются в качестве приоритетных. При этом государством формируются такие границы деятельности зарубежных и международных субъектов в информационном пространстве, которые должны обеспечить *противодействие их культурной и информационной экспансии и вмешательству во внутренние дела страны*.

В то же время отмечается, что стремление Белоруссии к информационному суверенитету не расходится с международными принципами обеспечения прав и свобод, гарантирующих конкурентное и свободное развитие в условиях мировой трансформации.

Информационный нейтралитет. Это еще один новый термин, который используется в тексте Концепции информационной безопасности Республики Беларусь. В ней указано, что реализация этого принципа предусматривает проведение *миролюбивой внешней информационной политики*, уважение общепризнанных прав любого государства в информационной сфере, невмешательство в информационную сферу других стран.

Вместе с тем, в Концепции отмечается необходимость повышения степени присутствия Белоруссии в мировом информационном пространстве и заключения соглашений по обеспечению международной информационной безопасности.

8 Безопасность информационной инфраструктуры

Этой проблеме в Концепции целиком посвящен Раздел 5, который включает в себя пять глав, в каждой из которых рассматриваются определенные аспекты этой проблемы.

Вначале здесь показаны новые риски, вызовы и угрозы, которые в современных условиях глобальной информатизации общества и нарастания противоборства в информационном пространстве и обуславливают необходимость обеспечения безопасности национальной информационной инфраструктуры.

В числе этих вызовов и угроз в качестве наиболее важных названы *киберпреступления*, количество которых в мире непрерывно растет, а также кибератаки и кибероперации, которые осуществляются как кибертеррористами, так и кибервойсками – специальными воинскими подразделениями, которые сегодня имеются в составе армий ряда стран мира.

Объектами этих операций могут быть критически важные системы жизнеобеспечения населения, а также автоматизированные системы промышленной, энергетической, транспортной и финансовой инфраструктуры страны. При этом, отмечается, что эти угрозы настолько серьезны, что в доктринальных стратегических документах ряда стран рассматривается возможность реагирования на такие кибератаки как на вооруженную агрессию.

В качестве приоритетных задач в данной области, в Концепции рассматривается необходимость обеспечения *киберустойчивости национального сегмента сети Интернет*, а также снижение зависимости страны от зарубежных производителей программного обеспечения и аппаратных средств информационной инфраструктуры. С этой целью ставится задача создания *единой государственной системы мониторинга национального сегмента сети Интернет* и формирования облачной платформы для предоставления комплексных сервисов информационной безопасности как государственному сектору, так и бизнес-сообществу страны.

При этом отмечается, что достижение необходимого уровня защиты сервисов электронного правительства и киберустойчивости государственных услуг должно обеспечиваться, главным образом, за счет их безопасного проектирования и эксплуатации.

9 Обеспечение безопасности информационных ресурсов

Этой проблеме посвящен отдельный раздел Концепции, состоящий из пяти глав. В нем показана возрастающая значимость информационных ресурсов в современном обществе и актуальность их защиты от несанкционированного доступа, хищения и деструктивных воздействий, которые в последние годы усиливаются и осуществляются не только в корыстных, но также и в политических, разведывательных и военных целях.

Рассмотрены источники этих угроз и основные направления государственной политики по обеспечению безопасности информационных ресурсов. Ее главными целями являются защита государственной и служебной тайны и персональных данных граждан страны, а также безопасность информации ограниченного распространения. При этом, государством обеспечивается запрет цензуры и гарантируется оперативное доведение до населения общедоступной информации.

Необходимо отметить, что столь детальное рассмотрение проблематики информационных ресурсов, которое представлено в данной Концепции, на уровне доктринальных документов такого уровня выполнено впервые. Это, безусловно, повышает научно-методологическую значимость и практическую полезность этой Концепции.

10 Критические замечания по содержанию Концепции

Проведенный выше анализ Концепции информационной безопасности Республики Беларусь показал, что по ее содержанию можно сделать следующие замечания:

1. В числе угроз для национальной и информационной безопасности не указан *кризис культуры*, который в настоящее время приобрел системный характер и является одной из глобальных угроз для дальнейшего развития цивилизации [11]. Одной из проблем противодействия этой угрозе является обеспечение *интеллектуальной безопасности*, направленное на защиту интеллектуальной сферы общества от внешних и внутренних деструктивных воздействий, а также на сохранение способностей человека понимать и адекватно оценивать происходящие события и процессы [12].
2. Значительное внимание в Концепции уделено проблемам защиты национальных духовных ценностей от внешних и внутренних деструктивных воздействий. Однако, источники этих угроз не показаны, поэтому и необходимые мероприятия по противодействию этим угрозам остаются безадресными и недостаточно конкретными.
3. Недостаточно раскрыта в Концепции проблема обеспечения *лингвистической безопасности* [13], связанная с использованием в Белоруссии русского языка. В ней указано, что в стране существует двуязычие, однако когнитивная роль русского языка, на котором сегодня представлены не только ценности русскоязычной культуры, но также и многие современные знания в области науки, технологий, медицины и образования [14], в этом документе не раскрываются. Поэтому разделы Концепции, посвященные государственной политике в данной области, являются не полными.
4. Не рассмотрена весьма острая сегодня проблема *информационно-психологической безопасности*, которая быстро нарастает в условиях массового распространения мобильной информационной техники, глобального телевидения и развития социальных компьютерных сетей. Исследования показывают, что она приобретает глобальный характер и особенно опасна для молодого поколения [15]. Эта проблема сегодня явно недооценивается, хотя она выдвигается на первый план и требует безотлагательных и эффективных мер противодействия этой новой угрозе.
5. Практически не представлены в Концепции новые риски, вызовы и угрозы, связанные с развитием интернета вещей и *технологий искусственного интеллекта*, бурное развитие которых в мире уже началось и в ближайшие годы будет быстро нарастать [16].
6. Не сформулирована в Концепции также и проблема формирования в обществе *культуры информационной безопасности*, решение которой требует адекватных изменений в содержании образования [17,18].
7. В Концепции отмечается прямая зависимость жизни и здоровья населения, а также экономической и социальной безопасности от *надежности и защищенности* автоматизированных систем на объектах промышленности, транспорта и энергетики, электросвязи, здравоохранения и систем жизнеобеспечения. Однако, этого недостаточно, поскольку эта зависимость быстро возрастает и становится одним из критических факторов риска. Поэтому необходимо также решать и проблему обеспечения *живучести автоматизированных систем* на этих объектах. Они должны обладать способностью выполнять свои важнейшие функции (пусть, в ограниченном составе) также и в условиях выхода из строя их некоторых компонентов. Концептуальные подходы к решению этой проблемы уже разрабатываются в России [19,20].

Заключение

Разработка и принятие Концепции информационной безопасности Республики Беларусь, безусловно, является важным шагом на пути укрепления национальной безопасности этой страны. Вместе с тем, это также и новое достижение в области методологии комплексной постановки проблемы обеспечения информационной безопасности, которая в последние годы становится все более актуальной и для других стран, включая Россию. Поэтому, несмотря на приведенные выше замечания по содержанию Концепции, которые нам представляются принципиально важными, она заслуживает самого внимательного изучения.

Представляется также целесообразным активировать сотрудничество между российскими и белорусскими специалистами в данной области, предметное поле которой быстро расширяется и становится все более значимым для обеспечения национальной и международной безопасности.

Литература

1. Концепция информационной безопасности Республики Беларусь. Утверждена Постановлением Совета Безопасности Республики Беларусь № 1 от 18 марта 2019 г.
2. Колин К.К. Информационная безопасность как гуманитарная проблема // Открытое образование, 2006, № 1. С. 86-93.
3. Соколов И.А., Колин К.К. Развитие информационного общества в России и актуальные проблемы информационной безопасности // Информационное общество, 2009, № 4-5. С. 98-107.
4. Зацаринный А.А., Киселев Э.В., Козлов С.В., Колин К.К. Информационное пространство цифровой экономики. Концептуальные основы и проблемы формирования. М.: ФИУ ИУ РАН, 2018. 236 с.
5. Шваб Клаус. Четвертая промышленная революция. М.: Изд-во «Э», 2017. 208 с.
6. Колин К.К. Информационная цивилизация. М.: ИПИ РАН, 2001. 112 с.
7. Колин К.К. Социальная стабильность общества как стратегический фактор национальной и глобальной безопасности / Стратегические приоритеты, 2018, № 2. С. 4-11.
8. Астафьева О.Н., Колин К.К. Концептуальные основы государственной политики в области духовной культуры для обеспечения единства российского народа и национальной безопасности Российской Федерации. Челябинск.: Челябинская государственная академия культуры и искусств, 2010. 68 с.
9. Указ Президента РФ «О национальных целях Российской Федерации на период до 2030 года» от 21 июля 2020 г. № 474.
10. Зацаринный А.А., Колин К.К. Теория и практика цифровой трансформации общества в рамках приоритетов научно-технологического развития России // Проектирование будущего. Проблемы цифровой реальности, 2019. С. 29-39.
11. Колин К.К. Системный кризис культуры: структура и содержание проблемы // Стратегические приоритеты, 2014, № 3. С. 6-27.
12. Колин К.К. Интеллектуальная безопасность – новая глобальная проблема XXI века // Стратегические приоритеты, 2019, № 3-4. С. 6-27.
13. Колин К.К., Кошкин Р.П., Сибиряков П.Г. Лингвистическая безопасность России и проблемы защиты русского языка // Стратегические приоритеты, 2019, № 1. С. 91-128.
14. Колин К.К. Русский язык и актуальные проблемы национальной безопасности России и стран Евразии // Alma mater (Вестник высшей школы), 2007, № 7. С. 3-12.
15. Колин К.К. Биосоциология молодежи и проблема интеллектуальной безопасности в информационном обществе // Знание. Понимание. Умение. 2012, № 3. С. 156-162.
16. Колин К.К. Цифровая революция и искусственный интеллект: новые горизонты и опасности // Партнерство цивилизаций, 2020, № 1-2. С. 100-106.
17. Колин К.К., Роберт И.В. Социальные аспекты информатизации образования. М.: ИИО РАО, ИПИ РАН, 2004. 53 с.
18. Соколов И.А., Колин К.К. Новый этап информатизации общества и актуальные проблемы образования // Информатика и ее применения, 2008. Т.2, № 1. С. 67-76.
19. Быстров И.И. Живучесть автоматизированных организаций. М.: Майор: Осипенко, 2016. 506 с.
20. Быстров И.И., Веселов В.Н., Колин К.К. Основы живучести автоматизированных организаций информационного общества // Системы и средства информатики, 2018. Т. 28. № 4. С. 106-117.

THE CONCEPT OF INFORMATION SECURITY OF THE REPUBLIC OF BELARUS: A NEW UNDERSTANDING OF THE STRUCTURE AND CONTENT OF A COMPLEX PROBLEM

Kolin, Konstantin Konstantinovich

Doctor of technical sciences, professor

Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Institute of Informatics Problems

Moscow, Russia

kolinkk@mail.ru

Abstract

The article analyzes the structure and content of the problem of ensuring information security of the country, presented in the concept of information security of the Republic of Belarus. It shows the high scientific and methodological level of development of this topical and complex problem, as well as the need for its further study by specialists in this field, as well as scientists and University teachers. A number of significant comments and recommendations on the content of the Concept text are formulated and some important results obtained in this field by Russian scientists are shown.

Keywords

information security, information sphere, humanitarian problems, intellectual security, Russian language, survivability of information systems

References

1. Kontsepsiya informatsionnoy bezopasnosti Respubliki Belarus. Utverzhdena Postanovleniyem Soveta Bezopasnosti Respubliki Belarus, № 1 ot 18 marta 2019 g.
2. Kolin K. K. Informatsionnaya bezopasnost' kak gu-manitarnaya problema [Information security as a human-itarian problem] // Otkrytoe Obrazovanie [Open Education], 2006, No1. S. 86-93.
3. Sokolov I. A., Kolin K. K. 2009. Razvitie infor-matsionnogo obshchestva v Rossii i aktual'nye problemy informatsionnoy bezopasnosti [Information society de-velopment in Russia and problems of information secu-rity]. // Informatsionnoe Obshchestvo [Information Society], No 4-5. S. 98-107.
4. Zatsarinnyy A.A., Kiselev E.V., Kozlov, S.V., Kolin, K.K. Informatsionnoye prostranstvo tsifrovoy ekonomiki. Kontseptualnyye osnovy i problemy formirovaniya. M.: FIC IU RAN, 2018. 236 s.
5. Shvab Klaus. Chetvertaya promyshlennaya revolyutsiya. M.: Izd-vo «E», 2017. 208 s.
6. Kolin K.K. Informatsionnaya tsivilizatsiya. M.: IPI RAN, 2002. 112 s.
7. Kolin K.K. Sotsialnaya stabilnost obshchestva kak strategicheskii faktor natsionalnoy i globalnoy bezopasnosti // Strategicheskiye prioritety, 2018, No. 2. S. 4-11.
8. Astafyeva O.N., Kolin K.K. 2010. Kontseptualnyye osnovy gosudarstvennoy politiki v oblasti dukhovnoy kultury dlya obespecheniya edinstva rossiyskogo naroda i natsionalnoy bezopasnosti Rossiyskoy Federatsii. . Chelyabinsk: Chelyabinskaya gosudarstvennaya akademiya kultury i iskusstv, 2010. 68 s.
9. Ukaz Prezidenta RF «O natsionalnykh tselyakh Rossiyskoy Federatsii na period do 2030 goda» ot 21 iyulya 2020 g. № 474.
10. Zatsarinnyy A.A., Kolin K.K. 2019. Teoriya i praktika tsifrovoy transformatsii obshchestva v ramkakh prioriteto-vo nauchno-tekhnologicheskogo razvitiya Rossii // Proyektirovaniye budushchego. Problemy tsifrovoy realnosti. 2019, No 2. S. 29-39.
11. Kolin K.K. Sistemnyy krizis kultury: struktura i sodержaniye problemy // Strategicheskiye prioritety, 2014, No. 3. S. 6-27.
12. Kolin K.K. Intellektualnaya bezopasnost – novaya globalnaya problema XXI veka // Strategicheskiye prioritety, 2019, No. 3-4. S. 6-27.
13. Kolin K.K., Koshkin R.P., Sibiryakov P.G. Lingvisticheskaya bezopasnost Rossii i problemy zashchity russkogo yazyka // Strategicheskiye prioritety, 2019, No. 1. S. 91-128.

14. Kolin K.K. Russkiy yazyk i aktualnyye problemy natsionalnoy bezopasnosti Rossii i stran Evrazii // Alma mater (Vestnik vysshey shkoly), 2007, No 7. S. 3-12.
15. Kolin K.K. Biosotsiologiya molodezhi i problema intellektualnoy bezopasnosti v informatsionnom obshchestve // Znaniye. Ponimaniye. Umeniye, 2012, No. 3. S. 156-162.
16. Kolin K.K. 2020. Tsifrovaya revolyutsiya i iskusstvennyy intellekt: novyye gorizonty i opasnosti // Partnerstvo tsivilizatsiy. 1-2. 100-106.
17. Kolin K.K., Robert. I.V. Sotsialnyye aspekty informatizatsii obrazovaniya. M.: IIO RAO. IPI RAN. 2004. 53 s.
18. Sokolov, I. A., Kolin, K.K. 2008. Novyy etap informatizatsii obshchestva i aktual'nye problemy obrazovaniya [The new stage of the society informatization and actual problems of education]. Informatika i ee Primeneniya. 2(1):67-76.
19. Bystrov I.I. Zhivuchest avtomatizirovannykh organizatsiy. M.: Mayor: Osipenko, 2016. 506 s.
20. Bystrov I.I., Veselov V.N., Kolin K.K. 2018. Osnovy zhivuchesti avtomatizirovannykh organizatsiy informatsionnogo obshchestva // Sistemy i sredstva informatiki, 2018, No 4. S. 106-117.