УДК 338.2
ББК 67.301

DOI 10.24411/2618-9852-2020-15101

МЕЖДУНАРОДНЫЙ ОПЫТ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***И. Д. Бекмурзаев*[1], *А. Х. Курбанов*[2], *С. Д. Хажмурадова*[1]**

[1] Чеченский государственный университет, Грозный, Россия
[2] Военная академия материально-технического обеспечения им. генерала армии А. В. Хрулёва, Санкт-Петербург, Россия

В современной России существует целый ряд сложных проблем в сфере информационной безопасности, требующих безотлагательного и кардинального решения. Для развития эффективной системы национальной информационной безопасности необходимо тщательное изучение опыта ведущих стран мира, которые осуществляют эффективную информационную защиту своего государства и граждан. В современном мире уже разработаны основные принципы и инструментальные средства формирования эффективной защиты национального информационного пространства. Новизна работы заключается в предложениях по разработке целостного кодификационного документа, который полноценно охватил бы различные аспекты формирования государственной политики в сфере национальной безопасности, а также определил конкретный инструментарий ее реализации.

Ключевые слова: *экономика, политика, культура, информационное пространство, информационная безопасность, политика информационной безопасности.*

INTERNATIONAL EXPERIENCE IN ENSURING NATIONAL INFORMATION SECURITY

***I.D. Bekmurzaev*[1], *A.Kh. Kurbanov*[2], *S.D. Khazhmuradova*[1]**

[1] Chechen State University, Grozny, Russia
[2] Military Academy of logistics named after General of the army A.V. Khrulev, Saint-Petersburg, Russia

In modern Russia, there are a number of complex problems in the field of information security that require urgent and radical solutions. To develop an effective system of national information security, it is necessary to carefully study the experience of the leading countries of the world that carry out effective information protection of their state and citizens. In the modern world, the basic principles and tools for creating effective protection of the national information space have already been developed. The novelty of the work lies in the proposals for the development of a complete codification document that would fully cover various aspects of the formation of state policy in the field of national security, as well as identify specific tools for its implementation.

Keywords: *economy, politics, culture, information space, information security, information security policy.*

Информация стала мощным средством манипулирования общественным и индивидуальным сознанием, а также реальным оружием, которое используется в конфликтах нового типа, конфронтациях и противостояниях. Создание возможностей доступа каждого к источникам информации, формирование умения пользоваться ею и одновременно защита людей от грязных информационных потоков создают своеобразное предметно-исследовательское поле, одним из наиболее актуальных аспектов которого является проблема формирования и реализации политики информационной безопасности на государственном, общественном и гражданском уровнях.

Еще одним аспектом актуализации проблематики информационной безопасности является то, что именно информация является одним из основных инструментов выстраивания архитектуры современной глобальной цивилизации. Государства-лидеры глубоко осознают, что именно контроль над информационными ресурсами и эффективное использование новейших информационных технологий способны поддерживать их лидерство. Это в значительной мере актуализирует проблематику информационной безопасности и суверенитета отдельных государств, являющихся как субъектами, так и объектами информационных воздействий различного характера.

Исследованию этой проблематики посвящено значительное количество научных публикаций и рекомендаций практических политиков. В западной научной литературе веское слово в этом контексте выразили такие знаменитые исследователи, как Д. Белл [3], И. Масуда [13], Т. Стоуньер [11] и др.

Не выработано эффективной модели системного обеспечения информационной безопасности государства, общества и человека, хотя такая необходимость зафиксирована на конституционном уровне. Поэтому сегодня очень важно разработать целостный кодификационный документ, который полноценно охватил бы различные аспекты формирования государственной политики в сфере национальной безопасности, а также определил конкретный инструментарий ее реализации.

В различных государствах разработаны основные принципы и инструментальные средства формирования эффективной защиты национального информационного пространства. Применяя различные средства, страны-лидеры достаточно эффективно осуществляют национальную политику информационной безопасности. Российской Федерации необходимо изучить и адекватно применить зарубежный опыт, трансформируя его в соответствии с национальной спецификой и уникальной ролью государства в современной геополитике. В нашей стране имеется ряд сложных проблем в сфере информационной безопасности, требующих безотлагательного и кардинального решения. В то же время их решение предполагает не только концептуально-теоретическое исследование вопросов информационной безопасности, но и формирование такого национального законодательства, которое бы обеспечило эффективную нормативно-правовую основу деятельности различных субъектов информационного пространства. Наиболее развитые системы информационной безопасности функционируют в США, Великобритании, Израиле, ФРГ, Китае. То есть в тех странах, которые постоянно находятся под мощным внешним информационным воздействием, а потому вынуждены создавать национальные системы информационной защиты. Притом указанные системы перечисленных стран имеют и достаточную активную составляющую, благодаря чему существует возможность проведения информационно-психологических мероприятий и кибернетических атак против стран-противников.

Особой эффективностью система информационной безопасности отличается у такого глобального геополитического игрока, как Соединенные Штаты Америки. Необходимо отметить, что система информационной безопасности в США является чрезвычайно многомерной и сложной, опирающейся на достаточно детализированное, но подчиненное единой стратегии федеральное и местное законодательство. «Законодательство США в сфере обеспечения информационной безопасности — это совокупность федеральных законов и законов штатов, которые создают правовую основу для осуществления государственной политики в этой сфере. Довольно полно в законодательстве урегулирован вопрос относительно обеспечения безопасности информации в государственных компьютерных системах (закон “О компьютерной безопасности”, закон “О совершенствовании информационной безопасности”), борьбы с компьютерной преступностью (закон “О компьютерном мошенничестве и злоупотреблениях”, закон “О злоупотреблении компьютерами”), регулирования соотношения прав граждан на получение информации (закон “О свободе информации”, закон “Об освещении деятельности правительства”) и конфиденциальность их частной жизни (закон “Об охране личных тайн”). Административно-организационное обеспечение информационной безопасности в США направлено на координацию всех действий по защите информации и проведение единой государственной политики информационной безопасности. Президент США является

основным ответственным лицом за обеспечение национальной безопасности в целом и информационной безопасности в частности» [9].

Развитые страны Европы также большое внимание уделяют всестороннему обеспечению в рамках национальной политики безопасности гражданского общества от информационных угроз, возникающих в современном глобальном информационном обществе. Так, во Франции информационный сектор функционирования национального общества определяется одним из ключевых, наряду с экономикой, политикой, культурой. Защита информационного пространства признается одним из ключевых и важнейших направлений обеспечения национальной безопасности. «Франция считает, что в ряде основных секторов, нуждающихся в государственной защите наряду с энергетикой, транспортом, финансами является информационная сферы, в частности система обеспечения безопасности информации ограниченного пользования, прежде всего, государственной тайны и телекоммуникационные службы. Можно сделать вывод, что именно в этом проявляется новый элемент в понятии современной многовекторности геостратегии французской правящей элиты, что непосредственно влияет на особенности выбора способов использования оперативных возможностей национальных спецслужб, СМИ и других государственных и неправительственных структур, привлеченных к реализации политики информационной безопасности французского общества и государства. Как следствие, национальное информационное пространство Французской Республики становится основным объектом защиты во время формирования соответствующих задач, структуры механизма и современного понятия тактики реализации его сил и средств в разведывательно-информационных и разведывательно-подрывных мероприятиях, в частности в деятельности спецслужб по проведению специальных мероприятий, связанных с защитой французского информационного пространства от негативных внешних проявлений» [8]. Таким образом, информационное пространство во Франции рассматривается как один из приоритетных объектов защиты, который осуществляется всеми возможными законотворческими, организационно-управленческими, силовыми и информационно-технологическими средствами. Попутно французское правительство и гражданское общество постоянно проводят мониторинговые мероприятия, всячески предотвращая возможные попытки со стороны государственных функционеров ограничивать демократию, оправдываясь необходимость осуществления определенных мер по контролю над национальным информационным пространством.

Менее демократично в этом вопросе ведет себя правительство Китайской Народной Республики. В информационной политике Китая доминируют принципы воплощения достаточно моноцентрических оборонительных и наступательных доктрин. Использование мощной и широкой ресурсной базы позволяет Китаю проводить достаточно эффективную информационную политику, даже несмотря на ее недемократическую направленность. «Политика информационной безопасности определяет приоритетными направлениями деятельности государства разработку национальных стратегий, которые объединяют оборонительные и наступательные доктрины для обеспечения национальных интересов и защиты внутренней информационной среды и информационной инфраструктуры, преодоление асимметричности информационного развития. Все структурные составляющие государственной информационной политики обусловлены необходимостью обеспечения национальных интересов путем реализации китайской модели информационного общества и специфики интеграции КНР в глобальную информационную среду. Включение стратегии государственной информационной политики в правительственные программы дает Китаю возможность реформировать политическую идеологию в контексте современных тенденций международного развития. Участие КНР в процессах международной региональной интеграции формирует стратегию информационной политики государства, которая заключается в одновременной интеграции в мировую систему международных отношений и практической реализации национальной модели информационализма как фактора модернизации политической системы КНР и ее потенциального лидерства на региональном и международном уровнях» [4]. Таким образом, можно отметить успешные попытки Китая в реализации собственной модели информационной политики, которая охватывает как внутренние проблемы страны, так и ее региональные и глобальные геополитические притязания. Во многом именно благодаря разработке собственной модели информационализма КНР постепенно преуспевает, выполняя задачи по превращению в одного из ключевых игроков в глобальной геополитической «шахматной доске», создавая значительную конкуренцию не только Европе, но и Соединенным Штатам Америки.

Таким образом, в мире существуют страны с разными традициями государственного управления, которые достаточно эффективно осуществляют национальную политику

информационной безопасности, применяя различные средства: от создания систематизированной нормативно-правовой базы до использования значительных материально-технологических ресурсов. Изучая успешный опыт стран-лидеров, можно извлекать определенные моменты, которые повлекли бы положительное влияние на решение многих проблем, существующих сегодня в безопасности информационного пространства.

Для построения эффективной системы информационной безопасности в первую очередь необходимо провести значительную аналитическую подготовку, на основе которой четко определиться с приоритетами и ориентирами дальнейшей государственной информационной политики. Кроме того, важно выбирать такие средства информационной защиты, которые бы были достаточно эффективными на данный момент. Это также требует серьезного концептуально-теоретического поиска в области определения основных принципов государственной информационно-политики безопасности.

Продолжением концептуально-теоретических исследований в области информационной безопасности должно стать создание систематизированного национального законодательства, что подводило бы нормативно-правовую основу под деятельность различных субъектов, в том числе и государства, в сфере обеспечения различных уровней информационной безопасности общества. Особенно важно, с нашей точки зрения, учесть при этом успешный опыт европейских стран, эффективно защищающих свое информационное пространство от внеш0них воздействий. Назрела насущная необходимость осуществления кодификации информационного законодательства нашей страны. Внимание акцентируется на необходимости принятия такого нормативно-правового акта, положениями которого предусмотрены основные принципы информационного развития государства, регулирующего деятельность органов государственной власти по обеспечению информационной безопасности, определению ключевых принципов обеспечения информационной безопасности человека, общества, государства и дальнейшего информационного развития, своевременному выполнению которых будет способствовать укреплению информационной безопасности и выведению деятельности по ее укреплению на качественно новый уровень.

Отличительными чертами кодификации являются: 1) при подготовке кодифицированного документа пересматривается вся система правовых норм; 2) кодификация осуществляется периодически, в зависимости от накопления нормативного материала и объективной необходимости; 3) кодификация затрагивает правовые предписания и юридические институты; 4) результатом кодификационной работы система права пополняется новым источником права; 5) носит официальный характер.

Цель кодификации — обновление правового регулирования, устранение несогласованности, противоречий между действующими нормами.

Таким образом, кодификация национального законодательства в области информационной безопасности может решить проблему систематизации данной сферы государственной и общественной жизнедеятельности. Важно лишь, чтобы такая кодификация происходила на основе четко разработанных и структурно выстроенных теоретико-методологических основ исследования информационно-безопасного сегмента деятельности государства и гражданского общества.

Кроме того, теоретическая проблематика информационной безопасности исследуется в рамках современного философско-политологического дискурса, доказывает свою актуальность и в вопросах государственного и общественного управления. Именно информация становится инклюзивным, интегративным, сквозным ресурсом, что позволяет максимально эффективно управлять сообществом в рамках современной информационной цивилизации.

Эффективное управление современным информационным обществом должно обязательно предусматривать формирование государственной информационной политики и создание условий ее реализации, а целью этой деятельности должно стать согласование системно-функциональной и информационной составляющих в условиях стремительного распространения процессов глобализации. Отсюда понятно, почему проблема обеспечения информационной безопасности вошла в число наиболее значимых и приоритетных задач, решение которых необходимо для существования и дальнейшего развития нашего общества. Информационная безопасность важна потому, что мы защищаем свое информационное пространство, а следовательно, свои информационные ресурсы, свою национальную культуру. Таким образом, философская специфика проблематики информационной безопасности заключается в том, что информация сегодня стала ресурсом глобального объединения человечества, что несет много новых возможностей, но ставит перед отдельными сообществами и человечеством в целом новые вызовы и риски. От того, сможем ли мы ответить на эти вызовы максимально адекватно, защитив свое информационное пространство от многих опасностей, во многом зависит успех и своевременность государственных усилий.

Сегодня успешное развитие демократическо-правового государства и гражданского общества возможно только в условиях полноценного использования информационных ресурсов, а также установления четкой государственной политики, которая обеспечила бы высокий уровень национальной информационной безопасности. Фактически информационная безопасность государства и национального социума становится ключевым фактором демократических преобразований внутри страны, а также ее выхода на конкурентоспособный уровень в региональном и глобальном масштабе. Практическое обеспечение национальной информационной безопасности возможно за счет единства всех факторов: политического, экономического, правового, организационного и др. Национальная информационная безопасность — реальный фактор успешной геостратегической политики, одновременно с демократическим общественным развитием. Это и обуславливает значительный уровень актуальности концептуально-теоретических исследований философско-политологического характера, направленных на изучение всей полноты возможностей, которые позволяют современным государствам и обществам защищать свое информационное пространство от огромного количества вызовов и проблем, возникающих в рамках глобальной информационной цивилизации. Этим обусловлена актуальность и важность определения теоретико-методологических основ исследования информационной безопасности.

Таким образом, определившись с основными источниками и детерминантами актуальности проблемы информационной безопасности, рассмотрев различные дискурсивные традиции и способы определения категории «информационная безопасность», а также проведя компаративный анализ отражения проблемы информационной безопасности в системе информационной политики нашей страны и ведущих стран мира, можем сделать ряд взаимосвязанных выводов.

Во-первых, определив основные истоки и детерминанты проблемы информационной безопасности, подтверждена значительная актуальность и многомерность концептуально-теоретического изучения и анализа данной проблемы в современном дискурсе. Прежде всего основной детерминантой актуальности проблематики информационной безопасности является значительный рост информационных потоков и обменов на глобальном уровне. Такой рост ставит много вызовов и трудностей, которые требуют постоянного исследования и решения. При этом информационные вызовы стоят перед всеми: человеком, обществом и государством. Это и создает чрезвычайную сложность концептуально-теоретического исследования проблем информационной безопасности. В нашем исследовании одним из основных методов определен комплексно-системный подход, на основе которого осуществляется целостное изучение проблем информационной безопасности, возникающих перед человеком, перед обществом и перед государством.

Во-вторых, проанализировав основные принципы и критерии определения понятия «информационная безопасность» общества в контексте современного философско-политологического дискурса, подчеркнуто значительное разнообразие таких определений. Отечественные и зарубежные исследователи данной проблематики, определяя категорию информационной безопасности, обращаются к таким ее аспектам, как глобально-цивилизационная значимость, роль в обеспечении национальной безопасности и обороны, определения информационно-технологических параметров безопасности, значение обеспечения информационной безопасности каждой отдельной личности или конкретных социальных общностей. Учитывая такое многообразие подходов, ключевым теоретико-методологическим принципом нашего исследования избран принцип системности, на основе которого делается комплексный, структурно-функциональный анализ категории «информационная безопасность» с учетом ее индивидуальных, социальных, государственных и глобальных измерений. При таком рассмотрении особенно важно сформулировать интегративные факторы, объединяющие информационную безопасность государства и общества с информационно-психологической и идейно-феноменологической безопасностью каждого человека. Учитывая такие теоретико-методологические основы исследования проблемы информационной безопасности, мы определяем данное понятие как вид национальной безопасности, направленный на обеспечение прав и свобод человека относительно свободного доступа к информации, создания и внедрения безопасных информационных технологий и защиту прав собственности всех участников информационной деятельности.

В-третьих, осуществив компаративный обзор проблемы информационной безопасности в системе информационной политики, доказана необходимость разработки систематизированной стратегии формирования информационно-политики безопасности в нашем государстве. На сегодня в нашей стране еще не сформировано соответствующей современным геополитическим вызовам системы информационной безопасности. Существует необходимость усиления буквально

на всех направлениях: нормативно-правовом, организационно-управленческом, информационно-технологическом. Но прежде всего существует насущная необходимость выработки четкой стратегии осуществления преобразований в секторе информационной безопасности государства и национального общества. Такая стратегия должна основываться на прочном концептуально-теоретическом, научно-практическом базисе, который должен сформироваться в рамках национального политологического дискурса. Именно поэтому исследование многоаспектной проблематики информационной безопасности государства и человека является сегодня чрезвычайно актуальной и важной задачей, которая стоит перед научным сообществом нашей страны.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев, Ю. В. Проблемы суверенитета и международная безопасность / Ю. В. Андреев // Власть. — 2011. — № 1. — С. 34—35.

2. Бауман, З. Глобализация. Последствия для человека и общества / З. Бауман ; пер. с англ. Г. М. Дашевского. — Москва : Весь Мир, 2004. — 188 с.

3. Белл, Д. Социальные рамки информационного общества. Новая технократическая волна на Западе / Д. Белл ; под ред. П. С. Гуревича. — Москва : Прогресс, 1986. — С. 330—342. — URL: http://www.nethistory.ru/biblio/1043172230.html (дата обращения: 19.10.2019).

4. Государственная стратегия по обеспечению безопасности информационного пространства: Центральная ведущая группа по кибербезопасности КНР. — URL: http://www.cac.gov.cn/201612/27/c_1120195926.htm (дата обращения: 19.10.2019).

5. Дадаев, Я. Э. Цифровая экономика и четвёртая промышленная революция: перспективы для бизнеса / Я. Э. Дадаев, И. Д. Бекмурзаев // Современные контуры цифровой экономики России : материалы Междунар. науч.-практ. конф. — Грозный : Чечен. гос. пед. ун-т, 2018. — С. 639—643.

6. Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» : документ WSIS-03/GENEVA/DOC/4-R от 12.12.2003. — URL: http://goo.gl/EOXB6c (дата обращения: 19.10.2019).

7. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : утв. Президентом Рос. Федерации 24.07.2013 № Пр-1753. — URL: http://www.consultant.ru/document/cons_doc_LAW_178634/ (дата обращения: 19.10.2019).

8. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. — 3-е изд., стереотип. — Москва : Горячая линия — Телеком, 2018. — 542 с.

9. Противостоять угрозам терроризма и экстремизма страны БРИКС будут все вместе. — URL: http://www.yoki.ru/news/news/09-07-2015/441929-0/ (дата обращения: 19.10.2019).

10. Селиванов, А. И. Координация систем научного обеспечения стратегического управления стран БРИКС: задачи и перспективы / А. И. Селиванов. — URL: http://www.lawinrussia.ru/node/359017 (дата обращения: 19.10.2019).

11. Стоуньер, Т. Информационное богатство: профиль постиндустриальной экономики. Новая технократическая волна на Западе / Т. Стоуньер ; под ред. П. С. Гуревича. — Москва : Прогресс, 1986. — С. 392—410. — URL: http://www.nethistory.ru/biblio/1043172230.html (дата обращения: 19.10.2019).

12. Тэпскотт, Д. Цифровая экономика: перспективы и опасность в эпоху сетевого интеллекта / Д. Тэпскотт. — New York : McGraw-Hill, 1995. — 342 с.

13. Masuda, Y. The Information Society as Postindustrial Society / Y. Masuda. — Washington : World Future Soc. — 1983. — P. 29.

СВЕДЕНИЯ ОБ АВТОРАХ

Бекмурзаев Иса Дуквахович — кандидат экономических наук, доцент, и.о. заведующего кафедрой коммерции и маркетинга Чеченского государственного университета, Грозный, Россия. bekmurzaev71@mail.ru

Курбанов Артур Хусаинович — доктор экономических наук, профессор кафедры материального обеспечения Военной академии материально-технического обеспечения им. генерала армии А. В. Хрулёва, Санкт-Петербург, Россия. *kurbanov-83@yandex.ru*

Хажмурадова Самарт Денисламовна — студентка Чеченского государственного университета, Грозный, Россия. b*ekmurzaev71@mail.ru*

REFERENCES

1. Andreev Ju.V. Problemy suvereniteta i mezhdunarodnaja bezopasnost' [Problems of sovereignty and international security]. *Vlast'* [Power], 2011, no. 1, pp. 34—35. (In Russ.).

2. Bauman Z. *Globalizacija. Posledstvija dlja cheloveka i obshhestva* [Globalization. Consequences for a person and society]. Moscow, Ves' Mir Publ., 2004. 188 p. (In Russ.).

3. Bell D. *Social'nye ramki informacionnogo obshhestva. Novaja tehnokraticheskaja volna na Zapade* [The social framework of the information society. New technocratic wave in the West]. Moscow, Progress Publ., 1986. Pp. 330—342. Available at: http://www.nethistory.ru/biblio/1043172230.html, accessed 19.10.2019 (In Russ.).

4. *Gosudarstvennaja strategija po obespecheniju bezopasnosti informacionnogo prostranstva: Central'naja vedushhjaja gruppa po kiberbezopasnosti KNR* [State Strategy for Ensuring the Security of the Information Space: Central Leading Cybersecurity Group of China]. Available at: http://www.cac.gov.cn/201612/27/c_1120195926.htm, accessed 19.10.2019. (In Russ.).

5. Dadaev Ja.Je., Bekmurzaev I.D. Tsifrovaja jekonomika i chetvjortaja promyshlennaja revoljucija: perspektivy dlja biznesa [Digital economy and the fourth industrial revolution: prospects for business]. *Sovremennye kontury cifrovoj jekonomiki Rossii* [Modern contours of the digital economy of Russia]. Groznyj, Chechenskij gosudarstvennyj pedagogicheskij universitet Publ., 2018. Pp. 639—643. (In Russ.).

6. *Deklaracija principov «Postroenie informacionnogo obshhestva — global'naja zadacha v novom tysjacheletii»* [Declaration of Principles «Building an Information Society — A Global Challenge for the New Millennium»]. Available at: http://goo.gl, accessed 19.10.2019. (In Russ.).

7. *Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti na period do 2020 goda* [Fundamentals of the state policy of the Russian Federation in the field of international information security for the period until 2020]. Available at: http://www.consultant.ru/document/cons_doc_LAW_178634, accessed 19.10.2019. (In Russ.).

8. Manojlo A.V., Petrenko A.I., Frolov D.B. *Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny* [State information policy in the conditions of the information-psychological war]. Moscow, Gorjachaja linija — Telekom Publ., 2018. 542 p. (In Russ.).

9. *Protivostojat' ugrozam terrorizma i jekstremizma strany BRIKS budut vse vmeste* [The BRICS countries will confront the threats of terrorism and extremism all together]. Available at: http://www.yoki.ru/news/news/09-07-2015/441929-0, accessed 19.10.2019. (In Russ.).

10. Selivanov A.I. *Koordinacija sistem nauchnogo obespechenija strategicheskogo upravlenija stran BRIKS: zadachi i perspektivy* [Coordination of scientific support systems for strategic management of the BRICS countries: tasks and prospects]. Available at: http://www.lawinrussia.ru/node//, accessed 19.10.2019. (In Russ.).

11. Stoun'er T. *Informacionnoe bogatstvo: profil' postindustrial'noj jekonomiki. Novaja tehnokraticheskaja volna na Zapade* [Information wealth: a profile of the post-industrial economy. New technocratic wave in the West]. Moscow, Progress Publ., 1986. Pp. 392—410. Available at: http://www.nethistory.ru/biblio/1043172230.html, accessed 19.10.2019. (In Russ.).

12. Tjepskott D. *Cifrovaja jekonomika: perspektivy i opasnost' v jepohu setevogo intellekta* [Digital economy: prospects and danger in the era of network intelligence]. New York, McGraw-Hill Publ., 1995. 342 p. (In Russ.).

13. Masuda Y. *The Information Society as Postindustrial Society*. Washington, World Future Soc Publ., 1983. P. 29.