Сильное государство через право на информационную глобальную компетенцию
The strong state through the right to the information global competence

С.И. Луценко[1]

Эксперт НИИ Корпоративного и проектного управления (г. Москва). Аналитик Института экономический стратегий Отделения общественных наук Российской академии наук.

Соавтор документа «Стратегия развития электросетевого комплекса Российской Федерации».
Автор проекта «Контуры Концепции развития финансового кластера Российской Федерации на долгосрочную перспективу»
E-mail: scorp_ante@rambler.ru

S.I. Lutsenko

Lutsenko Sergej Ivanovich, Expert, The Corporate and Project Management Institute (Moscow), Analyst, Institute for Economic Strategies of the Social Sciences Division of the Russian Academy of Sciences (Moscow).
The co-author of the document «Strategy of development of an electric grid complex of the Russian Federation».
The author of the project «Contours of the Concept of Developing Financial Cluster of the Russian Federation in the Long-Term Period».

Автор рассматривает особенности пути развития России через цифровой пространство. Речь идет о создании интегрированной информационной системе (платформе) для формирования единого цифрового пространства. Единая информационная платформа должна базироваться на использовании отечественного программного обеспечения и отечественных средств защиты. В основе данной платформы должен быть принцип национальной безопасности.

The author considers features of a way of development of Russia through digital space. It is a question of creation to the integrated information system (platform) for forming of uniform digital space. The uniform information platform should be based on use of the domestic software and domestic protection frames. At the heart of the given platform there should be a principle of national security.

Ключевые слова: национальная безопасность, информационная платформа, цифровая экономика, цифровое пространство, KPI

Keywords: national security, information platform, digital economy, digital space, KPI

На сегодняшний день, вызывает обеспокоенность со стороны общества, связанная с быстрым развитием технологий и общества, поскольку Интернет и мобильные устройства повсеместно используются в повседневной жизни («сплошная компьютеризация»), и бизнес-модели большинства интернет-компаний строятся на обработке персональных данных, считает, что масштаб данной проблемы беспрецедентен, отмечает, что возможно возникновение ситуации, когда инфраструктура для массового сбора и обработки данных может быть использована в неправомерных целях при смене политического режима.

[1] Автор благодарит за Чеснокова А.Н. за идею и неоценимый вклад в статью.

Генеральная Ассамблея Организации Объединенных Наций приняла Резолюцию № 68/167 от 18.12.2013 «Право на неприкосновенность личной жизни в цифровой век», в которой она выразила глубокую обеспокоенность тем, что слежение за сообщениями и/или их перехват, включая экстерриториальное слежение за сообщениями и/или их перехват, а также сбор личных данных, особенно в массовом масштабе, могут иметь негативные последствия для осуществления и реализации прав человека.

Верховным комиссаром Организации Объединенных Наций по правам человека был представлен 30.06.2014 доклад о праве на неприкосновенность личной жизни в цифровой век.

В частности, в докладе отмечалась обеспокоенность по поводу сообщений о том, что Агентство национальной безопасности Соединенных Штатов Америки совместно с Центром правительственной связи Соединенного Королевства Великобритании и Северной Ирландии разработали технологии, позволяющие получить доступ практически ко всему мировому интернет-трафику, спискам телефонных звонков в США, электронным адресным книгам отдельных лиц и огромным объемам другой цифровой информации, и что эти новые средства были развернуты при помощи транснациональной сети с использованием стратегических партнерств разведслужб обоих государств, рычагов регулирования деятельности частных компаний и коммерческих контрактов, Верховный комиссар ООН подчеркнул, что перехват электронно-цифровых коммуникаций и сбор личных данных могут сказываться и на осуществлении других прав, помимо права на неприкосновенность частной жизни, к которым относятся право на свободу убеждений и их свободное выражение, право искать, получать и распространять информацию, право на свободу мирных собраний и свободу ассоциации, право на семейную жизнь.

Не может считаться соразмерной практика обязательного хранения данных третьей стороны - стандартная практика слежения во многих странах, где государства обязывают телефонные компании и компании, поставляющие интернет-услуги, хранить метаданные о контактах и местоположении клиентов для последующего использования в рамках правоохранительной деятельности, равно как и для предоставления разведывательным агентствам.

Тот факт, что Интернет и остальное цифровое пространство во многом контролируются частными структурами (по преимуществу корпорациями США), угрожает верховенству права. Частные компании могут навязывать ограничения (или же «поощряться» за это) в отношении доступа к информации, при этом не подвергаясь ограничениям на основании конституционного и международного права, поскольку последние распространяются исключительно на государства. Эти частные компании могут также получать указания от национальных судов, действующих по просьбе других частных компаний, осуществлять весьма интрузивный анализ данных для выявления реальных (или вероятных) нарушений прав частной собственности, а зачастую и прав интеллектуальной собственности. Могут быть даны указания «изъять» данные, в том числе правительственные, коммерческие и личные, из серверов в других странах для целей соблюдения закона или для обеспечения национальной безопасности. Это может происходить в отсутствие согласия другой страны, компании или иных субъектов этих данных, в нарушение суверенитета стран, коммерческой тайны, а также в нарушение прав человека в отношении лиц, информация о которых подвергается воздействию [8].

Можно сказать, что США (в том числе, американские корпорации) определяет глобальную компетенцию в сфере цифрового пространства.

Небольшое отступление.

Приведем пример глобальной компетенции в международном финансовом праве.

Так, К. Брамер пишет, что международное финансовое право происходит из межведомственных институтов с неоднозначным правовым статусом [10], а К. Александер, Р. Дюмель и Дж. Итвел указывают, что эти комитеты не имеют формального мандата и дей-

ствуют через неформальный консенсус при принятии стандартов лучшей практики для регулирования валютных и финансовых вопросов [11].

Прежде всего речь идет о финансовых регуляторах, мандат которых закрепляется в заявлении или коммюнике о его создании.

Эти финансовые регуляторы имеют специализированную глобальную компетенцию, дублирование исключается.

Базельский комитет по банковскому надзору отвечает за выработку регулирования для банковского сектора, Международная организация комиссий по ценным бумагам - для рынков ценных бумаг, Международная ассоциация страховых надзоров - для сферы страхования.

В Послании Президента РФ Федеральному Собранию [2] отмечается о необходимости формирования собственных цифровых платформ, что позволить по-новому организовать производственные процессы, финансовые услуги и логистику.

По данным ОЭСР, ежегодный оборот на мировом рынке высоких технологий и наукоемкой продукции в несколько раз превышает оборот рынка сырья, включая нефть, нефтепродукты, газ и древесину и составляет почти 3 трлн. долларов США, из которых 35% приходится на продукцию США, 20% - Японии, 13% - Германии, 12% - Китая, 5% - Южной Кореи, тогда как доля России на этом рынке составляет лишь 0,3%. В рейтинге Global Innovation Index за 2017 год Россия занимает лишь 45 место, в то время как Китай, располагающий пока значительно меньшим доходом на душу населения, находится на 22 месте. Более того, Россию по данному показателю опережают и многие восточноевропейские страны бывшего «социалистического блока» - Эстония (25 место), Словения (32 место), Латвия (33 место), Словакия (34 место), Болгария (36 место). В данном контексте падение цен на нефть, несколько лет назад ставшее для Российской Федерации серьезнейшей проблемой, следует рассматривать, в том числе, как катализатор, стимулирующий государство и бизнес к поиску экстраординарных решений для дальнейшего развития.

Так, с 2011 по 2016 годы внутренние затраты на исследования и разработки увеличились с 1,02% до 1,10% ВВП, однако аналогичный показатель для Южной Кореи и Израиля составил 4,3% (2014 и 2015 годы соответственно), США - 2,7% (2013 год), Японии - 3,6% (2014 год), Китай - 2,1% (2015 год). Из этого следует, что для достижения конкурентоспособных позиций на мировом рынке высоких технологий Россия должна в разы увеличить затраты на исследования и разработки.

Отдельно хотелось бы обратить внимание инфраструктуру национальной инновационной системы, в которой необходимо определить KPI и сориентировать данную институцию преимущественно на поддержку высокотехнологичных проектов в производственной сфере.

Для оценки результатов работы инновационной системы можно использовать сбалансированную систему ключевых показателей эффективности, состоящую, например, из следующих групп показателей и направлений:

KPI, характеризующие инновационную деятельность институции: развитие инфраструктуры и человеческого потенциала; осуществление разработок и инновационных проектов.

KPI, характеризующие результаты инновационной деятельности институции: рост технологического уровня; достижение стратегических целей и государственных приоритетов.

В настоящее время обязательным условием сохранения конкурентоспособности государств в глобальном масштабе становится эффективное использование цифровых технологий всеми участниками экономической системы.

Для Российской Федерации развитие и внедрение цифровых технологий во все сферы хозяйственной деятельности является еще и уникальным шансом переориентировать экономику, обеспечив ее устойчивость в долгосрочной перспективе [1].

По состоянию на начало 2016 года доля цифровой экономики в России составляла 2,1% ВВП, что в 1,3 раза больше, чем в 2011 году, однако в 2 - 4 раза меньше, чем у лидеров цифровизации. По данным Boston Consulting Group, доля цифровой экономики в среднем по Европейскому Союзу превышает 5% ВВП, в США составляет 6% ВВП, а в Великобритании, Норвегии, Южной Корее данный сектор формирует более 8% ВВП.

Безусловно, за последние 5 лет Российская Федерация достигла определенных успехов в развитии цифровой экономики. Так, онлайн-потребление росло опережающими темпами (в среднем на 27% в год) и к началу 2016 года составило 2 трлн. рублей, интенсивно развивались новые интернет-зависимые сегменты (туризм, игры, медиа, банковские услуги), которые суммарно формируют более половины объема отечественной электронной коммерции. По степени использования онлайн-возможностей Россия также улучшила свои позиции (в том числе благодаря развитию государственных электронных сервисов, а также высокой активности интернет-пользователей).

Необходимо отметить, что относительно других стран цифровая экономика России до 2014 года развивалась эволюционно - без прорывных успехов (как, например, у Китая), но и без потери позиций. Однако в условиях кризиса 2014 года резкое снижение инвестиционной активности государства и бизнеса привело к тому, что доля цифровой экономики в ВВП в 2014 - 2015 годах последовательно снижалась, и сейчас отставание Российской Федерации от лидеров «Индекса цифровизации экономики» составляет 5 - 8 лет. Между тем, мировой опыт показывает, что стагнация уровня цифровизации экономики (так называемая «венесуэльская модель») приводит к быстрому увеличению отставания от лидеров.

Отсутствие целенаправленных действий (в том числе - серьезных инвестиций в цифровой сегмент) может привести к тому, что развитие цифровизации экономики в Российской Федерации практически остановится доля цифрового экономики в ВВП и останется на текущем уровне, равном 2,1% - 2,2% ВВП. В этом случае отставание России от лидеров к 2021 году увеличится с текущих 5 - 8 лет до 15 - 20 лет. А учитывая, что разрыв между лидерами и отстающими странами растет экспоненциально, преодолеть такое отставание будет крайне сложно.

Ключевая роль в цифровой трансформации российской экономики должна принадлежать государству, поскольку именно оно является акционером ряда крупнейших промышленных предприятий, где даже малый эффект цифровизации создаст ощутимый результат, который, в свою очередь, может стать катализатором цифровизации в масштабах всей страны.

В связи с вышесказанным, существует необходимость в создании единого информационного пространства, прежде всего, среди государств-участников Евразийского экономического союза.

В соответствии с распоряжением Совета ЕЭК [9] создана рабочая группа по выработке предложений по формированию цифрового пространства Евразийского экономического союза.

Международно-правовую основу для информационной интеграции в рамках ЕАЭС составляет Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза [5].

Согласно данному Протоколу «интегрированная информационная система Союза» - организационная совокупность территориально распределенных государственных информационных ресурсов и информационных систем уполномоченных органов, информационных ресурсов и информационных систем Евразийской экономической комиссии, объединенных национальными сегментами государств-членов и интеграционным сегментом Евразийской экономической комиссии.

Создание интегрированной информационной системы Союза и развитие трансграничного пространства доверия являются первыми, базисными шагами для формирования единого цифрового пространства ЕАЭС (Евразийского экономического союза).

«Цифровизация» рассматривается в качестве этапа интеграции на евразийском пространстве, в рамках которого к свободам движения товаров, услуг, капитала и рабочей силы в перспективе добавляется также свобода движения информации, а цифровая платформа ЕАЭС - как среда формирования цифровых экосистем, обеспечивающих условия для развития новых цифровых рынков и спроса на новые сервисы и услуги.

В свою очередь, под цифровым пространством следует понимать - пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования [7].

Как отмечается в Постановлении Совета Министров Республики Беларусь «Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016 - 2020 годы» [4], одним из основных направлений развития цифровой экономики в ближайшее пятилетие будет дальнейшее формирование единого информационного пространства для оказания электронных услуг как в рамках отдельных видов деятельности, так и на основе интеграции информационных систем.

Однако, отсутствие согласованной политики государств-членов Евразийского экономического союза в цифровой сфере может стать препятствием для достижения синергетических эффектов в развитии цифровой экономики государств-членов и цифрового пространства Евразийского экономического союза.

Ключевой проблемой является интегрирование информационной системы государственных органов государств-членов, а также цифрового пространства и трансграничного пространства доверия на цифровом пространстве Евразийского экономического союза в рамках информационного обмена и с применением средств межгосударственного электронного документооборота.

Для формирования новых цепочек добавленной стоимости, создания интероперабельной бесшовной цифровой инфраструктуры, перехода к сетям последнего поколения и развития трансграничных сервисов и трансграничного пространства доверия, а также цифровой трансформации транспортной, энергетической и других отраслевых инфраструктур потребуется реализовать целостный комплекс проектов. Потребуется определить критические цифровые инфраструктурные элементы (совместно используемые и обеспечивающие интеграционные процессы), выработать общий порядок обеспечения защищенности таких цифровых процессов и инфраструктуры, включая (при необходимости) разработку и внедрение механизмов международной защиты протоколов и процедур, разработанных с учетом целей и задач Евразийского экономического союза [7].

Государства-члены Евразийского экономического союза самостоятельно разрабатывают, формируют и реализуют национальную политику в сферах цифровизации экономики, связи и информатизации, обеспечения устойчивого функционирования и безопасности единого информационного пространства и инфраструктуры связи, в том числе реализуют национальные мероприятия по развитию цифровой повестки.

Распоряжением Правительства РФ «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019 - 2021 годы» [6] была поставлена задача создание единой информационной платформы, которая должна обеспечить выполнение требований в отношении информационной безопасности государства.

Единая информационная платформа должна базироваться на принципах использования отечественного общесистемного, прикладного программного обеспечения, отечественных средств защиты информации и информационно-телекоммуникационной инфраструктуры, а также обеспечение интеграции с информационными системами органов и организаций государственного сектора, существующими и разрабатываемыми компонентами инфраструктуры, обеспечивающей информационно-технологическое взаимодействие действующих и создаваемых информационных систем, используемых для предо-

ставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее - инфраструктура электронного правительства), и с другими информационными системами.

При реализации единого информационного пространства (единой информационной платформы) в основу должна быть положена информационная безопасность государства.

Цель обеспечения безопасности информационно-психологической компоненты информационной сферы состоит в сохранении информационного суверенитета и проведении политики информационного нейтралитета, а также формировании устойчивого иммунитета против деструктивных информационно-психологических воздействий на массовое общественное сознание, а в необходимых случаях - и противодействие им.

Необходимо обеспечивать формирование, использование и развитие единого информационного пространства исключительно в целях социального, экономического и культурного развития государства, а также постоянную, активную и эффективную деятельность государственных органов, организаций, научно-экспертного сообщества в информационном пространстве, особенно наращивать ее в сети Интернет.

В частности, сформирована развернутая правоприменительная практика соблюдения уже установленных требований в сфере обеспечения информационной безопасности, по результатам которого будут внесены необходимые изменения в законодательство; проведена ревизия образовательных программ и профессиональных стандартов, увеличено количество и качество подготавливаемых специалистов в области информационной безопасности, обеспечено повышение квалификации действующих работников, занятых в этой сфере; выстроена эффективная схема взаимодействия и кооперации между промышленностью и наукой в создании отечественных разработок, что создаст основу для развития национального и отраслевых оперативных центров информационной безопасности, что позволит на втором этапе обеспечить: - ключевое участие IT-компаний в обеспечении национальной информационно - коммуникационной инфраструктуры системами информационной безопасности; загрузку отечественных предприятий электронной промышленности заказами на приобретение государственными органами и квазигосударственным сектором телекоммуникационного оборудования, произведенного и прошедшего процедуры сертификации на соответствие требованиям информационной безопасности на территории страны.

Для полноценной оценки состояния защищенности объектов информатизации с учетом характера деятельности киберпреступников и иностранных технических компьютерных разведок, рассчитывающих на самоуспокоенность и небрежность со стороны владельцев информационных ресурсов и систем, необходимо стремиться к непрерывному мониторингу состояния информационных систем и ресурсов техническими средствами контроля защищенности и проведению работы по выявлению каналов утечки информации (уязвимостей, вирусов, троянских программ, недекларируемых функций и закладок).

Такой подход позволит обеспечить сохранение возможности реализации государственных функций в случае чрезвычайных происшествий технологического, социального характера, вызванных инцидентами информационной безопасности, угрожающими национальной и общественной безопасности, а в случае чрезвычайного или военного положения возможности использования устойчивой информационно - коммуникационной инфраструктуры сил обеспечения национальной безопасности в интересах функционирования критически важных объектов информационно - коммуникационной инфраструктуры.

Наряду с выстраиванием работы с объектами критической информационно - коммуникационной инфраструктуры из числа стратегических и особо важных государственных объектов, объектов стратегических отраслей экономики, пересмотреть критерий отнесения к критически важным объектам информационно - коммуникационной инфраструктуры с возможностью отнесения к критически важным объектам, ориентированных на оказание информационно - коммуникационных услуг населению.

Распространять предупредительные и профилактические меры не только на государственные органы и собственников частных информационных систем, интегрируемых с государственными, но и на владельцев промышленных предприятий, финансовых организаций и других категорий объектов экономики, имеющих автоматизированные технологические процессы, нарушение которых может негативно сказаться на экономическом развитии государства.

На основе Единых требований и действующих Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства» предусмотреть разработку руководящих документов, служащих ориентиром не только для государственного сектора, но и для объектов, находящихся в частной собственности, в целях эффективной локализации и предотвращения реализации угроз в общенациональном масштабе.

Для создания высоко адаптированной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно - коммуникационной инфраструктуры можно рекомендовать следующие мероприятия (используя опыт Республики Казахстан [3]: государственным органам и поставщикам услуг принять риск-ориентированный подход к безопасности, уделяя первоочередное внимание усилиям, которые обеспечивают наиболее высокий уровень надежности создаваемых информационных систем в нормальном и внештатном режимах и устойчивости их к умышленным сбоям.

Расширить взаимодействие между ведомственными и отраслевыми структурами мониторинга и реагирования на инциденты информационной безопасности для оказания содействия владельцам информационных ресурсов и систем и взаимного оповещения о возникающих угрозах. Их участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования, проектирования, разработки и эксплуатации отраслевых информационных систем и сетей и стать опорными точками, определяющими устойчивость всей информационно - коммуникационной инфраструктуры страны.

Специализация служб реагирования на инциденты информационной безопасности позволит расширить круг вовлеченных организаций и экспертов, что будет способствовать росту профессионализации работников, занятых в сфере информационной безопасности с учетом отраслевой специфики, и содействовать расширению рынка услуг аудита информационной безопасности для малого бизнеса, который часто не имеет возможности содержать квалифицированных специалистов в области IT и информационной безопасности.

Компьютерные атаки, запущенные из зарубежного пространства, максимально предотвращать на «электронной границе» - виртуальном периметре государства.

Руководящие документы Единой сети телекоммуникаций с учетом ее растущей уязвимости в результате конвергенции сетей телекоммуникаций и информационно - коммуникационных сетей и необходимости снижения объемов вредоносного трафика и своевременного блокирования операторами связи аномальной сетевой активности необходимо актуализировать.

Создание условий для эффективной борьбы с киберпреступностью путем постоянного повышения квалификации личного состава специализированных подразделений, расширения арсенала технических средств фиксации и криминалистических исследований «цифровых» доказательств.

Для объединения усилий при участии научного сообщества, частного сектора подготовить создание единого координационного центра информационной безопасности, который в онлайн режиме будет обрабатывать информацию о состоянии защищенности «электронной границы», а также наиболее важных компонентов национальной информационной инфраструктуры и обеспечить обмен информацией, что позволит: обеспечить гражданам и бизнесу доступ к квалифицированным оценкам угроз в сфере информационной безопасности и получению дополнительных знаний о том, как уменьшить негативное влия-

ние от угроз использования уязвимостей в программном обеспечении и информационных и телекоммуникационных системах.

Государственным органам поддерживать высокий уровень отказоустойчивости и предупреждения возникновения технологических сбоев, а также своевременного устранения их последствий в инфраструктуре, входящей в состав «электронного правительства» и других государственных информационных систем и ресурсов; собственникам критически важных объектов информационно - коммуникационной инфраструктуры получать своевременную информацию о возможном влиянии на безопасность принадлежащих им автоматизированных систем управления технологическими процессами.

На внешнеполитическом и внешнеэкономическом уровне последовательно продвигать интересов участников единого информационного пространства, направленные на преодоление «цифрового» разрыва между участниками международного сообщества в информационной сфере, обозначив в качестве приоритетов реализацию инициатив по укреплению, на основе норм и принципов международного права, системы международной информационной безопасности.

В рамках двух и многосторонней дипломатии России необходимо укреплять роль в качестве сильного и последовательного партнера, выступающего против использования ИКТ в военных целях, следующего курсу открытости, укрепления мер доверия в области международной информационной безопасности, при безусловном соблюдении суверенного равенства государств в выборе путей технологического развития. Ключевыми диалоговыми площадками должны стать международные, региональные и субрегиональные организации (ООН, ШОС, ЕАЭС, ОДКБ, СНГ и др.) с дальнейшим продвижением их инициатив на различных международных площадках.

Литература

1. Заключение Комитета по экономической политике, промышленности, инновационному развитию и предпринимательству «По Прогнозу социально-экономического развития Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов»
2. Послание Президента РФ Федеральному Собранию от 01.03.2018 // Доступ из СПС «Консультант Плюс».
3. Постановление Правительства Республики Казахстан от 30.06.2017 № 407 «Об утверждении Концепции кибербезопасности» // Доступ из СПС «Консультант Плюс».
4. Постановление Совета Министров Республики Беларусь от 23.03.2016 № 235 «Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016 - 2020 годы» // Доступ из СПС «Консультант Плюс».
5. Приложение № 3 к Договору о Евразийском экономическом союзе от 29.05.2014 «Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза» // Доступ из СПС «Консультант Плюс».
6. Распоряжение Правительства РФ от 03.06.2019 № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019 - 2021 годы» // Собрание законодательства РФ. 2019. № 23.
7. Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // // Доступ из СПС «Консультант Плюс».
8. Тематический доклад, опубликованный Комиссаром Совета Европы по правам человека «Верховенство права в Интернете и в остальном цифровом мире» // Доступ из СПС «Консультант Плюс».

9. Распоряжение Совета Евразийской экономической комиссии от 17.03.2016 № 6 «О создании рабочей группы по выработке предложений по формированию цифрового пространства Евразийского экономического союза» // Доступ из СПС «Консультант Плюс».
10. Brummer C. Why Soft Law Dominates International Finance - And Not Trade // URL: https://poseidon01.ssrn.com/delivery.php?ID=878026005027092083127074109088096010103027035008001066117066021121081078100096125101059057107022010023114103099072090091120108122051044060017001080113118096125066062023080067025125108027073027020091123122106099103072101123095076091118119112127019110&EXT=pdf (дата обращения: 13.07.2019).
11. Alexander K., Dhumale R., Eatwell J. Global Governance of Financial Systems. The International Regulation of Systemic Risk // Oxford, University Press, USA. 2006.