DOI 10.22394/1726-1139-2019-1-29-39

Информационный потенциал государства как основа информационного суверенитета

Кефели И. Ф., Мальмберг С. А.*

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; geokefeli@mail.ru

РЕФЕРАТ

В статье рассматриваются противоборство государств в информационном пространстве и аспекты государственной информационной политики в части защиты информационного суверенитета. Целями настоящего исследования являются введение понятия «информационный потенциал государства» и обоснование необходимости его использования при планировании и организации внутриполитической и внешнеполитической управленческой деятельности для защиты информационного суверенитета государства. На основе исследования с применением методов сравнительного и ситуационного анализов выявлен и определен общий фактор, определяющий возможности государств в информационном пространстве, — «информационный потенциал государства». Определена сущность понятия «информационный потенциал государства» и продемонстрировано, что информационный потенциал государства является основой информационного суверенитета. Проведен анализ отечественного и зарубежного опыта применения информационного потенциала государства в проведении информационной политики с целью защиты информационного суверенитета. Проанализированы шаги по обеспечению соблюдения законодательства Российской Федерации на примере блокировки доступа к мессенджеру Telegram с территории Российской Федерации. В результате данного анализа сделан вывод о невозможности обеспечения законодательства Российской Федерации в информационном пространстве с применением текущего информационного потенциала государства. Для решения данной проблемы в статье предлагается использовать не только технические, но и организационные меры. Для недопущения повторения данной ситуации в дальнейшем предлагается ввести определенное в данной статье понятие «информационный потенциал государства» в нормативно-правовые акты, регулирующие государственную информационную политику (Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Федеральный закон № 149-ФЗ).

Ключевые слова: информационный потенциал, информационное общество, информационная политика, информационный суверенитет

State Information Capacity as Information Sovereignty Basis

Igor F. Kefeli, Sergey A. Malmberg*

[a]Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management of RANEPA), Saint-Petersburg, Russian Federation; geokefeli@mail.ru

ABSTRACT

This article examines the confrontation of states in the information space and aspects of the state information policy in terms of protecting information sovereignty. The purpose of this study is to introduce the concept of “information capacity of the state” and justify the need for its use in planning and organizing internal and external policy management activities to protect the information sovereignty of the state. On the basis of research, using the methods of comparative and situational analyzes, a common factor has been identified. This factor determines capabilities of states in the information space, it is “information capacity of the state”. The essence of the concept of “information capacity of the state” is defined and it was demonstrated that the information capacity of the state is the basis of information sovereignty. The analysis of domestic and foreign experience of applying the information capac-

ity of the state in the conduct of information policy in order to protect information sovereignty was done. The steps to ensure compliance with the legislation of the Russian Federation on the example of blocking access to the Telegram messenger from the territory of the Russian Federation were analyzed. As a result of this analysis, it was concluded that it is impossible to ensure the legislation of the Russian Federation in the information space using the current information capacity of the state. To solve this problem, the article proposes to use not only technical, but also organizational measures. To prevent this situation from recurring in future, it is proposed to introduce the concept of "information capacity of the state", defined in this article, into the regulatory acts governing the state information policy (National Security Strategy of the Russian Federation, Doctrine of Information Security of the Russian Federation, Federal Law № 149-ФЗ).

Keywords: information capacity, information society, information policy, information sovereignty

Введение

Современное общество, сформировавшееся под влиянием информационных технологий [13] и их использования в ежедневной деятельности, в документах, регулирующих национальную государственную информационную политику в современном государстве, получило название «информационное общество»[1]. В Российской Федерации информатизация общества является частью государственной политики, реализуемой в рамках государственной программы «Информационное общество (2011–2020)». Информатизация, направленная на все сферы жизни общества [12; 15], приводит к тому, что при стратегическом планировании того или иного вида деятельности, отдельно необходимо учитывать ее информационную составляющую.

Противоборство в современном мировом сообществе происходит во многих областях, но в последние годы наиболее явно эта активность осуществляется в информационной сфере. В настоящее время вопросы обеспечения информационной безопасности стали одними из основополагающих факторов национальной безопасности современного государства [4]. Внутриполитические протестные движения сопровождаются массированной информационной кампанией как внутри страны, так и за рубежом. И, как правило, такая кампания направлена на дестабилизацию внутриполитической ситуации [14].

Таким образом, гипотезой настоящего исследования является тот факт, что в современных условиях для проведения государственной политики в международной и внутриполитической сферах необходимо отдельно учитывать информационную составляющую государственного суверенитета, национальной безопасности и других определяющих факторов. Также для оценки проводимой государством информационной политики необходим инструментарий для определения возможностей государства в информационном поле.

Целями настоящего исследования являются введение понятия «информационный потенциал государства» и обоснование необходимости его использования при планировании и организации внутриполитической и внешнеполитической управленческой деятельности для защиты информационного суверенитета государства.

Для достижения необходимых результатов в данной работе использованы элементы ситуационного и сравнительного анализов.

---

[1] Informations gesellschaft [Электронный ресурс] // Die Bundesregierung. URL: https://www.bundesregierung.de/Content/DE/Lexikon/EUGlossar/I/ 2005-11-21-informationsgesellschaft.html; Государственная программа «Информационное общество» (2011–2020 годы) [Электронный ресурс] // Минкомсвязь России. URL: http://minsvyaz.ru/ru/activity/programs/1/

Материалы и методы

В данной работе при описании зарубежного опыта в проведении информационной политики и применении информационного потенциала государства с целью защиты информационного суверенитета (обеспечение соблюдения национального законодательства в информационном пространстве и т. п.) и сравнении с отечественным опытом в данной сфере использованы элементы сравнительного анализа.

Для оценки текущего положения в развитии информационной политики Российской Федерации, информационных потребностей государства, аспектов информационного суверенитета использованы методы ситуационного анализа. При этом в качестве внутренних переменных использованы следующие: информационные потребности, национальное законодательство в информационной сфере. В качестве внешних переменных использованы следующие: информационные угрозы национальной безопасности и информационному суверенитету, действия иностранных государств в части развития и использования собственного информационного потенциала.

Противоборство в информационном пространстве

В современном мире противоречия между ведущими мировыми державами, группами государств и региональными структурами приводят к усиленному противоборству между ними в информационном пространстве.

Любое современное государство, которое заинтересовано в отстаивании своих национальных интересов и защите государственного суверенитета (в их информационных составляющих), проводит государственную информационную политику, направленную на информатизацию общества и сфер государственного управления на всех уровнях, обеспечение информационной безопасности критической информационной инфраструктуры и систем, необходимых для полноценного функционирования всех государственных институтов.

В Российской Федерации данный аспект нашел свое отражение в Стратегии национальной безопасности Российской Федерации до 2020 г.[1], в Доктрине информационной безопасности Российской Федерации[2], в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»[3], а также в целом ряде других Федеральных законов, указов Президента Российской Федерации и постановлений Правительства Российской Федерации.

Информационный потенциал и информационные потребности государства

Несмотря на то, что информационная составляющая играет ведущую роль во внешней и внутренней политике, отсутствует единый взгляд на возможности государства в «информационном поле» [8] на внутренней и внешней арене и на оценку этих возможностей. Многие научные и массовые издания применяют для этого термин «информационный потенциал» [9; 10]. Использование в данном случае понятия «потенциал» неслучайно. «Потенциал», как одно из базовых понятий экономической теории, позволяющее определить уровень социально-экономического развития [1],

[1] Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС КонсультантПлюс.

[2] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС КонсультантПлюс.

[3] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» // СПС КонсультантПлюс.

применяется на международном и общегосударственном уровне. Данное понятие [2] перешло в экономику из физики, где оно означает величину потенциальной энергии в определенной точке пространства. В более широком смысле потенциал — это возможность (тела или системы) производить какие-либо изменения [11]. При этом зависимость между возможностью системы производить изменения и величиной потенциала — прямо пропорциональная.

В настоящее время ученые и специалисты вкладывают в понятие «информационный потенциал» в каждом случае нечто «свое» — это либо совокупность информационных ресурсов, либо набор информационных массивов данных, либо способность отражать злонамеренные информационные воздействия. В нормативно-правовых актах Российской Федерации такое понятие в принципе отсутствует. Вместе с тем введение и определение такого понятия в нормативно-правовых актах, регулирующих государственную информационную политику, необходимо для оценки эффективности выполнения постановлений Правительства Российской Федерации, общих концепций и планов (сформулированных в рамках доктрин и стратегий) в рамках проведения государственной информационной политики. Информационный потенциал государства должен включать в себя все вышеперечисленные факторы, а также уровень использования отечественных аппаратных и программных средств для государственных и муниципальных нужд. Таким образом, сущность информационного потенциала государства заключается в возможностях страны в информационном пространстве [5; 6]. Исходя из этого, дадим определение данному понятию.

Информационный потенциал государства — это возможность удовлетворять государственные информационные потребности за счет отечественных технических систем и средств, осуществлять сбор, анализ и систематизацию необходимой информации, организовывать научную и производственную работу в части информатизации и информационной безопасности, проводить независимую информационную политику, влияя на внутреннее и внешнее информационное поле, отражать и предупреждать злонамеренные компьютерные воздействия на государственные, инфраструктурные и военные объекты.

Здесь необходимо отдельно остановиться на информационных потребностях государства. Во-первых, очевидно, что руководству любой страны для реализации возложенных на них государственных полномочий ежедневно необходимо принимать целый ряд управленческих и стратегических решений. Принятие таких решений невозможно без справочного аналитического материала. Управленческое решение должно быть предварено получением данных аналитической обработки информации о социально-экономических и хозяйственных показателях, актуальной информацией от силовых структур в части обеспечения безопасности и другой целевой информации [5; 16]. На основе полученных данных может быть проведен, например, многофакторный статистический анализ с целью прогнозирования дальнейшего развития ситуации и предложены варианты управленческих решений с применением сценарного подхода дальнейшей реализации ситуации. Таким образом, информационные потребности государства заключаются в наличии полной и достоверной информации для принятия управленческих решений.

Во-вторых, информационные потребности заключаются в проведении информатизации и реализации политики информационной безопасности во всех направлениях государственной политики (военная, образовательная, государственно-управленческая, научная, медицинская и другие сферы деятельности).

В-третьих, информационные потребности государства заключаются в удовлетворении информационных потребностей общества, в части предоставления доступа, распространения и своевременного доведения необходимой информации населению.

Государственный информационный суверенитет

Как уже было сказано, повсеместная информатизация общества приводит к необходимости учитывать информационную составляющую всех факторов и процессов. Это справедливо также для понятия «государственный суверенитет» — «государственный информационный суверенитет». И действительно, в настоящее время многие ученые и специалисты [3], говоря о государственном суверенитете Российской Федерации, отдельно выделяют понятие «информационный суверенитет». Очевидно, что суверенитет — это обязательный признак государства, который заключается в верховенстве государственной власти, национального законодательства, а также самостоятельности и независимости от каких бы то ни было внешних структур.

На данный момент не существует устоявшегося понятия «информационный суверенитет». Работу в правовом и научном определении данного термина в разное время вели В.Н. Супрун, А.А. Сергунин, М.М. Кучерявый и др. Данное понятие закреплено в Доктрине информационной безопасности Российской Федерации: «основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства являются: защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере»[1].

Государственный информационный суверенитет заключается в способности государства проводить независимую информационную политику и обеспечивать верховенство государственного законодательства в информационном пространстве, т.е. фактически информационный потенциал как «возможность» государства в информационном пространстве является определяющим фактором для государственного информационного суверенитета. Очевидно, что если государство не в состоянии обеспечить возможность проведения независимой информационной политики, влияя, таким образом, на внешнее и внутреннее информационное поле и обеспечивая соблюдение законодательства в информационном пространстве, то фактически у государства отсутствует информационный суверенитет. Таким образом, информационный потенциал государства является основой информационного суверенитета. Рассмотрим на практике некоторые аспекты того, как Российская Федерация использует свой информационный потенциал в части проведения независимой информационной политики и обеспечения соблюдения законодательства в информационном пространстве.

Информационный потенциал государства как основа информационного суверенитета. Отечественный и зарубежный опыт

С 2012 г. все российские интернет-провайдеры были обязаны блокировать доступ к ресурсам, находящимся в Реестре запрещенных сайтов. Оператором Реестра запрещенных сайтов является Роскомнадзор[2]. Федеральный закон от 27.07.2006 № 149-ФЗ ввел возможность немедленных внесудебных блокировок в информационно-телекоммуникационной сети Интернет страниц с информацией, «содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию

[1] Доктрина информационной безопасности Российской Федерации // [Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 25.01.2018).

[2] Федеральный закон от 28.07.2012 № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // СПС КонсультантПлюс.

в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка»[1].

С 1 ноября 2017 г. согласно Федеральному закону № 276-ФЗ[2] владельцы VPN-сервисов и анонимайзеров, а также операторы поисковых систем обязаны ограничивать доступ к запрещенной информации. Также в июле 2016 г. был принят ряд законов, а именно Федеральный закон № 374-ФЗ[3] и Федеральный закон № 375-ФЗ[4]. Согласно данным Федеральным законам, помимо прочего, операторы связи обязаны хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более чем за 6 месяцев). Также организаторы распространения информации в интернете обязаны по требованию Федеральной службы безопасности Российской Федерации предоставить ключи к зашифрованному трафику. Для выполнения данного положения Федерального закона № 374-ФЗ выпущен приказ Федеральной службы безопасности Российской Федерации № 432[5].

Необходимо отметить, что, несмотря на многочисленные акции протеста и заявления «экспертов» относительно невыполнимости и неправомочности данных нормативно-правовых актов[6], у наших «западных партнеров» не только подготовлена необходимая правовая база под действия подобного рода, но и активно применяется на практике процедура доступа к сообщениям и звонкам пользователей в различных мессенджерах и социальных сетях. Так, в 2016 г. в Великобритании был принят «Закон о полномочиях следствия» (Investigatory Powers Bill)[7], согласно которому интернет-провайдеры и операторы сотовой связи обязаны хранить информацию абонентов на протяжении 12 месяцев. Эти данные включают в себя сведения о телефонных звонках и посещенных веб-сайтах[8]. До 2015 г. в США действовал так называемый «Патриотический акт», принятый после терактов 11 сентября 2001 г. Так спецслужбы получили доступ к телефонным разговорам, СМС-переписке, электронной почте граждан, а также к сведениям о взятых в библиотеках книгах, посе-

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс.

[2] Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в закон «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс.

[3] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС КонсультантПлюс.

[4] Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС КонсультантПлюс.

[5] Приказ Федеральной службы безопасности Российской Федерации от 19.07.2016 г. № 432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» // СПС КонсультантПлюс.

[6] Около 12 тысяч человек пришли на митинг «За свободный интернет» в Москве [Электронный ресурс] // Телеканал Дождь. URL: https://tvrain.ru/teleshow/here_and_now/miting-462863/; Дуров о блокировке Telegram: конфиденциальность не продается [Электронный ресурс] // Настоящее время. URL: https://www.currenttime.tv/a/29165672.html

[7] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny [Электронный ресурс] // Government of the United Kingdom. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF

[8] Extreme surveillance' becomes UK law with barely a whimper [Электронный ресурс] // The Guardian. URL: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

щенных сайтах и т. д.[1] В настоящее время по некоторым данным[2] в США действует система разведки PRISM, которая позволяет получить доступ к сообщениям и звонкам пользователей через электронные системы коммуникации (Skype и пр.) [7]. В 2018 г. в США принят так называемый «Облачный закон» (CLOUD Act)[3]. Согласно данному закону спецслужбы имеют право получить доступ ко всем данным пользователей вне зависимости от того, где эта информация хранится[4]. Одним из последних, преданных широкой огласке, примеров сотрудничества компаний, предоставляющих услуги по интернет-коммуникациям, и спецслужб является передача Facebook-сообщений российских пользователей, связанных с выборами президента США, Конгрессу США[5]. По объективным причинам, в связи с наличием большого количества угроз безопасности государства (терроризм, организованная преступность, коррупция, свержение государственного строя и т. д.), которые планируются и готовятся посредством систем электронной коммуникации, спецслужбам для выполнения возложенных на них обязанностей по обеспечению безопасности в государстве необходимо иметь возможность доступа к отдельным данным пользователей для проведения оперативно-розыскных мероприятий.

Зарубежная правовая база в части информационной политики и неофициально используемые за рубежом системы разведки и слежения нацелены на аналогичные задачи, что и нормативно-правовые акты, и требования в данной области в Российской Федерации. Таким образом, все современные государства, проводящие активную информационную политику, в соответствии с существующими информационными угрозами, ведут правовую и техническую работу по увеличению информационного потенциала государства с целью защиты информационного суверенитета. Однако информационный потенциал государства, как возможность в информационном пространстве, характеризуется не принятыми на бумаге и каким-то образом реализуемыми мерами, а, собственно, возможностью достижения запланированного результата.

Рассмотрим как в Российской Федерации на практике приводят в исполнение мероприятия по защите государственного информационного суверенитета, на примере блокировки мессенджера Telegram. 13 апреля 2018 г. Таганский суд Москвы постановил заблокировать доступ к мессенджеру Telegram в России за несоблюдение положений упомянутых выше федеральных законов, а именно за отказ предоставить Федеральной службе безопасности Российской Федерации ключи для расшифровки сообщений пользователей[6]. 16 апреля 2018 г. Роскомнадзор приступил к процедуре блокировки мессенджера[7].

Однако по прошествии более полутора месяцев мессенджер Telegram был все еще доступен без использования каких-либо трудоемких процедур по настройке.

---

[1] Жизнь под «колпаком». Как «Патриотический акт» лишил американцев свободы [Электронный ресурс] // Аргументы и факты. URL: http://www.aif.ru/politics/world/zhizn_pod_kolpakom_kak_patrioticheskiy_akt_lishil_amerikancev_svobody

[2] Prism — глобальная машина наблюдения: как США уничтожают свободу в мире [Электронный ресурс] // Информационное агентство Regnum URL: https://regnum.ru/news/1669976.html

[3] H. R.4943 — CLOUD Act [Электронный ресурс] // United States Congress. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943

[4] CLOUD Act: новый законопроект США открывает доступ к персональным данным за рубежом [Электронный ресурс] // Habr. URL: https://habr.com/company/it-grad/blog/352402/

[5] Facebook передаст конгрессу США сообщения российских пользователей, связанные с выборами президента США [Электронный ресурс] // Регионы России. URL: https://www.gosrf.ru/news/32259/

[6] Суд постановил заблокировать Telegram в России [Электронный ресурс] // ТАСС. URL: http://tass.ru/obschestvo/5121612

[7] Роскомнадзор начал процедуру блокировки Telegram [Электронный ресурс] // ТАСС. URL: http://tass.ru/ekonomika/5129977

Более того, основатель мессенджера Павел Дуров сразу после решения суда опубликовал инструкции по обходу блокировки мессенджера Telegram[1], т. е. по саботажу решения Таганского суда Москвы. В данном случае понятны позиции и поступки всех действующих лиц: пользователи, привыкшие к мессенджеру, постараются вытерпеть некоторые неудобства от использования средств для обхода блокировки. Основатель мессенджера пытается спасти результат своих трудов, а позиция и действия Роскомнадзора, ответственного, согласно решению суда, за блокировку мессенджера, вызывают вопросы. Необдуманные действия Роскомнадзора по блокировке миллионов IP-адресов, якобы каким-то образом причастных к функционированию Telegram, в итоге привели к нарушению нормальной работы ряда законных сервисов и учреждений (банки, торговые сети, рестораны, музеи и т. д.)[2]. А число пользователей Telegram за это время только выросло[3]. Данная ситуация требует полного переосмысления самого подхода к блокировке незаконных ресурсов и приложений. Необходима выработка средств и механизмов, которые бы сделали использование технических средств по обходу блокировок не только неудобным, но и невыгодным, что невозможно сделать без привлечения к широкому обсуждению участников рынка, технических специалистов и других заинтересованных лиц. Также упомянутая ранее необходимость введения понятия «информационный потенциал государства» в нормативно-правовых актах, регулирующих государственную информационную политику, обусловливается еще и тем, что использование данного показателя позволило бы предупредить данную ситуацию с невозможностью блокировки Telegram на территории Российской Федерации и оценить в каких направлениях информационной политики необходимо проводить работы.

Результаты

В рамках данной работы получены следующие результаты.

Проанализировано текущее состояние противоборства государств в информационном пространстве. На основе анализа выявлен общий фактор, определяющий возможности государств в информационном пространстве — «информационный потенциал государства».

Введено понятие «информационный потенциал государства» и определена его сущность, продемонстрирована прямая зависимость между информационным суверенитетом и информационным потенциалом — информационный потенциал является основой информационного суверенитета.

Проведен анализ зарубежного опыта применения информационного потенциала государства в проведении информационной политики с целью защиты информационного суверенитета.

Проведен анализ применения информационного потенциала Российской Федерации в проведении информационной политики с целью защиты информационного суверенитета на примере исполнения постановления Таганского суда Москвы о блокировке доступа к мессенджеру Telegram с территории Российской Федерации. В результате данного анализа сделан вывод о невозможности обеспечения соблюдения законодательства Российской Федерации в информацион-

---

[1] Дуров рассказал, как обойти блокировку Telegram [Электронный ресурс] // Телеканал Санкт-Петербург. URL: https://topspb.tv/news/2018/04/13/durov-rasskazal-kak-obojti-blokirovku-telegram/

[2] Инфографика: кто пал в битве за Telegram [Электронный ресурс] // Банки.ру. URL: http://www.banki.ru/news/lenta/?id=10406025

[3] Эффект Стрейзанд: что пошло не так в блокировке Telegram? [Электронный ресурс] // Infostartjournal. URL: https://infostart.ru/journal/news/tekhnologii/effekt-streyzand-chto-poshlo-ne-tak-v-blokirovke-telegram_839169/ (дата обращения: 21.05.2018)..

ном пространстве с применением текущего информационного потенциала государства.

Для решения данной проблемы в работе предлагается использовать не только технические, но и организационные меры.

Для недопущения повторения данной ситуации в дальнейшем в данной работе предлагается ввести определённое в данной статье понятие «информационный потенциал государства» в нормативно-правовые акты, регулирующие государственную информационную политику (Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Федеральный закон № 149-ФЗ).

Заключение

Таким образом, информационный потенциал как основа информационного суверенитета страны требует действий со стороны государства и регулирующих органов не только в правовом поле, но и в технической и организационной областях. В настоящее время любые действия регулирующих органов по соблюдению законодательства в информационной сфере могут быть обойдены при помощи стандартных средств, т. е. информационный потенциал Российской Федерации в части защиты государственного информационного суверенитета находится на низком уровне. Введение стандартизированного и закрепленного нормативно-правовыми актами понятия «информационный потенциал государства» позволило бы вовремя предупредить данную ситуацию и понять необходимое направление работы в части корректировки информационной политики государства.

Литература

1. *Гацалова Л. Б., Парсиева Л. К.* Современные механизмы регулирования региональной демографической политики в условиях экономической нестабильности // Современные проблемы науки и образования. 2013. № 5. С. 433.
2. *Колесов С. В.* Инновационно-инвестиционный потенциал как экономическая категория и его роль в обеспечении жизнедеятельности предприятия [Электронный ресурс] // Научный диалог: экономика и управление. Чебоксары : ЦНС «Интерактив плюс». URL: https:/interactive-plus.ru/ru/article/2154/discussion_platform
3. *Кучерявый М. М.* Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 7–14.
4. *Кучерявый М. М., Вовенда Ю. В.* Региональная информационная безопасность в рамках евразийской интеграции // Управленческое консультирование. 2016. № 7. С. 19–26.
5. *Мальмберг С. А.* Информационный потенциал субъекта Российской Федерации и Ситуационный центр как инструмент управления информационным потенциалом // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 1–3 ноября 2017 г.: Материалы конференции / СПОИСУ. СПб., 2017. С. 367–369.
6. *Мальмберг С. А.* Сущность информационного потенциала государства // Сборник статей по материалам VII Международной научно-практической конференции Инновации в науке и практике (28 апреля 2018 г., г. Барнаул). В 5 ч. Ч. 5. Уфа : Дендра, 2018. С. 111–115.
7. *Мальмберг С. А., Семьянов П. В.* Обеспечение безопасной передачи данных в Skype // Студенческая научная конференция «Информатика и кибернетика» (ComCon–2015): материалы студенческой научной конференции «Информатика и кибернетика» (ComCon–2015). Институт информационных технологий и управления СПбПУ. СПб. : Изд-во Политехн. ун-та, 2015. С. 219–221.
8. *Манойло А. В.* Государственная информационная политика в особых условиях : монография. М. : МИФИ, 2003. 388 с.
9. *Молчанов Н. А.* Информационный потенциал зарубежных стран как источник угроз военной безопасности РФ // Военная мысль. 2008. № 10. С. 2–9.

10. *Проскура Д. В.* Информационный потенциал регионов России // Экономика глазами молодых: материалы V Международного экономического форума молодых ученых, (Минск, 1–3 июня 2012 года). Минск : БГАТУ, 2012. С. 429–431.
11. *Физический* энциклопедический словарь. М. : Советская энциклопедия, 1983. 928 с.
12. *Kochetkov, Dmitry M.* Economic Model of Information, Information Society, and information Literacy: A View from Russia // Library Philosophy and Practice (e-journal). 2017.
13. *Page, J. R. U.* Economics and Politics of Information Technology: Some Trends in its Application to Information for the Professional // IFLA Journal. 1984. N 10. P. 28.
14. *Spaiser, V., Chadefaux, T.* Communication power struggles on social media: A case study of the 2011–12 Russian protests // Journal of Information Technology and Politics. 2017. N 14. P. 132.
15. *Wheeler M.* High-tech politics: The impact of information communication technologies // Convergence: The Journal of Research into New Media Technologies. 1998. N 4. P. 42.
16. *Wordsworth P., Boughey J.* Information needs and information technology in management // Property Management. 1993. N 11. P. 288.

Об авторах:

Кефели Игорь Фёдорович, директор Центра геополитической экспертизы Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), доктор философских наук, профессор; geokefeli@mail.ru

Мальмберг Сергей Александрович, аспирант Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация); smalmberg@mail.ru

References

1. Gatsalova L. B., Parsieva L. K. Modern mechanisms of regulation of regional population policy in the conditions of economic instability // Modern problems of science and education [Sovremennye problemy nauki i obrazovaniya]. 2013. N 5. (In rus)
2. Kolesov S. V. Innovative investment potential as economic category and its role in ensuring activity of the enterprise [An electronic resource] // Scientific dialogue: economy and management. Cheboksary : Scientific Cooperation Center Interactive plus. URL: https:/interactive-plus.ru/ru/article/2154/discussion_platform (In rus)
3. Kucheryavyy M. M. State policy of information sovereignty of Russia in the conditions of the modern global world // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2015. N 2. P. 7–14. (In rus)
4. Kucheryavyy M. M., Vovenda Yu. V. Regional information security within the Eurasian integration // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2016. N 7. P. 19–26. (In rus)
5. Malmberg S. A. Information capacity of the territorial subject of the Russian Federation and Situational center as instrument of management of information potential // Information security of regions of Russia (IBRR-2017). Anniversary X St. Petersburg interregional conference. St. Petersburg, on November 1–3, 2017: Materials of conference / SPOISU. SPb., 2017. P. 367–369. (In rus)
6. Malmberg S. A. Essence of information potential the state // Collection of articles on materials of the VII international scientific and practical conference. Innovation in science and practice (on April 28, 2018, Barnaul). In 5 parts. Part 5. Ufa : Dendra, 2018. P. 111–115. (In rus)
7. Malmberg S. A., Semyanov P. V. Ensuring safe data transmission in Skype // Student's scientific conference "Informatics and Cybernetics" (ComCon–2015): materials of the student's scientific conference "Informatics and Cybernetics" (ComCon–2015). SPbSTU Institute of information technologies and management. SPb. : SPbSTU publishing house, 2015. P. 219–221. (In rus)
8. Manoylo A. V. State information policy in special conditions: monograph. M. : MEPhI, 2003. 388 p. (In rus)
9. Molchanov N. A. Information capacity of foreign countries as source of threats of military safety of the Russian Federation // Military thought [Voennaya mysl']. 2008. N 10. P. 2–9. (In rus)
10. Proskura D. V. Information capacity of regions of Russia // Economy by eyes of young people: materials of the V International economic forum of young scientists, (Minsk, on June 1–3, 2012). Minsk : BSATU, 2012. P. 429–431. (In rus)

11. Physical encyclopedic dictionary. M. : Soviet encyclopedia, 1983. 928 p. (In rus)
12. Kochetkov, Dmitry M. Economic Model of Information, Information Society, and information Literacy: A View from Russia // Library Philosophy and Practice (e-journal). 2017.
13. Page, J. R.U. Economics and Politics of Information Technology: Some Trends in its Application to Information for the Professional // IFLA Journal. 1984. N 10. P. 28.
14. Spaiser, V., Chadefaux, T. Communication power struggles on social media: A case study of the 2011–12 Russian protests // Journal of Information Technology and Politics. 2017. N 14. P. 132.
15. Wheeler, M. High-tech politics: The impact of information communication technologies // Convergence: The Journal of Research into New Media Technologies. 1998. N 4. P. 42.
16. Wordsworth, P., Boughey, J. Information needs and information technology in management // Property Management. 1993. N 11. P. 288.

About the authors:

Igor F. Kefeli, Director of the Geopolitical Expertise Center of North-West Institute of Management of RANEPA (St. Petersburg, Russian Federation), Doctor of Science (Philosophy), Professor; geokefeli@mail.ru

Sergey A. Malmberg, Ggraduate Student of North-West Institute of Management of RANEPA (St. Petersburg, Russian Federation); smalmberg@mail.ru