УДК 34 **DOI: 10.34670/AR.2020.91.11.007**

Организационно-правовые механизмы импортозамещения в сфере защиты цифрового суверенитета Российской Федерации

Колонтаевская Ирина Федоровна

Доктор педагогических наук,
кандидат юридических наук, профессор,
завкафедрой гражданского права и процесса,
Московский университет им. С.Ю. Витте,
115432, Российская Федерация, Москва, 2-й Кожуховский пр., 12/1;
e-mail: Kolontaevskaya@mail.ru

Статья опубликована в рамках поддержанного РФФИ научного проекта № 19-011-00373.

Аннотация

В статье определяется необходимость принятия в Российской Федерации эффективных организационно-правовых мер для стимулирования импортозамещения в информационной сфере. Обосновывается, что переход России на импортозамещение цифровых продуктов и программного обеспечения вызван реальными угрозами, которые несет в себе киберзависимость от зарубежных цифровых технологий. Раскрывается понятие цифрового (информационного) суверенитета, под которым понимается право государства самостоятельно формировать информационную политику независимо от внешнего влияния, осуществлять контроль над своей информационной средой и обеспечивать информационную безопасность как в национальном, так и в глобальном информационном пространстве. Анализируется современное состояние нормативно-правового обеспечение процессов импортозамещения в информационной сфере. Раскрываются нерешенные проблемы. Делаются конкретные предложения по совершенствованию организационно-правовой защиты цифрового суверенитета Российской Федерации.

Для цитирования в научных исследованиях

Колонтаевская И.Ф. Организационно-правовые механизмы импортозамещения в сфере защиты цифрового суверенитета Российской Федерации // Вопросы российского и международного права. 2019. Том 9. № 11А. С. 67-76. DOI: 10.34670/AR.2020.91.11.007

Ключевые слова

Цифровой (информационный) суверенитет, информационная безопасность, импортозамещение, софт, нормативно-правовое обеспечение, информационная инфраструктура.

Введение

Все, что нас окружает – предметы, явления или процессы – имеет как положительные, так и отрицательные свойства, характеристики и последствия. Не являются исключением и процессы масштабной цифровизации, охватившие в настоящее время в Российской Федерации практически все сферы жизнедеятельности. Многие человеческие действия сейчас происходят виртуальной среде: взаимодействие с органами власти, удаленная работа, коммерция, получение образования, медицинское консультирование и многое другое. Однако вместе с очевидными благами цифровизация несет в себе серьезные риски и угрозы. Люди становятся рабами цифры, подсаживаются на компьютерные игры и коммуникации, создается иллюзия общения, самозанятостим, самодостаточности. Жизненный успех для значительной группы пользователей Интернета измеряется не реальными достижениями или хотя бы материальными благами, а количеством лайков, полученных в Инстаграме за выложенные там рафинированные фото. Мы находимся в плену электронный сервисов – билеты на поезд, самолет, в театр, талоны к врачу, онлайн покупки, денежные транзакции, выбор оптимального маршрута и т.д. А если это все на какое-то время выключится или попадет под запрет? Но все это мелочи по сравнению с тем, какие риски и угрозы несет цифровизация обществу и государству в целом. Тотальная зависимость от цифровой среды, задействованной на иностранном программном обеспечении, создает уже угрозы информационной безопасности другого уровня, среди которых коммуникация преступников, в том числе террористов и экстремистов; организация протестных выступлений; информационная агрессия по отношению к странам, не имеющим собственных цифровых ресурсов и не способным защитить свой цифровой суверенитет; технологический шантаж под страхом отключения целых глобальных сервисов, обеспечивающих жизнедеятельность в различных сферах [Aminov, 2019]. В конце концов, под угрозой может оказаться экономическая и технологическая независимость страны, национальный цифровой суверенитет страны в целом.

Основная часть

Следует подчеркнуть, что зависимость России от зарубежного софта была предопределена тем, что Интернет, появившийся практически одновременно в военных лабораториях США, Великобритании и Франции 50 лет назад (1969 г.) [Byung-Keun Kim, 2005], стал активно распространяться у нас в стране лишь спустя 25-30 лет. Эти потерянные в информационно-технологическом отношении годы стали фактором существенного отставания российских разработчиков от западных игроков и, как следствие, вызвали стойкую импортозависимость в информационной сфере. Серьезные проблемы в обеспечении экономической безопасности России начались с 2014 года, когда западные платежные системы «Виза» и «Мастеркард» отказались обслуживать свои банковские карты в Крыму. После демарша компаний было принято решение создать свою платежную систему «Мир», которое было быстро и успешно реализовано.

Аналогичная угроза отключения России от системы межбанковских платежей S.W.I.F.T. вызвала упреждающие действия по созданию российского аналога, уже протестированного Центробанком.

Осуществляемый в настоящее время активный переход России на отечественное импортозамещение в сфере информационных технологий (IT) и программного обеспечения

(ПО) имеет принципиальное значение с точки зрения личной и общественной, экономической и информационной безопасности, национального цифрового суверенитета в целом. Перевод информационных процессов на отечественный софт (от англ. Software – программное обеспечение), вызван реальными угрозами, которые несет в себе киберзависимость от зарубежных цифровых технологий. Практически безграничные возможности, которые предоставляют телекоммуникационные системы, позволяют беспрепятственно вторгаться в различные сферы деятельности государств, осуществляя информационную агрессию по отношению к странам, не способным защитить свой цифровой суверенитет [Джойс, Симаков, 2018]. При этом основная угроза состоит в том, что в случае того или иного политически-мотивированного решения возможно отключение целых глобальных сервисов, обеспечивающих жизнедеятельность в различных сферах. В результате деловая жизнь в стране может, практически, остановится. Все современные технологии имеют средства удаленного контроля. Это означает, что оборудование иностранного производства находится под контролем другого государства. Российские объекты критической инфраструктуры базируются на американских и европейских технологиях, и в случае резкого ухудшения политических отношений в работу таких объектов можно вмешаться извне или вовсе отключить их дистанционно. Подобный инцидент произошел осенью 2019 г. с госкорпорацией «Газпромом», когда австрийский производитель закупленных российской компанией компрессоров LMF дистанционно, через спутник, отключил их, превратив в груду металлолома. И таких инцидентов уже случилось немало.

Очевидно, что государства без собственных цифровых платформ в условиях меняющегося мира могут потерять если не суверенитет, то огромное количеств возможностей и право на будущее [Носков, www].

Следует сразу отметить, что законодательство не содержит нормативного понятия цифрового суверенитета. В статье 1 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» определены отдельные принципы обеспечения государственного суверенитета России в информационном пространстве: создание условий для развития российской инфраструктуры связи, обеспечение централизованного управления российскими радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации, создание условий для обеспечения потребностей в связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

Обобщая различные точки зрения [Кучерявый, 2014; Зорина, 2017; Артамонов, 2017], цифровой (информационный) суверенитет можно определить, как право государства самостоятельно формировать информационную политику независимо от внешнего влияния, осуществлять контроль над своей информационной сферой и обеспечивать информационную безопасность как в национальном, так и в глобальном информационном пространстве. Информационный суверенитет включает в себя любые компоненты, связанные с информационной сферой государства: технологические, политические, экономические, организационно-правовые, идеологические, социальные.

В настоящее время в РФ идет формирование организационно-правовых основ, направленных на обеспечение безопасности национальной информационной инфраструктуры и создание отечественного софта, что стало особенно актуальным после введения, начиная с марта 2014 года странами Запада санкций против России [Ефремов, 2017].

Активные действия по продвижению в сторону импортозамещения программного обеспечения были сделаны в 2015 году, когда был принят Закон о создании Реестра российских

программ для ЭВМ и баз данных, ограничивающих для госструктур закупку иностранного софта[1].

Постановление Правительства РФ от 16.11.2015 №1236[2] и Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ (Минкомсвязи) от 01.04.2015 № 96[3] ввели запрет на осуществление закупок для муниципальных и государственных нужд программного обеспечения, не включенного в Единый реестр российских программ для электронных вычислительных машин и баз данных (далее Реестр). При этом логика инициативы Минкомсвязи состояла в том, что импортозамещение даст российским разработчикам и компаниям реальный шанс заключить выгодные контракты с госорганами и получить финансирование для развития бизнеса, что в свою очередь, будет способствовать росту доходов отечественных производителей цифровой продукции и увеличению новых рабочих мест.

Единый Реестр, содержащий сведения обо всем программном обеспечении, официально происходящем из Российской Федерации, начал функционировать в январе 2016 года [Носков, www]. Все попавшие в Реестр IT-решения стали пользоваться приоритетом при госзакупках. Как следствие, в настоящее время доля российского ПО в закупках госорганов составляет уже 65% (в 2015 г.– 20%) [Шмырев, www].

Аналогичные протекционистские и технологически ограничительные меры были приняты в отношении госкомпаний, которым также предписывалось при закупке софта отдавать предпочтение российским цифровым технологиям из Реестра. Предполагается, что к 2021 году доля российского программного обеспечения, закупаемого госкомпаниями, должна превысить 50%, а к 2024 – 70%. Для госорганов этот процент в 2024 году должен составить 90% [Степанова, www].

Кроме ограничительных и протекционистских механизмов правовой поддержки российских разработчиков цифровых технологий с 2009 года[4] для IT-компаний были введены пониженные ставки по страховым взносам[5].

Информационная функция государства и его информационная политика являются механизмами реализации и обеспечения государственного суверенитета в информационном пространстве [Ефремов, 2017]. В 2016 году Указом Президента РФ от 05.12.2016 № 646 была утверждена Доктрина информационной безопасности Российской Федерации[6].

С 1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О

[1] Федеральный закон от 29.06.2015 № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

[2] Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

[3] Приказ Минкомсвязи России «Об утверждении плана импортозамещения программного обеспечения» от 01.04.2015 № 96.

[4] Федеральный закон от 24 июля 2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования» (утратил силу).

[5] «Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов» (утв. Минфином России).

[6] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// СЗ РФ 12.12.2016, № 50, ст. 7074.

безопасности критической информационной инфраструктуры Российской Федерации», работа над которым продолжалась с 2006 по 2017 годы. Закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В 2019 году был утвержден федеральный проект «Информационная инфраструктура», который обозначил курс на создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных, а также функционирования цифровых платформ работы с данными для обеспечения потребностей граждан, бизнеса и власти на основе отечественных разработок[7].

В 2019 году президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам был утвержден Национальный проект «Национальная программа «Цифровая экономика Российской Федерации», который предусматривает Создание «сквозных» цифровых технологий преимущественно на основе отечественных разработок[8].

В рамках нацпроекта «Цифровая экономика РФ» реализуется подпроект «Нормативное регулирование цифровой среды», в ходе которого корректируется или разрабатывается огромное количество различных нормативных правовых актов. При этом предполагается создание двух-трех рамочных законов, которые будут регламентировать те или иные сферы. Рамочный формат законов предполагает, что их полноценная работа зависит от дополнительных подзаконных нормативных правовых актов, решений властей и развития информационных технологий.

С 1 ноября 2019 года вступил в силу Закон об обеспечении безопасной и устойчивой работы российского сегмента Интернета (Рунета) на случай, если его отключат от глобальной инфраструктуры сети[9]. В соответствии с Законом в России должна появиться дублирующая инфраструктура для бесперебойной работы Интернета. В случае угроз Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) сможет взять на себя централизованное управление сетью связи общего пользования. Список возможных угроз будет определен Правительством РФ. По словам министра цифрового развития, связи и массовых коммуникаций Российской Федерации К.Ю. Носкова, «этот закон – подушка безопасности: … если что-то произойдет, мы сможем продолжать жить обычной жизнью и ничего не лишимся» [Носков, www].

2 декабря 2019 года Президент РФ В.В. Путин подписал закон о предустановке отечественного софта на гаджеты, который вступает в силу с 1 июля 2020 года. Законом устанавливается, что при продаже отдельных видов технически сложных товаров с предварительно установленными программами для электронных вычислительных машин потребителю обеспечивается возможность использовать отдельные виды технически сложных товаров с предварительно установленными российскими программами для электронных

[7] Паспорт федерального проекта «Информационная инфраструктура» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9).

[8] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

[9] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон» Об информации, информационных технологиях и о защите информации».

вычислительных машин. На практике это означает, что на смартфонах, компьютерах, телевизорах с функцией Smart TV перед продажей в России должно быть установлено отечественное ПО. Перечень товаров, на которые должны устанавливать российский софт, и самих приложений определяет Правительство РФ. За отказ от предварительной установки российского софта ИП грозит штраф от 100 до 500 тыс. рублей, юрлицам от 500 тыс. до 1 млн рублей.

К настоящему времени РФ добилась ощутимых успехов в информационной сфере. Сейчас у нас есть собственные поисковые системы «Яндекс» и «Рамблер», свои популярные социальные сети «ВКонтакте» и «Одноклассники», справочно-правовые системы «Гарант» и «КонсультантПлюс», антивирус Касперского, крупнейшая почта Рунета «Mail.ru», портал Госуслуг, свои аналоги «Uber», пакеты «МойОфис», «Дело», система виртуализации «Тионикс». Есть российские сборки Linux, продукты 1С, ABBYY. Создан аналог международной платежной системы S.W.I.F.T. Проходит испытания национальная мобильная операционная система «Аврора». Продолжается работа над созданием альтернативы Microsoft Office, в ближайшее время начнется создание сети мобильной связи пятого поколения 5G. Локализован российский сегмент Интернета, выделена защищенная сеть военным. Построена российская многофункциональная система персональной спутниковой связи «Гонец», чем поставлен барьер на пути британского проекта спутниковой сети OwnWeb.

Чисто российским продуктом является Единая биометрическая система, разработанная ПАО «Ростелеком» и позволяющая подтвердить личность по лицу и голосу с помощью видеокамеры и микрофона собственного смартфона. Это технологическое достижение было санкционировано Федеральным законом от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», благодаря которому в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» появилась новая статья 14.1. «Применение информационных технологий в целях идентификации граждан Российской Федерации».

Вместе с тем, процессы импортозамещения наталкиваются на серьезные проблемы. В первую очередь, это – недофинансирование направления «Информационная безопасность» в нацпроекте «Цифровая экономика РФ». По объему финансирования это направление находится на последнем месте. Для обеспечения безопасности такой огромной страны, как Российская Федерация, семнадцать миллиардов рублей, выделенных на реализацию мер по направлению «Информационная безопасность» на три года, – это ничтожная сумма. В самый конец списка приоритетов нацпрограммы попало и все, что относится к импортозамещению [Шпунт, www].

Серьезной проблемой является неравномерность импортозамещения. По многим направлениям российским разработчикам удалось практически полностью вытеснить иностранных игроков. Однако, если по разработкам в сфере кибербезопасности и антивирусов, а также систем электронного документооборота российские компании уже заняли лидирующие позиции на отечественном рынке, то по большинству классов программного обеспечения успехи гораздо скромнее, например, по разработкам аппаратных компонентов и программно-аппаратных комплексов, баз данных, а также систем управления и проектирования, платформ для разработки прикладных систем, языков программирования, систем для промышленности и систем для проектирования.

На текущем этапе в контексте процессов импортозамещения должны решаться задачи не только удовлетворения потребностей внутреннего национального высокотехнологичного рынка, но и стимулирования технологического развития стратегических отраслей экономики, а

также экспорта дорогостоящей высокотехнологичной продукции [Бетелин, 2016]. Вместе с тем, существуют объективные причины ограничения востребованности российской цифровой продукции. Так, из-за санкций российские разработчики не могут предложить свои услуги для нефтегазовой отрасли платежеспособным иностранным клиентам. Вместе с тем законодательство позволяет отечественному заказчику обратиться к иностранным разработчикам, если российского аналога «с необходимыми функциональными, техническими и (или) эксплуатационными характеристиками» не существует. Этой легальной оговоркой часто пользуются госорганы, стремящиеся по инерции использовать привычный иностранный софт. К тому же некоторые компании с госучастием не хотят нести финансовые и орграсходы на программу импортозамещения [Александрова, www].

Современная практика развития правового регулирования информационных отношений в Российской Федерации может входить в определенные противоречия с процессами евразийской интеграции. Так реализация принципа импортозамещения в сфере информационных технологий, основанного на госзакупках в РФ лишь отечественного софта, вступила в противоречие с созданием единого рынка услуг в сфере разработки программного обеспечения в ЕАЭС. Для снятия острой ситуации было принято Постановление Правительства РФ от 20.12.2017 № 1594 «О внесении изменений в постановление Правительства Российской Федерации от 16 ноября 2015 г. №1236», вступившее в силу с 1 января 2018 года. Оно разрешает закупать и использовать программное обеспечение, происходящее из государств Евразийского экономического союза (ЕАЭС), для обеспечения государственных и муниципальных нужд.

Проблемой является и то, что многие государственные информационные системы (ГИС) работают в тесном взаимодействии с иностранным софтом – браузером Internet Explorer и операционной системой Windows, разработанными транснациональной корпорацией Microsoft. На решение этой проблемы направлено Постановление Правительства РФ «О централизованных закупках офисного ПО»[10], требующее, чтобы до 2020 года держатели всех ГИС обеспечили их совместимость с российским софтом.

Еще одной серьезной проблемой является правовая неопределенность в законодательстве понятия «российских продукт» (или «отечественный продукт») и «российская компания», что создает правовые трудности определения отечественных производителей и, соответственно, российских продуктов, для последующего их внесения в Реестр. В связи с тем, что при закупках программного обеспечения государственными органами и государственными компаниями приоритет должен отдаваться отечественным программным продуктам, необходимо в нормативно-правовую базу внести соответствующие поправки. В настоящее время российскими считаются компании, зарегистрированные в России, платящие налоги в российский бюджет и не нарушающие законодательство России. В то же время, в РФ зарегистрировано множество дочерних предприятий зарубежных компаний, которые по закону считаются российскими, хотя исполняют распоряжения зарубежных правообладателей программного обеспечения.

Беспокойство российских разработчиков вызывает решение Экспертного совета по импортозамещению, курирующего работу Реестра, о поэтапном исключении из него софта,

[10] Постановление Правительства РФ от 08.06.2018 № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности».

основанного на иностранных базах данных, серверах приложений и платформах. Из-за того, что четкого легального определения платформам не дано, остается неясным, какие именно продукты из Реестра могут убрать. В результате заказчики не хотят покупать отечественный софт, который скоро может быть исключен из Реестра. В такой ситуации заказчикам надо давать официальные разъяснения по содержанию Реестра, чтобы они понимали какие отечественные программы имеют спрос, опыт внедрения и пользуются надежной поддержкой.

Необходимо также разработать адекватные критерии включения цифровых продуктов в Реестр. В настоящее время принадлежность к отечественному софту определяется владельцем исключительных прав на софт и конечным бенефициаром, которые должны быть гражданами РФ. Однако российский разработчик может просто купить исключительные права у иностранной компании, что автоматически сделает ПО отечественным. Но это не гарантирует наличия в России реальных компетенций для поддержания и развития продукта. С другой стороны, представителей компьютерного и информационного бизнеса настораживают такие предложения в законодательство, чтобы российским ПО считать только то, что написано полностью с нуля на отечественном инструментарии и должно работать полностью на отечественных процессорах [Степанова, www].

Участие в программе импортозамещения требует от российских разработчиков больших затрат, в том числе на проведение дорогостоящей экспертизы на российское происхождение продукта. Поэтому следует расширять преференции и тем самым помочь российским компаниям попасть в Реестр, нарастить долю участия как на рынке госзакупок, так и в корпоративном сегменте.

Следовательно, необходимо совершенствование нормативно-правового сопровождения процессов цифровизации и обеспечения информационной безопасности.

Заключение

Можно заключить, что в настоящее время актуальность развития производства цифровой продукции на национальном уровне каждого государства обусловливается не только стремлением повысить уровень экономики страны, но и вопросами национальной безопасности и сохранения цифрового суверенитета. Задача при этом состоит не в том, чтобы обеспечить полное импортозамещение, а в том, чтобы снизить информационные риски страны.

В РФ имеется достаточный потенциал, чтобы гарантировать свой цифровой суверенитет. В то же время, Россия, развивая отечественные цифровые технологии, не ставит целью обособление от глобального рынка. Российская Федерация будет продвигать свои разработки за рубежом и намерена действовать совместно с международными партнерами. Цель цифровой экономики и цифрового развития в мире заключается построении единого безопасного цифрового пространства.

Библиография

1. Александрова Е. Охранительный софт. Насколько эффективны протекционистские меры по импортозамещению ПО. URL: https://www.kommersant.ru/doc/4125716
2. Артамонов Д.С. Информационный суверенитет, теоретический аспект // Материалы VIII Международного Конституционного Форума, посвященного 80-летию Саратовской области. 2017. С. 16-20.
3. Бетелин В.Б. О проблеме импортозамещения и альтернативной модели экономического развития России // Стратегические приоритеты. 2016. № 1 (9). С. 11-21.
4. Джойс Э.А., Симаков А.А. Цифровой суверенитет и правовое регулирование пиринговых платежных систем //

Научный вестник Омской академии МВД России. 2018. № 3 (70). С. 54-60.
5. Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201-215.
6. Зорина Е.Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. 2017. Т. 17. Вып. 3. С. 345-348.
7. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. Вып. 9 (69). С. 12.
8. Медведев Д.А. Цифровое будущее уже совсем рядом. URL: https://rg.ru/2019/11/03/dmitrij-medvedev-cifrovoe-budushchee-uzhe-sovsem-riadom.html
9. Носков К.Ю. Весь мир завидует нашим цифровым технологиям. URL: https://digital.gov.ru/ru/events/39402/
10. Степанова Ю. Иностранный код в виде исключения. Государство откажется от части зарубежного софта. URL: https://www.kommersant.ru/doc/4179553
11. Шмырев В. Информационные технологии в госсекторе. URL: https://cnews.ru/news/top/2019-04-24_dolya_rossijskogo_po_v_zakupkah_gosorganov_dostigla
12. Шпунт Я. Сложная, но необходимая работа. URL: http://www.comnews.ru/content/203348/2019-12-05/2019-w49/slozhnaya-no-neobkhodimaya-rabota
13. Aminov I.I. The significance of artificial intelligence and blockchain technologies in criminological and psychological forecasting and prevention of criminal behavior // Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth. 2019. P. 448-451.
14. Byung-Keun Kim. Internationalizing the Internet, the Co-evolution of Influence and Technology. Edward Elgar, 2005. P. 51-55.

Organizational and legal mechanisms of import substitution in the field of protection of digital sovereignty of Russian Federation

Irina F. Kolontaevskaya

Doctor of Pedagogy, PhD in Law, Professor,
Head of the Department of Civil law and procedure,
Witte Moscow University,
115432, 12/1, 2nd Kozhukhovskii ave., Moscow, Russian Federation;
e-mail: Kolontaevskaya@mail.ru

Abstract

The article defines the need to take effective organizational and legal measures in the Russian Federation to stimulate import substitution in the information sphere. It is proved that Russia's transition to import substitution of digital products and software is caused by real threats posed by cyber-dependence on foreign digital technologies. The concept of digital (information) sovereignty, which is understood as the right of the state to independently form information policy regardless of external influence, to exercise control over its information environment and to ensure information security both in the national and global information space, is revealed. The article analyzes the current state of legal regulation of import substitution processes in the information sphere. The unsolved problems are revealed. Specific proposals are made to improve the organizational and legal protection of the digital sovereignty of the Russian Federation. We can conclude that at present, the relevance of the development of digital production at the national level of each state is determined not only by the desire to improve the country's economy, but also by issues of national security and preservation of digital sovereignty. The task in this case is not to ensure complete import substitution, but to reduce the country's information risks. In the Russian Federation there is sufficient potential to guarantee its digital sovereignty. At the same time, Russia, developing

domestic digital technologies, does not set as its goal isolation from the global market.

For citation

Kolontaevskaya I.F. (2019) Organizatsionno-pravovye mekhanizmy importozameshcheniya v sfere zashchity tsifrovogo suvereniteta Rossiiskoi Federatsii [Organizational and legal mechanisms of import substitution in the field of protection of digital sovereignty of Russian Federation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (11A), pp. 67-76. DOI: 10.34670/AR.2020.91.11.007

Keywords

Digital (information) sovereignty, information security, import substitution, software, regulatory support, information infrastructure.

References

1. Aleksandrova E. *Okhranitel'nyi soft. Naskol'ko effektivny protektsionistskie mery po importozameshcheniyu PO* [Security software. How effective are protectionist measures for import substitution?]. Available at: https://www.kommersant.ru/doc/4125716 [Accessed 09/09/2019]
2. Aminov I.I. (2019) The significance of artificial intelligence and blockchain technologies in criminological and psychological forecasting and prevention of criminal behavior. In: *Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth.*
3. Artamonov D.S. (2017) Informatsionnyi suverenitet, teoreticheskii aspekt [Information sovereignty, theoretical aspect]. In: *Materialy VIII Mezhdunarodnogo Konstitutsionnogo Foruma, posvyashchennogo 80-letiyu Saratovskoi oblasti* [Materials of the VIII International Constitutional Forum dedicated to the 80th anniversary of the Saratov region].
4. Betelin V.B. (2016) O probleme importozameshcheniya i al'ternativnoi modeli ekonomicheskogo razvitiya Rossii [On the problem of import substitution and an alternative model of economic development of Russia]. *Strategicheskie prioritety* [Strategic priorities], 1 (9), pp. 11-21.
5. Byung-Keun Kim (2005) *Internationalizing the Internet, the Co-evolution of Influence and Technology.* Edward Elgar.
6. Dzhois E.A., Simakov A.A. (2018) Tsifrovoi suverenitet i pravovoe regulirovanie piringovykh platezhnykh sistem [Digital sovereignty and legal regulation of peer-to-peer payment systems]. *Nauchnyi vestnik Omskoi akademii MVD Rossii* [Scientific Herald of the Omsk Academy of the Ministry of Internal Affairs of Russia], 3 (70), pp. 54-60.
7. Efremov A.A. (2017) Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva [Formation of the concept of state information sovereignty]. *Pravo. Zhurnal Vysshei shkoly ekonomiki* [Law. Journal of the Higher School of Economics], 1, pp. 201-215.
8. Kucheryavyi M.M. (2014) Gosudarstvennaya politika informatsionnogo suvereniteta Rossii v usloviyakh sovremennogo global'nogo mira [State policy of information sovereignty of Russia in the modern global world]. *Upravlencheskoe konsul'tirovanie* [Management Consulting], 9 (69), p. 12.
9. Medvedev D.A. *Tsifrovoe budushchee uzhe sovsem ryadom* [The digital future is just around the corner]. Available at: https://rg.ru/2019/11/03/dmitrij-medvedev-cifrovoe-budushchee-uzhe-sovsem-riadom.html [Accessed 09/09/2019]
10. Noskov K.Yu. *Ves' mir zaviduet nashim tsifrovym tekhnologiyam* [The whole world is jealous of our digital technology]. Available at: https://digital.gov.ru/ru/events/39402/ [Accessed 09/09/2019]
11. Shmyrev V. *Informatsionnye tekhnologii v gossektore* [Information technology in the public sector]. Available at: https://cnews.ru/news/top/2019-04-24_dolya_rossijskogo_po_v_zakupkah_gosorganov_dostigla [Accessed 09/09/2019]
12. Shpunt Ya. *Slozhnaya, no neobkhodimaya rabota* [Complex, but necessary work.]. Available at: http://www.comnews.ru/content/203348/2019-12-05/2019-w49/slozhnaya-no-neobkhodimaya-rabota [Accessed 09/09/2019]
13. Stepanova Yu. *Inostrannyi kod v vide isklyucheniya. Gosudarstvo otkazhetsya ot chasti zarubezhnogo softa* [Foreign code as an exception. The state will refuse part of foreign software]. Available at: https://www.kommersant.ru/doc/4179553 [Accessed 09/09/2019]
14. Zorina E.G. (2017) Informatsionnyi suverenitet sovremennogo gosudarstva i osnovnye instrumenty ego obespecheniya [Information sovereignty of the modern state and the main tools to ensure it]. *Izvestiya Saratovskogo universiteta* [Bulletin of the Saratov University], 17, 3, pp. 345-348.