

Вопросы безопасности

Правильная ссылка на статью:

Дубень А.К. — Технологический суверенитет как основа национальной безопасности Российской Федерации // Вопросы безопасности. – 2023. – № 4. – С. 166 - 172. DOI: 10.25136/2409-7543.2023.4.69347 EDN: JZMTQE URL: https://nbpublish.com/library_read_article.php?id=69347

Технологический суверенитет как основа национальной безопасности Российской Федерации

Дубень Андрей Кириллович

научный сотрудник Института государства и права Российской академии наук

119019, Россия, Москва область, г. Москва, ул. Знаменка, 10

✉ k.duben@mail.ru



[Статья из рубрики "Научно-техническое обеспечение национальной безопасности"](#)

DOI:

10.25136/2409-7543.2023.4.69347

EDN:

JZMTQE

Дата направления статьи в редакцию:

16-12-2023

Дата публикации:

31-12-2023

Аннотация: Предмет исследования образует совокупность правовых норм нормативных правовых актов Российской Федерации, международных договоров (соглашений), регулирующих общественные отношения в сфере регулирования технологического суверенитета, правоприменительная практика, а также положения теоретических междисциплинарных исследований в указанной сфере. Исследование посвящено актуальной теме в юридической науке. Технологический суверенитет – это концепция, которая предполагает возможность государства контролировать свои технологии, данные и цифровую инфраструктуру. Эта проблема вызывает озабоченность в эпоху глобализации и растущей зависимости от технологий, поскольку государство стремится сохранить свою технологическую независимость и защитить свои интересы в цифровой сфере. В статье рассмотрена концепция технологического суверенитета и её значение в

современном мире с акцентом на необходимость контролировать данные. Методологической основой данной работы стала система современных общенаучных и частноправовых методов. Исследование формирования, развития, места и роли технологического суверенитета проводилось с использованием следующих общенаучных методов: анализа и синтеза, абстрагирования и моделирования, наблюдения, обобщения, описания, классификации и др. В работе использовались специальные частно-правовые методы познания сравнительно-правовой, формально-юридический. Для реализации целей и задач настоящего исследования, автор приводит краткий анализ существующих методологических подходов к технологическому суверенитету, как понятию в общей системе знаний, а также формулирует авторское определение данной категории. Автор делает вывод, что обеспечение технологического суверенитета позволит гарантировать национальную безопасность Российской Федерации, тем самым создавая условия для противодействия в условиях новых вызовов, угроз и рисков: внутренним и внешним информационным угрозам при использовании цифровых технологий; развивающимся деструктивным процессам, направленным на информационное пространство Российской Федерации, нарушение прав и свобод граждан, безопасности общества и государства, а также задачами обеспечения социально-экономического развития страны и отечественных цифровых технологий, технологического суверенитета Российской Федерации.

Ключевые слова:

технологический суверенитет, информация, независимость, правопорядок, защита данных, безопасность, национальная безопасность, конкуренция, понятие, безопасность данных

Достижение технологического суверенитета в критически важных отраслях, на сегодняшний день, это основная задача государства, так как обеспечение суверенитета в данной сфере позволит государству контролировать свои технологии, данные и цифровую инфраструктуру. Эта современная проблема вызывает озабоченность в эпоху глобализации и растущей зависимости от технологий, поскольку государство стремится сохранить свою технологическую независимость и защитить свои интересы в цифровой сфере в условиях новых вызовов, угроз и рисков.

Впервые задача об обеспечении технологического суверенитета была закреплена в Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, в которой одной из задач являлось «государственной политики в области создания условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами». Ранее в Указе Президента Российской Федерации от 20 апреля 2014 г. № 259 «Об утверждении Концепции государственной политики Российской Федерации в сфере содействия международному развитию» также были предусмотрены задачи по созданию условий для обеспечения «технологического суверенитета государств - получателей помощи в области информационных, коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися государствами».

Стоит отметить, что вопросу технологического суверенитета уделено особое внимание. В 2023 году Правительство Российской Федерации представило проект федерального

закона «О технологической политике в Российской Федерации». Данный законопроект нацелен на гармонизацию научной и промышленной политики ориентированный на развитие приоритетных технологий, определяемых государством в соответствии с потребностями рынка, а также на создание инфраструктуры для свободного развития перспективных технологий. Предлагается ввести специальные правовые режимы, которые позволят исключать отдельные аспекты из общего регулирования для ускорения разработки технологий и обеспечения долгосрочных изменений в этом направлении. Тем самым, законопроект поможет улучшить взаимодействие между представителями науки и промышленности и создаст основу для более успешной реализации инвестиционных проектов в области научных разработок, исследований и научно-исследовательских и опытно-конструкторских работ. На наш взгляд, в данном законопроекте целесообразно сформулировать отдельные положения, касающиеся организации и проведения экспертизы проектов технологического суверенитета (например, Федеральный закон от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике»).

Сегодня национальная система требует дополнительных мер по эффективному обеспечению технологического суверенитета, которая определяется многовекторностью развития общественных отношений в информационной сфере в современных условиях цифровизации, формирования многополярного мира, усиления противоборства и кибератак в информационном пространстве.

Усиление давления со стороны зарубежных хакерских группировок, увеличение масштаба компьютерных атак на российскую инфраструктуру разработчиков программ и оборудования способствовало актуализации достижения технологического суверенитета России и, соответственно, технического регулирования объектов в информационном пространстве и мер оперативного реагирования на вопросы организационного характера для обеспечения технологического суверенитета России и оптимизации управления технологическими и производственными процессами объектов критической информационной инфраструктуры. В этой связи особенно важным представляется принцип реализации политики технологического суверенитета в сфере информационно-коммуникационных технологий в целях обеспечения информационной безопасности.

В соответствии с Указом Президента РФ от 30 марта 2022 г. № 166 органам государственной власти с 1 января 2025 г. запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры. К такому программному обеспечению относятся операционные системы, среды виртуализации, браузеры, офисное программное обеспечение, СУБД, системы анализа и визуализации данных (BI-системы) и программное обеспечение транспортной технологической подсистемы [\[1, с. 9\]](#). В соответствии с Распоряжением Правительства Российской Федерации от 20 мая 2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» технологическое развитие осуществляется посредством комплексного, системного подхода к организации инновационного цикла, тем самым технологический суверенитет рассматривается как определенный уровень независимости страны от зарубежных производителей и поставщиков услуг в областях науки, техники и технологий, чем обеспечивается беспрепятственная реализация национальных интересов в информационной сфере с учетом существующих и прогнозируемых угроз.

Президент Российской Федерации отметил: «За короткий срок России предстоит создать или вывести на новый уровень собственные критически важные технологии в

микроэлектронике, IT-промышленности, транспорте, в разработке лекарств и новых материалов, в других важнейших для страны направлениях» [\[2\]](#). При этом Председатель Совета Федерации Федерального Собрания Российской Федерации отметила, что достижение технологического суверенитета в критически важных отраслях – это основная и главная задача государства на решение которой должны быть задействованы все силы [\[3\]](#).

Обеспечение технологического суверенитета позволит в дальнейшем снизить зависимость от импорта, которая, в свою очередь, повлияет на развитие собственной информационной инфраструктуры. Нормативно-правовое регулирование в данной сфере направлено на развитие отечественного производства информационно-коммуникационных технологий за счет использования протекционистских методов, способствующих снижению доли импорта зарубежной продукции и замещению данной продукции аналогичными товарами российского производства. Тем самым, позволит в дальнейшем повысить конкурентоспособность отечественной информационной продукции, в том числе средств защиты информации, а также увеличить количество рабочих мест в соответствующих отраслях экономики.

На наш взгляд, для обеспечения технологического суверенитета в информационной сфере необходима ориентация на развитие отечественных технических средств и информационно-коммуникационных технологий, что позволит свести к минимуму долю иностранной информационной продукции, импортируемой из зарубежных стран. Особенно это важно в отношении средств защиты информации и реализации политики импортозамещения. Подобные меры позволят добиться реализации задач сразу по нескольким направлениям: экономический рост и развитие страны, обеспечение суверенитета и возможности проведения независимой государственной политики в интересах Российской Федерации.

Одновременно при обеспечении цифрового суверенитета следует выстроить информационно-техническую систему, защищающую информацию от утечки при использовании информационных технологий зарубежных государств. Следует особо отметить, что в условиях трансформации и цифровизации права сформировалась необходимость в определении понятий «цифровой суверенитет» и «технологический суверенитет». Данные дефиниции не имеют сегодня правовой определенности несмотря на их ключевое значение в области обеспечения информационной безопасности. Так, в Приказе Минпромторга России от 29 мая 2019 г. № 1869 «Об утверждении концепции создания российского сегмента евразийской сети промышленной кооперации и субконтрактации» одной из основных задач российского сегмента промышленной кооперации является обеспечение цифрового суверенитета по защите информации в соответствии с законодательством России, вместе с тем в вышеуказанном акте данное определение отсутствует.

Вместе с тем, считаем, что под дефиницией «технологический суверенитет» следует понимать способность государства располагать технологиями, которые считаются критически важными для обеспечения благосостояния и конкурентоспособности государства и осуществления беспрепятственной реализации национальных интересов с учетом существующих и перспективных угроз.

Следует отметить, что в большинстве случаев государство выражает данную дефиницию через национальную идентификацию в сети Интернет [\[4, с. 32\]](#). При этом блокирование некоторых информационных ресурсов в сети Интернет трактуется как выражение

цифрового суверенитета. Несомненно, что в новых геополитических условиях глобальной технологической трансформации и экстерриториальности значимость цифрового суверенитета возрастает для обеспечения безопасности государства. Следует согласиться с позицией отдельных авторов относительно того, что наличие цифрового суверенитета способствует защите собственного национального сегмента общественного, политического, социально-экономического пространства, а в современных условиях от цифрового суверенитета зависит уровень государственного суверенитета в целом [\[5, с. 208\]](#). Полагаем, что цифровой суверенитет, с одной стороны, является компонентом технологического суверенитета, а с другой – в полной мере основан на последнем.

На наш взгляд, при наличии большого количества кибератак и отдельных угроз цифровой суверенитет является возможностью независимого суверенного государства самостоятельно определять степень и способ участия в информационной деятельности при применении цифровых технологий для реализации собственных интересов и противодействия противоправным действиям в национальном информационном пространстве.

Данные выводы показывают связь информационных рисков с потенциальными угрозами национальной безопасности России. А.Х. Валеев обращает внимание на то, что информационно-коммуникационная сеть Интернет выступает в качестве платформы по обмену мнениями отдельных лиц, тем самым данная площадка имеет негативные факторы распространения недостоверной информации и пропаганды идеологических мнений, которые в целом угрожают отдельным социальным группам, обществу и государству в целом [\[6, с. 125\]](#). Аналогичной точки зрения придерживалась И.Л. Бачило, которая в своих работах не раз обращала внимание на трансформацию информационных платформ, которые, в свою очередь, затрагивают конституционные права человека в части свободы слова и мысли [\[7, с. 286\]](#). В то же время технологический суверенитет государства в современных условиях позволит достичь информационной свободы в рамках обеспечения национальной безопасности.

В свою очередь, в новых геополитических условиях государственная политика в сфере обеспечения информационной безопасности изменилась. В настоящее время проблема обеспечения информационной безопасности имеет первостепенное значение и требует принятия новых правовых решений. Одним из основных способов решения вопросов обеспечения кибербезопасности стало создание Межведомственной комиссии Совета Безопасности России по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры. Согласно Указу Президента Российской Федерации от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации». Комиссия осуществляет деятельность по формированию мер безопасности критически важной инфраструктуры и контроль за государственными органами, в чьи полномочия входят вопросы обеспечения технологической независимости объектов информационной инфраструктуры. Анализируя динамику показателей кибератак на отечественные информационные объекты нельзя не отметить важность деятельности вышеуказанного специального органа государственной власти, который на постоянной основе осуществляет прогнозирование, выявление и оценку внутренних и внешних рисков и угроз, влияющих на национальную безопасность в области развития и совершенствования информационных технологий.

Таким образом, обеспечение технологического суверенитета позволит гарантировать национальную безопасность Российской Федерации, тем самым создавая условия для противодействия: внутренним и внешним информационным угрозам при использовании цифровых технологий; развивающимся деструктивным процессам, направленным на информационное пространство Российской Федерации, нарушение прав и свобод граждан, безопасности общества и государства, а также задачами обеспечения социально-экономического развития страны и отечественных цифровых технологий, технологического суверенитета Российской Федерации.

Библиография

1. Терещенко Д.В. Цифровая трансформация: актуальные задачи // Таможня. 2022. № 5 (464). С. 9-10.
2. Путин призвал обеспечить технологический суверенитет России // РИА Новости. URL: <https://ria.ru/20230208/putin-1850583456.html> (дата обращения: 11.05.2023).
3. В. Матвиенко: На достижение технологического суверенитета в критически важных отраслях должны быть направлены все силы государства, науки и бизнеса // Совет Федерации. URL: http://council.gov.ru/events/main_themes/139867/ (дата обращения: 11.05.2023).
4. Касенова М.Б. Идентификация лиц в Интернете и киберпространство социальных сетей // Юрист. 2014. № 6. С. 32.
5. Никонов В.А., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) // Вестник Томского государственного университета Философия. Социология. Политология. 2021. № 60. С. 208.
6. Валеев А.Х. Борьба с проявлением экстремизма в сети Интернет // Бизнес в законе. 2011. № 6. С. 125.
7. Бачило И.Л. Информационное право: основы практической информатики. М., 2001. С. 286.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться [здесь](#).

Представленная на рецензирование научная статья на тему: «Технологический суверенитет как основа национальной безопасности Российской Федерации» представляет собой актуальное исследование важной проблемы национальной безопасности российского государства и общества. В рецензируемой статье авторами определена цель исследования и его задачи, обоснована актуальность. В частности, авторами подчеркивается, что усиление давления со стороны зарубежных хакерских группировок, увеличение масштаба компьютерных атак на российскую инфраструктуру разработчиков программ и оборудования должно способствовать актуализации достижения технологического суверенитета России и, соответственно, технического регулирования объектов в информационном пространстве и мер оперативного реагирования на вопросы организационного характера для обеспечения технологического суверенитета России и оптимизации управления технологическими и производственными процессами объектов критической информационной инфраструктуры. В этой связи, особенно важным представляется принцип реализации политики

технологического суверенитета в сфере информационно-коммуникационных технологий в целях обеспечения информационной безопасности.

Предметом исследования в рецензируемой статье выступила проблема технологического суверенитета Российской Федерации в новых геополитических условиях. Сделан акцент на кардинальное изменение государственной политики в сфере обеспечения информационной безопасности и необходимости разработки и принятия новых правовых решений. Авторское внимание уделено основным положениям проекта федерального закона «О технологической политике в Российской Федерации». Разработаны и предложены рекомендации. В частности, ввести специальные правовые режимы, которые позволят исключать отдельные аспекты из общего регулирования для ускорения разработки технологий и обеспечения долгосрочных изменений в этом направлении. Тем самым, законопроект поможет улучшить взаимодействие между представителями науки и промышленности и создаст основу для более успешной реализации инвестиционных проектов в области научных разработок, исследований и научно-исследовательских и опытно-конструкторских работ.

Статья отличается своей методологической базой и использованными источниками. В частности, анализ источниковой базы исследования показал, что при подготовке рецензируемой статьи было использовано достаточное скромное количество научных работ (всего 7 позиций) разных лет. Некоторые из них – десяти или даже двадцатилетней давности. Как мы понимаем, статья в большей степени направлена на использование документов концептуального, стратегического характера и отдельные федеральные законы, их проекты. Однако, авторам все же удалось найти место для анализа теоретической базы исследования и представить авторское понимание, например, дефиниции «технологический суверенитет» и обосновать его.

Статья логична. Статья написана хорошим языком и способна вызвать читательский интерес.

Таким образом, исходя из вышеизложенного, считаем, что рецензируемая научная статья на тему: «Технологический суверенитет как основа национальной безопасности Российской Федерации» соответствует необходимым требованиям, предъявляемым к такому виду научных работ и ее можно рекомендовать к опубликованию в искомом научном журнале.