

ПРАВОВОЕ СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА

Э.Д. Гаврилова, студент
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-12-1-176-178

Аннотация. Автор ставит вопрос о выработке концепции информационного суверенитета, которая учитывает средства и мероприятия информационной политики, конкретизацию механизмов юридической ответственности органов публичной власти в информационной сфере, мониторинг защищенности ресурсов, формирование механизмов ликвидации последствия компьютерных атак. Проанализированы внесенные в 2020 году поправки к Конституции РФ, соответствующие документы стратегического планирования и подзаконные акты.

Ключевые слова: информационные технологии, информационный суверенитет, информационные сети, национальная информационная инфраструктура, обеспечение информационной безопасности.

В условиях активного развития информационных технологий и становления цифрового общества одной из основных национальных целей и задач Российской Федерации является обеспечение независимости и устойчивого положения отечественных информационных сетей на международной арене и обеспечение активного развития государства в сфере информационной безопасности. Сегодня многие государства так или иначе будут зависимы от поставщиков ИТ технологий, что способствует возникновению новых угроз: утечка стратегически значимой для реализации государственной политики информации и персональных данных пользователей информационной сети.

В теории государства и права одной из основных категорий является понятие суверенитета как способности государства обеспечивать свою независимость и верховенство во внутренней и внешней политике. Ввиду появления новых и усиления прежних угроз концепция суверенитета государства расширяется: получает развитие такая концепция, как информационный суверенитет.

На настоящий момент пунктом «м» ч. 1 ст. 71 Конституции РФ предусмотрено отнесение вопроса обеспечения безопасности субъектов правового регулирования при применении информационных технологий, обороте цифровых данных к ис-

ключительному ведению РФ. Указанный предмет ведения нашел отражение в тексте Конституции РФ в 2020 году в связи с обострившейся международной обстановкой и необходимостью обеспечить информационную безопасность РФ и независимость в вопросах производства. На наш взгляд, данное дополнение способствовало определению информационного суверенитета как способности государства независимо и самостоятельно осуществлять регулирование в информационной сфере и обеспечить безопасность, в том числе, в цифровом пространстве, создавая собственные линии разработок ИТ-технологий и укрепляя свое положение на конкурентном рынке.

Отметим, что аналогичное понимание информационного суверенитета было представлено и в юридической литературе: так, например, указывается на независимое осуществление государством информационной политики посредством кадровых, финансовых, технических и иных ресурсов, имеющихся у государства организационно-правовых механизмов [1, с. 16]. Думается, что обеспечение информационного суверенитета требует использования комплекса организационно-правовых средств и методов, которые должны найти отражение в отдельном документе, например, Концепции развития информационного суверенитета.

Отметим, что проблемы обеспечения информационного суверенитета были отражены в Стратегии национальной безопасности, утвержденной Указом Президента РФ от 02.07.2021 г. № 400 [2]: например, относится проблема ликвидации последствий компьютерных атак, устроенных с целью подрыва безопасности отечественных информационных сетей, риски совершения террористических актов на объекты информационной инфраструктуры. Вместе с тем, Указом Президента РФ от 01.05.2022 № 250 (далее – Указ № 250) предусмотрены организационные меры по обеспечению информационной безопасности [3]. Примечательно, что было закреплено положение о персональной ответственности руководителя уполномоченного федерального органа за обеспечение информационной безопасности. Вместе с тем, необходима конкретизация. Следует согласиться с необходимостью существования механизмов реализации юридической ответственности органов публичной власти: формулировки «несут ответственность» без должных механизмов ее реализации, действительно, несут только декларативный характер [4, с. 52].

В Указе № 250 нашло отражение предоставление ФСБ России и ФТЭК России

Библиографический список

1. Нарутто С.В, Колмаков С.Ю., Япрынцева И.М Информационный суверенитет: конституционно-правовые основы в условиях развития цифрового государства // Образование и право. – 2022. – №10. – С. 15-22.
2. Указ Президента РФ от 02.07.2021 № 400 // СПС «КонсультантПлюс».
3. Указ Президента РФ от 01.05.2022 № 250 // СПС «КонсультантПлюс».
4. Малько А.В., Липинский Д.А., Маркунин Р.С. Роль юридической ответственности в реализации принципа единства публичной власти в Российской Федерации // Правоприменение. – 2021. – Т. 5. – № 4. – С. 43-54.
5. Приказ ФСБ России от 11 мая 2023 г. № 213 // Информационно-правовой портал «Гарант.Ру».

доступа к информационным ресурсам, которые принадлежат органам (организациям) или используются ими, для реализации мониторинга защищенности информационных ресурсов. Сущность и порядок данной меры по укреплению информационного суверенитета раскрыты в Приказе ФСБ России от 11 мая 2023 г. № 213 [5]. Установлена обязанность системы исполнительной власти, а также государственных фондов, корпораций компаний, субъектов критической информационной инфраструктуры предоставлять сведения о доменных именах и внешних сетевых адресах информресурсов. Думается, подобный мониторинг осуществляется для того, чтобы оценить способности соответствующих ресурсов противостоять угрозам информационной безопасности и ликвидировать последствия компьютерных атак.

Таким образом, необходимо выработать концепцию информационного суверенитета, учитывающую средства и мероприятия информационной политики, конкретизацию ответственности органов публичной власти в информационной сфере, формирование механизмов ликвидации последствий компьютерных атак.

LEGAL IMPROVEMENT OF INFORMATION SOVEREIGNTY

E.D. Gavrilova, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *The author studies the concept of information sovereignty, measures of information policy, responsibility of public authorities in the information sphere, monitoring the security of resources, the formation of mechanisms to eliminate the consequences of computer attacks. The amendments to Russian Constitution, relevant strategic planning documents and by-laws introduced in 2020 are analyzed.*

Keywords: *information technology, information sovereignty, information networks, national information infrastructure, information security.*