

ПРИНЦИПЫ ЗАЩИТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВА

Ю.С. Алексеева

Санкт-Петербургский университет технологий управления и экономики

Аннотация

В настоящей статье автор оценивает актуальность внедрения принципов цифрового суверенитета государства в отдельном нормативном правовом акте – Цифровом кодексе РФ, а также на основе анализа научных публикаций и нормативных актов, иных материалов выделяет ряд принципов защиты цифрового суверенитета государства.

Ключевые слова: цифровой суверенитет, цифровизация, информационная безопасность, принципы защиты, Цифровой кодекс.

Цифровизация в настоящее время пронизывает все сферы жизни человека и постепенно входит в плоскость государственного управления. Материалы для настоящей статьи, например, собраны автором с использованием цифровых технологий и Всемирной информационной компьютерной сети. Оплатить административный штраф либо получить выписку из государственного реестра, записаться на приём к врачу либо подать документы для получения лицензии предпринимателем - все эти действия сегодня можно осуществить лишь в один клик. Очевидно, что управление цифровыми технологиями на государственном уровне существенно влияет на кибермощность государства. Вместе с тем, актуальной становится проблема информационной безопасности, обеспечения цифрового суверенитета государства в период цифровой трансформации отношений между человеком, бизнесом и государством.

Традиционно категория «суверенитет» рассматривается как высшая власть в процессе принятия решений государством. По мнению Е.Зиновьевой и Б. Яцзе, эта же трактовка применима и к анализу цифрового суверенитета современных государств [1]. В свою очередь, легальная дефиниция понятия «цифровой суверенитет», несмотря на большое количество концепций, поддерживающих и не поддерживающих идею цифрового сегментированного суверенитета государства [2], до настоящего времени отсутствует. Единого акта, который бы унифицировал разрозненные подходы к правовому регулированию электронного документооборота, облачных технологий, искусственного интеллекта и других элементов информационного пространства до настоящего времени также не разработано. Хотя стремительное изменение общества в эпоху развития научно-информационных технологий определяет Стратегию развития информационного общества в Российской Федерации на 2017-2030 годы. Как следствие, существует необходимость изменения принципов правового регулирования сложившихся отношений и формирования принципов защиты цифрового суверенитета государства. Противопоставление цифрового

суверенитета цифровой диктатуре стало темой одной из панельных дискуссий Петербургского международного экономического форума 15 июня 2023 года [3]. О Концепции Цифрового кодекса как унифицированного нормативного правового акта ведутся дискуссии с 2017 года [4]. Отметим, что несколько дней назад Минцифры РФ представили проект концепции Цифрового кодекса РФ [5], который призван обеспечить цифровой суверенитет государства. Все участники дискуссии об информационной безопасности государства безусловно утверждают, что необходимы основные начала, которые будут отражать содержание и перспективы обеспечения цифрового суверенитета, которые станут основой для защиты государства от внешних угроз. К таковым можно отнести следующие отраслевые принципы:

- *независимость и контроль государства над своими информационными ресурсами* - включает в себя развитие собственной информационной инфраструктуры, чтобы минимизировать зависимость от иностранных технологических компаний, а также установление нормативов, обеспечивающих государственный контроль над информационными системами на территории Российской Федерации. ;

- *обеспечение кибербезопасности*, то есть разработка и внедрение современных технологий защиты от кибератак и утечки персональных данных пользователей, подготовка соответствующих специалистов в данной отрасли, создание механизмов реагирования на возможные инциденты. По данным лаборатории цифровой криминалистики компании F.A.C.S.T., «количество атак программ-вымогателей за 9 месяцев 2023 года выросло на 75% по сравнению с аналогичным периодом 2022 года, а средняя сумма первоначального выкупа за расшифровку данных превысила 37 млн. рублей» [6]. Жертвами шифровальщиков чаще всего становились российские ритейлеры, производственные, строительные, туристические и страховые компании;

- *защита данных пользователей и конфиденциальности* – включает в себя усовершенствование системы сбора и хранения данных в Сети, регулярную оценку рисков для данных и информационных систем и принятие мер по их минимизации, регулярное законодотворчество в этой сфере. По данным Центра технологий кибербезопасности ГК «Солар», в 2023 году, основной киберугрозой для российского бизнеса стали ежемесячные утечки конфиденциальной информации, что привело к огромным финансовым издержкам и репутационным потерям [7];

- *государственная поддержка национальных инновационных проектов в сфере инновационных технологий* – предоставление финансовой поддержки инновационным проектам через государственные гранты, субсидирование, льготное налогообложение, кредитование, инвестиции в стартапы и венчурные фонды, создание инновационных центров и парков, государственные заказы на инновационный продукт. Указанные меры стимулируют повышение конкурентноспособности государства и обеспечение его кибермощности;

- развитие национальных цифровых платформ для обмена информацией и предоставления государственных услуг, государственная поддержка отечественных информационно-технологических компаний;

- повышение цифровой грамотности населения, обучение правилам цифровой гигиены – проведение обучающих семинаров, тренингов, создание образовательной среды для разных возрастных категорий. По данным экспертного центра безопасности Positive Technologies, цифровая гигиена пользователей Сети Интернет состоит в том, чтобы не переходить по сомнительным ссылкам, не открывать файлы, полученные из недостоверных источников, не устанавливать приложения из неофициальных источников, установить на смартфон антивирусное программное обеспечение, постоянно поддерживать актуальную версию операционной системы и приложений на устройстве [8]. Указанные и другие инструменты обеспечивают стабильность цифровой коммуникации между пользователями и информационной безопасности;

- сотрудничество с другими государствами в борьбе с киберугрозами и киберпреступностью, разработка унифицированных межгосударственных стандартов в сфере информационных технологий, участие в международных договорах по обеспечению информационной безопасности – Россия уделяет большое внимание дипломатическим усилиям и внешнеполитическим инициативам в области цифрового суверенитета, а также делает акцент на обеспечении международной информационной безопасности.

Следует отметить, что Министерством цифрового развития республики Кыргызстан одним из первых в СНГ разработан проект Цифрового кодекса, который правительство республики вынесло на общественное обсуждение в августе 2023 года [9]. Ст. 2 указанного законопроекта выделяет общеправовые принципы (справедливости, определенности, участия), целевые принципы (технологической нейтральности, контентной нейтральности, устойчивого развития, открытости, подотчетности) и отраслевые принципы регулирования отношений в цифровой среде. Однако, в указанном законопроекте не конкретизированы принципы защиты цифрового суверенитета государства. Очевидно, проблема защиты цифрового суверенитета требует разрешения на государственном и межгосударственном уровне.

Таким образом, защита цифрового суверенитета государства требует комплексного подхода, который будет включать в себя независимость и контроль, обеспечение кибербезопасности, защиту персональных данных пользователей, защиту конфиденциальности, развитие национальных информационных ресурсов и дипломатические отношения. Эти принципы позволяют обеспечить государству свою цифровую независимость и безопасность в современном информационном пространстве.

Список использованных источников:

1. Зиновьева, Е. Практика цифрового суверенитета в России и КНР / Е. Зиновьева, Б.Яцзе // Официальный сайт Российского Совета по Международным делам. – 2023. – 29 мая. – <https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/> (дата обращения – 18.10.2023).
2. Мартиросян, А. Реалии цифрового суверенитета в современном мире / А. Мартиросян // Международная жизнь. – 2021. – № 3. – <https://interaffairs.ru/jauthor/material/2483> (дата обращения – 18.10.2023).
3. В России нужен закон о цифровом суверенитете – Захарова // Официальный сайт Российского агентства правовой и судебной информации. – 2023. – 15 июня. https://rapsinews.ru/digital_law_news/20230615/309000798.html (дата обращения – 18.10.2023).
4. В университете имени О.Е. Кутафина (МГЮА) обсудили перспективы принятия Цифрового кодекса Российской Федерации // Официальный сайт Московского государственного юридического университета имени О.Е. Кутафина (МГЮА). – 2023. – 18 сентября. – <https://msal.ru/news/v-universitete-imeni-o-e-kutafina-mgyua-obsudili-perspektivy-prinyatiya-tsifrovogo-kodeksa-rossiysko/> (дата обращения – 18.10.2023).
5. Турчак: законодательство РФ в области цифры объединят в единый Цифровой кодекс // Официальный сайт газеты «Известия». – 2023. – 14 октября. – <https://iz.ru/1589434/2023-10-14/turchak-zaiavil-o-sozdanii-v-rf-edinogo-tcifrovogo-kodeksa> (дата обращения – 18.10.2023).
6. Количество кибердиверсий в России за год выросло на 140% // Официальный сайт TADVISER. Государство. Бизнес. Технологии. – 2023. – 20 октября. – <https://www.tadviser.ru/index.php/> (дата обращения - 20.10.2023).
7. Средний ущерб от одной утечки информации составил 5,5 млн рублей // Официальный сайт TADVISER. Государство. Бизнес. Технологии. – 2023. – 05 октября. – <https://www.tadviser.ru/index.php> (дата обращения – 18.10.2023).
8. Россиянам перечислили основные способы защиты смартфонов от слежки. // Официальный сайт новостного портала Lenta.Ru. – 2023. – 01 июня. – <https://m.lenta.ru/news/2023/06/01/positive/> (дата обращения – 18.10.2023).
9. Петров, А. В Кыргызстане разработали проект Цифрового кодекса / А. В. Петров // Официальный сайт Российской газеты. – 2023. – 02 августа. – <https://rg.ru/2023/08/02/kodeks-obsudiat-liudi.html> (дата обращения – 18.10.2023).