demonstrate that one of the objectives in the development of robotic network agents is the exertion of political influence and the promotion of ideological and value attitudes in the interests of certain political actors. The authors emphasize that the use of political bot technologies leads to a polarization of public sentiment and an increase in potential for conflict both in the virtual world and in offline political space. The ethical aspects of social networks' robotization, as well as the problems associated with identifying bots and minimizing the social and political risks of their expansion in the network environment, are studied. The authors conclude that a value-oriented approach to the development and implementation of innovative technologies is required, and that it is extremely important for professional communities, state institutions and civil society to draw attention to socio-political aspects of technological progress.
Keywords: *digital technologies, political communication, social networks, artificial intelligence, political bots, computational propaganda, information warfare*

КЛИМАШЕВСКАЯ Ольга Викторовна – кандидат политических наук, доцент Московского авиационного института (Национальный исследовательский университет) (125080, Россия, г. Москва, Волоколамское ш., 4; Klimawevskaya@yandex.ru)

ЦИФРОВАЯ МОДЕРНИЗАЦИЯ РОССИЙСКОГО ГОСУДАРСТВА И ОБЩЕСТВА: ПЛЮСЫ, ВЫЗОВЫ И РИСКИ

Аннотация. *В статье раскрываются актуальные вопросы государственной политики в области цифровой модернизации. Автор анализирует грядущие изменения через рассмотрение экспертного мнения вице-премьера России, изучает нормативно-правовые акты, попавшие под удар нарастающего вектора в сфере информационных технологий и цифровизации. В статье также показано отношение зарубежных стран к данному направлению.*
Ключевые слова: *цифровизация, трансформация, модернизация, информационное общество, цифровой кейс, электронный паспорт, единая база данных*

На сегодняшний день актуальными являются рекомендации для развития цифровых государств, которые подготовили министры стран «Большой двадцатки» (*G*20) в 2019 г. В них делается акцент на необходимости комплексного развития цифровой, экономической, социальной сфер и государственного управления. По их мнению, странам нужно стремиться к тому, чтобы базы данных о гражданах были емкими и доступными, но сами системы при этом – хорошо защищенными от несанкционированного доступа. Генеральный директор *SAP CIS* Наталия Парменова уверена, что «дальнейшее развитие цифровой экономики будет связано с переходом на новые формы взаимодействия между государством, бизнесом и гражданами – например, переход на электронные трудовые книжки, электронные больничные, расширение доступности телемедицины»[1].

В текущем контексте проводимой работы и преподнесения информации подавляющее большинство граждан России пребывают в состоянии полного доверия к реализуемой цифровой политике нашего государства и достаточно высокой ее поддержки.

Так, 12 сентября 2019 г. новостные ленты опубликовали важные сообщения

[1] https://plus.rbc.ru/news/5b88c8c67a8aa93fdffc3fbe?ruid=uUjlB1voBjM2XafZAwmKAg== (проверено 23.12.2019).

о том, что комитет Госдумы поддержал проект создания единого ресурса сведений о россиянах[1].

В государственной системе создается единая распределенная база данных на всех граждан России, где оператором будет Федеральная налоговая служба. В базу войдут сведения о гражданах, содержащиеся практически во всех государственных и муниципальных информационных ресурсах органов власти и органов управления государственными внебюджетными фондами. Ресурс будет содержать как базовые (фамилия, имя, отчество, дата и место рождения и смерти, пол, реквизиты записи актов гражданского состояния о рождении и смерти, СНИЛС, ИНН – пожизненные и посмертные номера граждан), так и дополнительные (семейное положение, родственные связи, состояние здоровья и иные) сведения о физическом лице.

«В единой базе данных будет аккумулироваться информация из ныне разрозненных реестров разных государственных структур – МВД, Минобороны, Минобрнауки, ФНС, Пенсионного фонда, Фонда ОМС и др. Подробный вариант перечня баз данных, которые будут входить в совокупную систему, рассмотрен в предыдущей статье [Климашевская 2019]. Пользоваться банком данных смогут органы власти всех уровней, органы управления внебюджетными фондами, такие как ОМС и прочие, а также избирательные комиссии. Кроме того, доступ к ней будет у многофункциональных центров (МФЦ)», – указывает «Парламентская газета» в статье «Что будет знать единая база данных населения»[2].

Кроме того, Федеральная служба безопасности (ФСБ) и Служба внешней разведки смогут вносить в базу сведения, ранее не учтенные в иных государственных и муниципальных информационных ресурсах. Однако, несмотря на предполагающиеся возможности, законопроект о создании цифровых профилей граждан России подвергся критике со стороны той же самой Федеральной службы безопасности. По ее мнению, обработка данных в рамках единой инфраструктуры значительно повысит риск утечек информации, в т.ч. о судьях, прокурорах, следователях и сотрудниках силовых ведомств. Нахождение данных в рамках единой инфраструктуры значительно повышает возможности для их неправомерного сбора и распространения.

С одной стороны, внедрение данного законопроекта в жизнь граждан обусловлено желанием ускорить принятие решений органами власти, улучшить качество государственных услуг, особенно предоставляемых в электронной форме, противодействовать мошенничеству при получении льгот и уплате налогов. Также в тексте указано, что база будет обеспечивать избирательные права граждан и процесс военного призыва, что обеспечит удобство и безопасность многих сфер жизни россиян.

Но, с другой стороны, какой видится обратная сторона всех этих «удобств»? О чем необходимо помнить, задавая новый цифровой вектор в государстве?

Ответить на эти вопросы поможет анализ последних тенденций в цифровой среде российского государства.

В них поможет разобраться интервью от 9 сентября 2019 г. по цифровому развитию Максима Акимова, опубликованное в газете «Известия»[3].

В тексте освещены некоторые детали строящейся в России системы: «Первое: рост доверия, когда государство становится платформой, а граждане – клиен-

[1] https://ria.ru/20190912/1558601487.html (проверено 23.12.2019).

[2] https://www.pnp.ru/social/chto-budet-znat-edinaya-baza-dannykh-naseleniya.html (проверено 23.12.2019).

[3] https://iz.ru/919075/irina-tcyruleva-petr-marchenko/ot-pervogo-vzdokha-do-grobovoi-doski-vse-nado-otregulirovat (проверено 23.12.2019).

тами». С точки зрения информационного права цифровая платформа – совокупность технологий, которые обеспечивают создание системы цифрового взаимодействия управляющих органов и пользователей по обмену информацией и ценностями. Далее в своем интервью вице-премьер сообщает читателям: «В таком мире рост доверия между человеком и тем, кто предоставляет сервисы, – в данном случае государством, – критически важен. Люди не пойдут за тобой, если ты не будешь давать современный качественный продукт». Необходимо также отметить, что собранная информация будет храниться во Всемирной сети на постоянной основе, даже после смерти человека.

Таким образом, на высшем государственном уровне ставится задача формирования высокого уровня доверия российских граждан к обновленным структурам «цифровой власти».

Знакомясь с поставленными задачами, изложенными в интервью, уместно сопоставить их с текстом ныне действующей Концепции формирования информационного общества в России от 28 мая 1999 г. № 32, где сказано: «На начальном этапе создания социально значимых информационно-коммуникационных систем и комплексов (в сферах трудоустройства, образования, здравоохранения, социального обеспечения и других) государство берет на себя основные расходы, но в дальнейшем уходит с рынка»[1].

Таким образом, после возможного «ухода государства с рынка» вся информация о гражданах России может быть передана владельцам коммуникационных систем и баз данных, в т.ч. и зарубежным. В случае если правительство, как и запланировано, передаст свои конституционные полномочия собственникам систем, то соответствующие коммерческие, наднациональные структуры уже не будут иметь никаких конституционных обязанностей перед гражданами России, т.к. цель любой коммерческой структуры – это не обеспечение конституционных прав граждан, а в первую очередь извлечение прибыли. Данные риски необходимо принимать во внимание, и не преуменьшать последствия возможного развития событий.

Затем по тексту интервью следует еще одно любопытное утверждение: «Уже есть понимание, как технологически сделать гораздо более сложную вещь – построить управление государством на цифровых кейсах». Кейс – это пошаговое описание способа реализации проекта со всеми подробностями до конечной цели с учетом возможных трудностей. Например, какой режим работы социального учреждения (например, детского сада) лучше организовать, исходя из анализа маршрутов родителей на работу в конкретном микрорайоне путем сбора данных об их перемещениях; какова наиболее удобная модель работы; кто, когда и по какому маршруту ведет ребенка в садик, а потом забирает.

Данный шаг в применении цифровых кейсов – это проявление заботы об институте семьи, о родителях и их детях или развитие кейсовой системы, которое грозит тотальным отслеживанием всех передвижений россиян? На текущий момент поставленный вопрос – это повод задуматься о целесообразности таких мер в рамках проводимой цифровой политики, о степени готовности россиян к высокой прозрачности жизни, ограничению свободы передвижения, доступу к личной и семейной информации.

Крайне актуальным остается вопрос о внедрении «электронного паспорта». В перспективе в паспорте будет два компонента: карта с чипом и приложение на мобильном устройстве.

В цифровом обществе идет полемика о том, что «приложение на мобильном устройстве» в качестве удостоверения личности – технология весьма небезопас-

[1] http://www.iis.ru/library/riss/ (проверено 23.12.2019).

ная. Практически все эти устройства выпускаются нашими зарубежными партнерами и работают на их программном обеспечении. Ко всему прочему сотовые операторы предложили дополнительно внедрить в электронные паспорта систему *Mobile ID*. Об этом сообщил «Коммерсантъ» в статье «Сотовые операторы заглянули в электронный паспорт»[1]. Эта технология может использоваться абонентом в любой точке России, где доступна сотовая связь, в т.ч. на устройствах, не являющихся смартфонами. Такая система может быть как встроенной в мобильное приложение электронного паспорта, так и самостоятельным способом удаленной идентификации гражданина через *sim*-карты, в т.ч. для абонентов, не имеющих смартфонов.

Необходимо подвести итоги сказанному выше.

Во-первых, в результате принятия закона о создании единого федерального информационного ресурса на всех граждан России произойдет полная отмена ст. 23 Конституции РФ («Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну... на тайну переписки... и иных сообщений»), а также ч. 1 ст. 24 Конституции РФ («Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются») и целого ряда других статей Основного закона страны. Под угрозу ставятся такие понятия, как приватность и конфиденциальность. Граждане становятся «прозрачными» для операторов, а также собственников единой системы данных.

Во-вторых, создание единой базы противоречит и федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных». Согласно ч. 3 ст. 5 ФЗ № 152, «не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой». Принятие закона о едином федеральном ресурсе также вступает в противоречие с позицией государственно-правового управления Президента РФ. Считаются «недопустимыми любые формы принуждения граждан к использованию электронных идентификаторов, автоматизированных средств сбора, обработки и учета персональных данных и личной конфиденциальной информации».

Зарубежный опыт демонстрирует отказ развитых стран от создания единых распределенных баз данных. В Великобритании, Германии и Франции законодательно запрещено создание единого банка персональных данных на всех граждан страны. Парламенты и высшие конституционные органы этих стран расценили попытки построения подобной системы как покушение на основополагающие права и свободы граждан. Соответственно, создание единой распределенной базы данных на всех граждан России создает также реальную угрозу национальной безопасности государства и каждого гражданина.

В-третьих, необходимо помнить о проблемах кибербезопасности. В частности, в п. 17 Доктрины информационной безопасности РФ (утв. указом Президента РФ от 05.12.2016 № 646) говорится: «Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран». Однако вопрос, касающийся информационной безопасности, затрагивается экспертами в значительно меньшей степени, нежели вопросы «неоспоримых преимуществ» процесса цифровой модернизации.

В-четвертых, помимо глобального риска, существует элементарный челове-

[1] https://www.kommersant.ru/doc/4073784?from=main_3 (проверено 23.12.2019).

ческий фактор. Достаточно одного непорядочного системного администратора, и все данные могут попасть к геополитическим противникам России. Пока никто не задумывается, что фактически появляется новый класс управленцев – операторы-специалисты в области цифровых технологий, которые не только будут обладать абсолютной властью над оцифрованным населением, но от них, операторов, будут в полной зависимости и представители власти – государственные служащие, депутаты, судьи и другие руководители всех уровней. Сейчас активно происходит продвижение цифровых инициатив и коммерческого сектора *IT*-технологий, что впоследствии может привести к потере определенного объема власти. С каждым «цифровым шагом» наличие государства в данном процессе будет становиться все меньшим и меньшим. В глобальном смысле впоследствии могут появиться новые, наднациональные политические институты.

Таким образом, если не учитывать существующие выводы-риски, представленные выше, необыкновенно усиливается натиск на права и свободы человека, а также на суверенитет Российского государства.

Список литературы

Климашевская О.В. 2019. Проблемы реализации государственной политики РФ в области построения цифрового общества. – *Власть*. Т. 27. № 1. С. 82-86.

KLIMASHEVSKAYA Olga Viktorovna, Cand.Sci. (Pol.Sci.), Associate Professor at the Moscow Aviation Institute (National Research University) (4 Volokolamskoe Highway, Moscow, Russia, 125080; Klimawevskaya@yandex.ru)

DIGITAL MODERNIZATION OF THE RUSSIAN STATE AND SOCIETY: POSITIVE ASPECTS, CHALLENGES AND RISKS

Abstract. *The article reveals current issues of state policy in the field of digital modernization. The author analyzes upcoming changes through consideration of the expert opinion of the current Deputy Prime Minister of Russia and studies legal acts that have come under the blow of the growing vector in the field of information technology and digitalization. The article shows the attitude of foreign countries to this direction.*

Keywords*: digitalization, transformation, modernization, information society, digital case, electronic passport, single database*