А.Г. Дейнеко,
кандидат юридических наук,
профессор НИУ «Высшая школа экономики»
e-mail: adeineko@hse.ru

РЕАЛИЗАЦИЯ ОСНОВНЫХ ПУБЛИЧНО-ПОЛИТИЧЕСКИХ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА В КИБЕРПРОСТРАНСТВЕ

Аннотация. В статье проанализировано влияние органических свойств киберпространства, таких как трансграничность, децентрализованность и анонимность на реализацию основных публично-политических прав и свобод человека и гражданина. По результатам анализа ключевых угроз для реализации публично-политических прав личности будут намечены системные подходы к обеспечению их реализации и защиты в условиях киберпространства.

Ключевые слова: права человека, Интернет, киберпространство, анонимность, трансграничность, электронная демократия, искусственный интеллект, конституционное право, информационное право

A.G. Deineko

REALIZATION OF FUNDAMENTAL POLITICAL HUMAN RIGHTS AND FREEDOMS IN CYBERSPACE

Abstract: The paper will analyze the impact of the organic properties of cyberspace, such as cross-bordering, decentralization and anonymity on the implementation of the basic political Human Rights and Freedoms. Based on the results of the analysis of key threats to the realization of political rights, systematic approaches to ensuring their protection in cyberspace will be outlined.

***Keywords*:** Human Rights, Internet, Cyberspace, anonymity, cross-border, digital democracy, artificial intelligence, constitutional law, information law

Представляется, что актуальность вопроса о реализации основных прав и свобод личности в киберпространстве не нуждается в дополнительном обосновании. В ходе VI Международной научно-практической конференции «Бачиловские чтения» тезис о высокой степени влияния процессов цифровизации на общественные отношения прозвучал в выступлениях большинства докладчиков. Если сконцентрировать наше внимание на публично-политических правах, то прежде всего, следует констатировать, что, несмотря на громкие предсказания исследователей о наступлении в XXI

веке «третьей великой эпохи демократии» [1] (вслед за «первой эпохой» прямой демократии Древнего Рима и «второй эпохой» развитого парламентаризма XVII – XX вв.) или о переходе от представительной демократии индустриального общества к «партисипативной» демократии прямого участия, характерной для информационного общества[2], качественных изменений взаимоотношений власти и общества пока не наблюдается. Так, по результатам социологических исследований жители стран Юго-Восточной Азии и Ближнего Востока нередко оценивают свои страны, как более демократичные в сравнении с жителями стран Западной Европы и США[3]. Кроме того, само наличие подобных прогнозов и исследований в западных общественных науках в последние десятилетия свидетельствует о неудовлетворённости текущим состоянием демократических институтов.

В публично-политической сфере сохраняется тренд на цифровизацию существующих механизмов государственного управления и избирательного процесса[4], в документах стратегического развития нашей страны упоминается о необходимости развития механизмов электронной демократии[5], однако пока мы наблюдаем не революционный, а эволюционный путь развития. По мнению *Т.А. Васильевой*, это обусловлено тем, что представительные учреждения опираются на традиции и очень инертны в отношении любых изменений: их организационная структура и правила процедуры сохраняют стабильность в течение длительного времени[6].

Одной из ярких иллюстраций столкновения технологий киберпространства с механизмами традиционной представительной

[1] Такой прогноз в 1985 г. сделал американский медиаменеджер *Л. Гроссманн*. См.: *Grossmann L.K.* The Electronic Republic: Reshaping Democracy in the Information Age – N.Y., 1985.

[2] Автор этого прогноза – японский социолог *Е. Масуда*. См.: *Masuda I.* The Information Society as Post-Industrial Society – Washington: World Future Society, 1981.

[3] Так, по результатам опроса фонда «*Alliance of Democracies*» 2022 г. на вопрос «Является ли ваша страна демократической?» положительно ответили 83% жителей Китая, 77% жителей Вьетнама и 70% жителей Индии. В Германии, Италии и США эти показатели составили соответственно, 63%, 53% и 49%, в России – 46%.

[4] Одной из первых в нашей стране об этом писала И.Л. Бачило. См.: *Бачило И.Л.* Государство и право XXI в. Реальное и виртуальное. М.: Юркомпани, 2013.

[5] см. подп. «ж» п. 40 Стратегии развития информационного общества в РФ на 2017–2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. № 203) // СПС «Консультант Плюс».

[6] *Васильева Т.А.* Парламент online: проблемы функционирования // Конституционализм: универсальное и национальные измерения: монография / Под ред. Т.А. Васильевой, Н.В. Варламовой. М.: ИГП РАН, 2022. С. 142-144.

демократии стало появление в 2022 г. в Дании «антиполитической» Синтетической партии (*Det Syntetiske Parti*), управляемой при помощи алгоритма искусственного интеллекта[7]. В основе данного проекта лежит идея о том, что число избирателей, не представленных в датском парламенте, составляет около 20%, и для успешного результата на выборах необходимо составить гибридную программу, отвечающую их ожиданиям. Для этого алгоритм проанализировал программы партий, не прошедших в парламент Дании за последние 50 лет, отзывы соперников и избирателей на них. «Лидер» Синтетической партии по имени Ларс воплощен в киберпространстве в виде чат-бота, отвечающего на вопросы избирателей, однако среди его программных заявлений легко обнаружить и прямые логические противоречия[8]. Но даже такое сходство чат-бота со многими современными политиками вряд ли позволит ему присутствовать в законодательном органе и принимать участие в правотворчестве.

Современные исследователи «цифровой» или «облачной» демократии, как правило, концентрируют свой взгляд на проблемах обеспечения надежности информационных систем и технологий, обеспечивающих учет избирателей и подсчет отданных ими голосов. Стоит отметить, что отечественная ГАС «Выборы» с момента своего создания в 1995 г.[9] прошла впечатляющий путь развития от функции пассивного учета вводимых результатов подсчета бюллетеней до функций по обеспечению дистанционного электронного голосования, и в недалеком будущем – актуализации списков избирателей с использованием данных органов ЗАГС, МВД России и пр.[10]

---

[7] Det Syntetiske Parti [Электронный ресурс] // URL: https://detsyntetiskeparti.wordpress.com (дата обращения: 01.09.2023 г.).

[8] This Danish Political Party is Led by an AI [Электронный ресурс] // URL: https://vice.com/en/article/jgpb3p/this-danish-political-party-is-led-by-an-ai ((дата обращения: 01.09.2023 г.).

[9] Указ Президента Российской Федерации от 18 августа 1995 г. № 861 (ред. от 18 декабря 2018 г.) «Об обеспечении деятельности Государственной автоматизированной системы Российской Федерации «Выборы»; Федеральный закон от 10 января 2003 г. № 20-ФЗ (ред. от 14 марта 2022 г.) «О Государственной автоматизированной системе Российской Федерации «Выборы» // СПС «Консультант Плюс».

[10] В 2025 году в соответствии с Федеральным законом от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» должны завершиться работы по созданию такого регистра (ЕФИР), одной из функций которого является актуализация списков избирателей – *прим. авт.*

Отметим и высокую динамику правотворчества в исследуемой сфере. В 2019 г. в режиме правового эксперимента состоялось первое в нашей стране голосование на цифровых избирательных участках на выборах в Мосгордуму и дополнительных выборах депутатов Государственной Думы Федерального Собрания Российской Федерации, в 2020-2021 гг. этот эксперимент был продолжен на федеральных, региональных и муниципальных выборах, а уже в 2022 г. в законодательство о выборах были внесены изменения, сделавшие дистанционное электронное голосование одной из регулярных форм проведения выборов и референдумов[11].

В числе недостатков дистанционного электронного голосования отечественные исследователи традиционно указывают на невозможность достоверно установить факт отсутствия давления на избирателя в момент голосования[12], а также на невозможность присутствия наблюдателей на цифровых избирательных участках при подсчете голосов[13]. Отметим здесь и пласт проблем, связанных с обеспечением надлежащей идентификации субъектов правоотношений, происходящих в киберпространстве[14].

Впрочем, член ЦИК России *И.Б. Борисов* справедливо отмечает, что даже те страны, которые на протяжении 10-15 лет используют дистанционные формы голосования, регулярно подвергаются критике на различных международных площадках за недостаточную прозрачность применяемых цифровых технологий[15]. Так, в законодательстве ряда штатов в США до сих пор применяется крайне архаичная процедура проверки подписей избирателей, проголосовавших по почте. Попытки цифровизации этой процедуры при помощи технологии искусственного интеллекта привели

---

[11] Федеральный закон от 14 марта 2022 г. № 60-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «Консультант плюс».

[12] *Гриценко Е.В.* Обеспечение основных гарантий избирательных прав в условиях информатизации избирательного процесса // Конституционное и муниципальное право. 2020. № 5. С. 45.

[13] *Дзидзоев Р.М.* Конституционное право в информационном и цифровом пространстве России // Конституционное и муниципальное право. 2019. № 10. С. 22.

[14] Подробнее о проблеме идентификации – см.: *Наумов В.Б.* Институт идентификации в информационном праве: дисс. … докт. юрид. наук – М., 2021.

[15] *Борисов И.Б.* На пути к электронной демократии. Цифровые технологии в системе демократического воспроизводства властных институтов // Избирательное законодательство и практика. 2019. № 3. С. 3-10.

к росту числа случаев, когда подписи избирателей, которые изменились в силу возраста или состояния здоровья, были признаны недействительными[16].

На наш взгляд, вектор цифровой трансформации гражданского участия в управлении делами государства в ближайшие годы будет смещаться от дистанционного голосования избирателей к развитию механизмов общественного обсуждения в киберпространстве. В отдельных субъектах Российской Федерации широко распространены мобильные приложения (такие, как «Активный гражданин», «Добродел» и др.), позволяющие гражданам высказываться по различным инициативам органов исполнительной власти, а также направлять индивидуальные и коллективные петиции. В связи с этим представляется интересным предложение *О.А. Фомичевой* о дополнении системы обеспечения законодательной деятельности Государственной Думы Федерального Собрания Российской Федерации и сайтов представительных органов власти субъектов Российской Федерации функционалом по приёму комментариев пользователей к конкретным законопроектам[17].

Наряду с угрозами нарушения публично-политических прав граждан технического характера стоит отметить наличие в киберпространстве широкого круга угроз манипулятивного воздействия на граждан, действие которых не ограничивается периодом избирательных кампаний. Еще в 1987 г. член-корреспондент Афинской академии наук *С. Симитис* предупреждал: «обработка информации превращается в необходимый элемент долгосрочных стратегий манипулирования, направленных на формирование и корректировку поведения индивида»[18]. Принятые в 2020 г. рекомендации Комитета министров Совета Европы «О влиянии алгоритмических систем на соблюдение прав человека» называют в числе ключевых рисков применения

[16] Automatic Signature Verification Software Threatens to Disenfranchise U.S. Voters [Электронный ресурс] / URL: https://venturebeat.com/2020/10/25/automatic-signature-verification-software-threatens-todisenfranchise-u-s-voters (дата обращения: 01.09.2023 г.).

[17] *Фомичёва О.А.* Перспективы демократизации законотворческого процесса в Российской Федерации // Конституционализм: универсальное и национальные измерения: монография / под ред. *Т.А. Васильевой, Н.В. Варламовой* – М.: ИГП РАН, 2022. С. 162.

[18] *Simitis S.* Reviewing Privacy in Information Society // University of Pennsylvania Law Review. 1987. Vol. 135 (3). P. 710.

технологии искусственного интеллекта «рост возможностей для вторжения в частную жизнь и манипулирования» [19].

Одним из ярких примеров такого вторжения стала деятельность компании *Cambridge Analytica* в рамках агитационной кампании на выборах Президента США в 2016 г. По результатам трёхлетнего расследования Федеральной торговой комиссии США были установлены многочисленные нарушения конфиденциальности пользователей социальной сети *Facebook*[20]. В частности, было доказано, что *Cambridge Analytica* сформировала цифровые «политические» профили от 50 до 87 млн. пользователей без их согласия и подвергла их «микротаргетированной» политической рекламе в пользу одного из кандидатов[21]. Такие профили содержали десятки тысяч характеристик каждого пользователя, значимых для предвыборной агитации: отношение к легализации оружия, мигрантам, проблеме абортов, сексуальным меньшинствам и мн. др. Исходя из характеристик профиля алгоритмом *Cambridge Analytica* подбиралась политическая реклама, которая сможет произвести наиболее сильное впечатление на избирателя. Примечательно, что даже рекордный оборотный штраф в $5 млрд., который был наложен на *Facebook* по результатам расследования, не смог сдержать дальнейший рост капитализации этой компании[22].

В 2016 г. Специальный докладчик Совета ООН по правам человека по вопросу о поощрении и защите права на свободу мнений и их свободное выражение *Д. Кайе* в своём докладе возложил ответственность за реализацию публично-политических прав граждан как на частный сектор, владеющий цифровыми платформами, так и на государства, которые могут оказывать «избыточное давление на предмет ограничения выражения мнений, которые

[19] Рекомендации Комитета министров Совета Европы государствам-членам № CM/REC (2020)1 «О влиянии алгоритмических систем на соблюдение прав человека».

[20] Данная социальная сеть признана экстремистской и запрещена в России – *прим. авт.*

[21] см. например: *Cadwalladr C, Graham-Harrison E.* Revealed; a 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach [Электронный ресурс] / URL: https://theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (дата обращения: 01.09.2023 г.).

[22] см. например: Facebook оштрафовали в США на $5 млрд за работу с данными пользователей [Электронный ресурс] / URL: https://rbc.ru/technology_and_media/24/07/2019/5d386e939a79470f5ea67d3d (дата обращения: 01.09.2023 г.).

считаются экстремистскими или ненавистническими, враждебными или оскорбительными»[23]. На наш взгляд, основным источником угроз для публично-политических прав граждан в киберпространстве являются не органы государственной власти, а профессиональные пропагандисты и манипуляторы, которые пытаются влиять на общественный дискурс через социальные сети и распространяемые в цифровой форме средства массовой информации.

Вирусный характер распространения намеренно искажённой информации (*fake news*) не вызывает сомнений, поскольку информация такого рода распространяется в киберпространстве в 6 раз быстрее подлинных новостей, а вероятность её перепоста пользователями на 70 % выше[24]. Противодействовать распространению такой информации весьма сложно, поскольку объём размещаемого в киберпространстве контента давно превысил возможности человека по его восприятию и осмыслению, а алгоритмы искусственного интеллекта плохо справляются с задачей по выявлению публикаций, содержащих *fake news* или *hate speech*. Такие публикации имеют сложную и изменчивую языковую специфику, зачастую неподвластную машинному переводу и логическому анализу, поэтому цифровые платформы вынуждены нанимать и обучать модераторов, являющихся носителями языка и способных распознавать сарказм, скрытые призывы к насилию или дискриминации. Рекомендации по внедрению подобных практик содержатся в частности, в Руководящих принципах регулирования цифровых платформ, утверждённых ЮНЕСКО в 2023 году[25].

Таким образом, киберпространство само по себе не является фактором, оказывающим негативное или положительное влияние на реализацию

[23] пп. 1-3, 8, 85 Доклада Специального докладчика Совета ООН по правам человека по вопросу о поощрении и защите права на свободу мнений и их свободное выражение от 11 мая 2016 г. № A/HRC/32/38 [Электронный ресурс] // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/14/PDF/G1609514.pdf (дата обращения: 01.09.2023 г.).

[24] *Козловский Б.М.* Максимальный репост: Как соцсети заставляют нас верить фейковым новостям – М.: Альпина Паблишер, 2019. С. 26.

[25] п. 101 Руководящих принципов регулирования цифровых платформ: Многосторонний подход к обеспечению свободы выражения мнений и доступа к информации – ЮНЕСКО, 2023. [Электронный ресурс] // URL: https://unesdoc.unesco.org/ark:/48223/pf0000387385.locale=ru (дата обращения: 01.09.2023 г.).

публично-политических прав граждан. Использование потенциала цифровых технологий может повысить доступность избирательного процесса, точность подсчета голосов, информированность и вовлеченность граждан в политическую жизнь, но вместе с тем, способно создать новые угрозы для реализации конституционных прав. Рассмотрим те меры, которые принимает российский законодатель для минимизации таких угроз.

Во-первых, следует отметить меры, направленные на обеспечение цифрового суверенитета Российской Федерации, достижение которого является одной из стратегических целей Доктрины информационной безопасности нашей страны[26]. В 2018 г. вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»[27], установивший требования к уровню безопасности информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, внесённых в соответствующий реестр, а также сетей электросвязи, используемых для организации взаимодействия таких объектов. В 2019 г. в развитие положений указанного закона в информационное законодательство были внесены масштабные поправки, получившие в средствах массовой информации наименование «Закон о суверенном рунете»[28]. По оценкам специалистов, все крупные российские провайдеры к настоящему времени выполнили требования указанных законов, благодаря чему даже в условиях масштабных хакерских атак обеспечивается бесперебойная работа российского сегмента киберпространства[29].

---

[26] Подробнее об этом – см.: Информационное пространство: обеспечение информационной безопасности и право: сб. науч. трудов / под ред. *Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева* – М.: ИГП РАН, 2018; Динамика институтов информационной безопасности. Правовые проблемы: сб. науч.тр. / отв. ред. *Т.А. Полякова, В.Б. Наумов, Э.В Талапина* – М.: Канон Плюс, РООИ "Реабилитация", 2018.

[27] ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «Консультант Плюс».

[28] Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».

[29] см.: Суверенная сеть [Электронный ресурс] / URL: https://vedomosti.ru/importsubstitution/state_regulation/articles/2023/04/25/972408-cuverennaya-set (дата обращения: 01.09.2023 г.).

Во-вторых в 2021 г. по поручению Президента Российской Федерации *В.В. Путина* был разработан и принят Федеральный закон «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»[30], содержащий условия для введения в российскую юрисдикцию транснациональных компаний, владеющих цифровыми платформами. Аналогичные подходы к локализации IT-компаний, преследующие целью решение проблемы трансграничности киберпространства, можно встретить и в законодательстве зарубежных стран. Так, с 2018 г. в Германии вступил в силу Закон «О защите прав пользователей в социальных сетях»[31], согласно которому любая социальная сеть с аудиторией свыше 2 млн. пользователей должна открывать представительство в ФРГ и обеспечивать блокировку противоправного контента. Такие же требования, за исключением блокировки контента, предъявляет к крупным социальным сетям принятый в 2020 г. французский закон «О противодействии ненависти в Интернете»[32].

В-третьих, в целях борьбы с *fake news* в российское информационное законодательство в 2016 г. был введён новый субъект – новостной агрегатор, на который в частности, возложена обязанность не допускать сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественной значимой новостной информации под видом достоверных сообщений[33].

В-четвертых, для повышения прозрачности работы рекомендательных алгоритмов цифровых платформ в 2023 г. были приняты поправки к информационному законодательству, установившие для владельцев интернет-сайтов, информационных систем или программ для ЭВМ обязанность

[30] Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» // СПС «Консультант Плюс».

[31] Network Enforcement Act (*Netzdurchsetzunggesetz, NetzDG*) [Электронный ресурс] / URL: https://germanlawarchive.iuscomp.org/?p=1245 (дата обращения: 01.09.2023 г.).

[32] LOI № 2020-766 du 24 Juin 2020 *Visant à Lutter Contre Les Contenus Haineux Sur Internet*. [Электронный ресурс] / URL: https://legifrance.gouv.fr/loda/id/JORFTEXT000042031970/2021-10-27/ (дата обращения: 01.09.2023 г.).

[33] подп. 3 п. 1 ст. 10.4 Федерального закона от 27 июля 2006 г. № 149-ФЗ (ред. от 29 декабря 2022 г.) «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».

публикации документов, описывающих правила применения таких технологий[34]. Большинство крупных цифровых платформ, функционирующих в российском сегменте киберпространства, уже выполнили данное требование, разместив в открытом доступе соответствующие документы. Впрочем, многие из них характеризуются обтекаемыми формулировками, не позволяющими составить однозначное представление о характере данных, вычисляемых цифровой платформой.

На наш взгляд, дальнейшее развитие гарантий реализации публично-политических прав и свобод граждан должно привести к закреплению в российском законодательстве права граждан участвовать в политической жизни общества (в т.ч. осуществлять своё волеизъявление на выборах и референдумах) как цифровыми, так и нецифровыми способами. Кроме того, граждане должны быть защищены от цифрового профилирования в политических и иных целях, а также от информационно-психологического манипулирования, недостоверной информации (*fake news*) и проявлений ненависти (*hate speech*) в киберпространстве.

Для достижения этих целей необходимо не только дальнейшее совершенствование законодательства, но и принятие документов стратегического развития, устанавливающих общие принципы обеспечения прав человека в киберпространстве. *Т.Я. Хабриева* справедливо указывает на общую неэффективность законодательного регулирования отношений в киберпространстве в сравнении с иными способами, поскольку преобладание законодательных актов сокращает возможность законодателя оперативно реагировать на изменения, происходящие в предмете регулирования[35].

Подобные стратегические документы уже принимаются органами публичной власти применительно к отдельным направлениям развития

[34] ст. 10.2-2 Федерального закона от 27 июля 2006 г. № 149-ФЗ (ред. от 29 декабря 2022 г.) «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».

[35] *Хабриева Т.Я.* Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9 (261). С. 10.

цифровых технологий[36], а также хозяйствующими субъектами, преимущественно в сфере этического саморегулирования[37]. Сочетание указанных способов регулирования общественных отношений позволит создать сбалансированную систему, обеспечивающую защиту прав и свобод граждан, развитие российской IT-индустрии и отвечающую национальным интересам нашей страны.

Библиографический список

1. Бачило И.Л. Государство и право XXI в. Реальное и виртуальное. М.: Юркомпани, 2013.

2. Борисов И.Б. На пути к электронной демократии. Цифровые технологии в системе демократического воспроизводства властных институтов // Избирательное законодательство и практика. 2019. № 3. С. 3-10.

3. Васильева Т.А. Парламент online: проблемы функционирования // Конституционализм: универсальное и национальные измерения: монография / Под ред. Т.А. Васильевой, Н.В. Варламовой. М.: ИГП РАН, 2022. С. 142-144.

4. Гриценко Е.В. Обеспечение основных гарантий избирательных прав в условиях информатизации избирательного процесса // Конституционное и муниципальное право. 2020. № 5. С. 41-49.

5. Дзидзоев Р.М. Конституционное право в информационном и цифровом пространстве России // Конституционное и муниципальное право. 2019. № 10. С. 21-22.

6. Динамика институтов информационной безопасности. Правовые проблемы: сб. науч.тр. / отв. ред. *Т.А. Полякова, В.Б. Наумов, Э.В Талапина* – М.: Канон Плюс, РООИ "Реабилитация", 2018.

7. Информационное пространство: обеспечение информационной безопасности и право: сб. науч. трудов / под ред. *Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева* – М.: ИГП РАН, 2018.

8. Козловский Б.М. Максимальный репост: Как соцсети заставляют нас верить фейковым новостям – М.: Альпина Паблишер, 2019.

[36] см. например, Концепцию развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г. (утв. распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р) // СПС «Консультант Плюс».

[37] см. например, Национальный кодекс этики искусственного интеллекта [Электронный ресурс] / URL: https://a-ai.ru/wp-content/uploads/2021/10/Кодекс_этики_в_сфере_ИИ_финальный.pdf (дата обращения: 01.09.2023 г.).

9. Наумов В.Б. Институт идентификации в информационном праве: дисс. … докт. юрид. наук – М., 2021.

10. Фомичёва О.А. Перспективы демократизации законотворческого процесса в Российской Федерации // Конституционализм: универсальное и национальные измерения: монография / под ред. *Т.А. Васильевой, Н.В. Варламовой* – М.: ИГП РАН, 2022.

11. Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9 (261). С. 5-16.

12. Grossmann L.K. The Electronic Republic: Reshaping Democracy in the Information Age. N.Y., 1985.

13. Masuda I. The Information Society as Post-Industrial Society.Washington: World Future Society, 1981.

14. *Simitis S.* Reviewing Privacy in Information Society // University of Pennsylvania Law Review. 1987. Vol. 135 (3). Pp. 707-744.