Федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи

Васекин Артем Сергеевич

ЦИФРОВОЙ СУВЕРЕНИТЕТ ЛИЧНОСТИ: СОЦИОЛОГИЧЕСКИЙ АНАЛИЗ

Специальность: 5.4.4 Социальная структура,

социальные институты и процессы

Диссертация
на соискание ученой степени кандидата социологических наук

Научный руководитель:

Литвинцева Елена Ананьевна,
заведующий кафедрой организационного
проектирования систем управления ИГСУ РАНХиГС,
Почетный работник сферы образования Российской Федерации,
ученый секретарь Ученого совета ИГСУ РАНХиГС,
доктор социологических наук, доцент

Москва 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. В настоящее время проблема формирования цифрового суверенитета личности в контексте глобальных социальных изменений приобретает особое значение и выходит на передний план исследований в сфере гуманитарных наук. Этому способствует характер деятельности человека в современных условиях, предусматривающий значительную степень взаимодействий и взаимной зависимости в быстро развивающейся цифровой среде.

Процессы цифровизации, виртуализации и сетевизации значительно повышают открытость социальных институтов, воздействуют на адаптацию личности и социальных групп в цифровой среде, влияют на регулирование и управление информационными данными. Активно развивается сетевая инфраструктура, расширяется сфера онлайн услуг, виртуальные пространства, такие как социальные сети и онлайн-платформы, становятся основными местами общения и свободного выражения мнений. Серьезной трансформации подвергаются принципы коммуникативных процессов, в частности, изменение форматов и роли участников коммуникации[1], доступности информации и анонимизации пользователей т.п.

Процесс цифровизации легализовал информацию в качестве товара, в связи с чем в сферу такого товарообмена вовлекаются персональные данные и сведения о частной жизни граждан. Формирование цифровой экономики, в которую вовлекаются не только финансовые институты, но и все без исключения сферы общественной деятельности (здравоохранение, образование, социальное обеспечение и т.д.), приводит к значительному ускорению социально-экономических коммуникаций, глобализации производства, новым формам трудовой занятости и одновременно к несправедливости в распределении ресурсов, утрате социальной идентичности и зависимости от крупных технологических компаний.

[1] Кожевникова Л. В., Старовойтова И. Е. Виртуальная коммуникация в цифровой образовательной среде . Образование и право. 2024. №9. С.397

Возникает потенциальная опасность возникновения тотального интернет-контроля, когда происходит социальное и психологическое давление на интернет-пользователя, отмечаются факты «цифровой дискриминации» личности[1]. Многократно возрастают проблемы информационной безопасности, почвой для которой зачастую является специфика права собственности на информационные платформы и серверы, многие из которых принадлежат зарубежным компаниям. Подавляющая часть виртуальных инструментов и ресурсов, которые использует современный человек, представляет собой чужую собственность или является объектом исключительных прав транснациональных корпораций, что ведет к возможной утере (или передаче) персональных данных граждан не только непосредственным участникам правоотношений, но и третьим лицам.

Представляется, что недостаточная теоретическая проработанность различных элементов цифрового суверенитета личности может привести к таким практическим последствиям, как усиление цифрового неравенства, утрата личной автономии, увеличение рисков утечки персональных данных, вовлечение граждан в деструктивную деятельность, подрыв традиционных ценностей.

Таким образом, актуальность темы исследования обусловлена следующими обстоятельствами:

во-первых, воздействием глобальной цифровизации на идентичность и социальные отношения. Цифровой суверенитет личности включает в себя аспекты, касающиеся сохранения культурной и социальной идентичности в условиях цифровизации, что позволяет людям сохранять свою уникальность и защищать свои ценности в виртуальном пространстве.

во-вторых, необходимостью уменьшения цифрового неравенства и обеспечения равного доступа к цифровым технологиям и ресурсам. Цифровой

[1] Подопригора Л.М. Современные проявления цифровой дискриминации. Сборник научных трудов Конференции Российское общество и государство на современном этапе. Том Выпуск 2. Владимир, 2022. Стр.195

суверенитет предполагает создание условий для равного доступа к цифровым услугам и ресурсам, что способствует социальной справедливости и уменьшению разрыва между различными группами населения.

в-третьих, увеличением зависимости общества от цифровых технологий, что создает риски утраты контроля над персональными данными и личной информацией. В условиях, когда персональные данные становятся объектом коммерческой эксплуатации, цифровой суверенитет личности может выступить как механизм, позволяющий гражданам сохранять контроль над персональными данными и чувствительной информацией.

в-четвертых, необходимостью защиты прав личности в цифровом пространстве как ключевого аспекта социальных процессов, направленных на реализацию интересов пользователей и предотвращение злоупотреблений со стороны крупных технологических компаний. Цифровой суверенитет подразумевает создание социальных и этических норм, которые обеспечивают защиту прав граждан и способствует формированию ответственного отношения к персональным данным.

Таким образом, исследование цифрового суверенитета личности в контексте глобальных социальных изменений является важным шагом к пониманию и решению современных вызовов, связанных с цифровизацией и ее последствиями для общества.

Степень научной разработанности проблемы. Общий комплекс исследований по вопросам цифрового суверенитета личности можно разбить на пять групп работ.

Первую группу составляют работы, посвященные исследованию формирующейся цифровой реальности и формированию цифрового общества в социологическом аспекте. В ракурсе изучения цифровой реальности тема

анализировалась в работах В.И. Аршинова[1] , А.В Комаровой[2], Д. Коэна[3], Ю. Хабермаса[4] К. Шваба[5], М. Кастельса[6], С.А. Кравченко[7] и др. Коммуникативные процессы в цифровой реальности рассматривались в трудах М. Кастельса[8], А.В. Агеевой[9], С.В. Девятовой[10], А.Г. Капустиной[11] , Е.А. Лазининой[12] и др. Социально- политологические аспекты формирования цифровой реальности раскрываются в исследованиях П. Друкера[13], Б.Б.

[1] Аршинов В.И. Цифровая реальность в оптике постнеклассической парадигмы сложностности //Проектирование будущего. Проблемы цифровой реальности: труды 1-й Международной конференции (8-9 февраля 2018 г., Москва). - М., 2018. - С.147-151 [Электронный ресурс]. Режим доступа: http: //keldysh.ru/future/2018/22.pdf - (Дата обращения: 01.09.2022).

[2] Комарова А. В. Динамика информационно-коммуникационных процессов и их влияние на социокультурные институты // Верхневолжский филологический вестник. 2024. № 3 (38). С. 223–233. http://dx.doi.org/10.20323/2499-9679-2024-3-38-223. https://elibrary.ru/ZNLRQT

[3] Коэн Д., Шмидт Э. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств /Перевод с английского С.Филина. - М.: Издательство «Манн, Иванов и Фербер», 2013. - 368 с.

[4] Хабермас Ю. От картин мира к жизненному миру /Habermas J. Von den Weltbildern zur Lebenswelt. - М.: Идея-Пресс, 2011. - 128 с.

[5] Шваб К. Четвертая промышленная революция. - М.: Издательство «Эксмо», 2016. - 138 с. [Электронный ресурс]. Режим доступа: http: //ncrao.rsvpu.ru/sites/default/files/library/k._shvab_chetvertaya_promyshlennaya_revolyuciya_2016.pdf. - (Дата обращения: : 01.09.2022).

[6] Кастельс М. Информационная эпоха: экономика, общество и культура: Пер. с англ. под науч. ред. О.И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.

[7] Кравченко С.А. Социология риска и безопасности: учебник и практикум для вузов / С. А. Кравченко. — Москва : Издательство Юрайт, 2023. — 272 с.

[8] Кастелъс М. Власть коммуникации /Перевод с английского Н.М.Тылевич; предисловие к изданию 2013 года А.А.Архиповой; под научной редакцией А.И.Черных. 2-е издание, дополненное. - М.: Издательский дом Высшей школы экономики, 2017. - 591 с.

[9] Агеева А.В., Красноцветов Г.В. «Мягкая сила» в онлайн-пространстве: практический опыт применения технологий интернет-коммуникации //Власть. - 2020. - Том 28. - №2. - С.96-100.

[10] Девятова С.В., Казарян В.П. Многомерность проблемы коммуникации в цифровом обществе //Российский гуманитарный журнал. - 2020. - Том 9. -№3. - С.165-173.

[11] Капустина А.Г. Правовой статус субъектов информационно-коммуникативной деятельности в Интернете //Актуальные проблемы гуманитарных и естественных наук. - 2015. - №11-7. - С.43-46.

[12] Лазинина Е.В.Коммуникативные процессы в виртуальной реальности цифрового общества. Монография. Ставрополь, 2023 г. – 173 С

[13] Друкер П.Ф. Управление в обществе будущего /Перевод с английского и редакция Е.В.Трибушной. - М.: Издательство «Вильямс», 2007. - 306 с.

Славина[1], Ф. Хейлинга[2] и др. Понимание цифровой реальности как идентичной цифровому обществу изучены Т. Адорно, Д. Беллом[3], Дж. Нейсбитом[4], Э. Тоффлером[5], М. Хоркхаймером[6] и др. Прогностический (футуристический) подход к исследованию цифровой реальности был применен в работах А.В. Турчина[7], Ю.Н. Харари[8] и др. авторов. Технократический подход к анализу цифровой реальности нашел отражение в трудах В.И. Аршинова[9], Д.В. Кравцова[10] и др. Отметим также значение исследований Л.А. Василенко[11], которая исследует вопросы становления и развития цифрового общества.

---

[1] Славин Б. Когда цифровая демократия не работает //Ведомости. -12.11.2019. - №212. - С.7 [Электронный ресурс]. Режим доступа: http: //elib.fa.ru/art2019/bv2106.pdf. - (Дата обращения: 01.09.2022).

[2] Рождение коллективного разума. О новых законах сетевого социума и сетевой экономики и об их влиянии на поведение человека. Великая трансформация третьего тысячелетия /Ф.Хейлинг и др.; под редакцией Б.Б.Славина. - М.: URSS, 2013. - 285 с.

[3] Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования /Перевод с английского, под редакцией В.Л.Иноземцева. -М.: «Academia», 2004 (ОАО Можайский полиграфический комбинат). - 786 с.

[4] Нейсбит Дж. Мегатренды /Перевод с английского М.Б.Левина. -М.: АСТ: Ермак, 2003. - 380 с.

[5] Тоффлер Э. Третья волна /Переводчики: Барабанов С., Бурмистров К., Бурмистрова Л., Заритовская З., Комарова Е., Кротовская Н., Кулагина-Ярцева В., Микиша А., Москвина-Тарханова И., Руднева Е., Татаринова К., Хмелик Н. Научный редактор П.С.Гуревич. - М.: ООО «Фирма "Издательство АСТ"», 2004. - 261 с.

[6] Хоркхаймер М., Адорно Т. Культурная индустрия. Просвещение как способ обмана масс /Перевод с немецкого: Т.Зборовская. - М.: Ад Мар-гинем Пресс, 2016. - 103 с.

[7] Турчин А.В., Батин М.А. Футурология. XXI век: бессмертие или глобальная катастрофа? - М.: Бином. Лаборатория знаний, 2012. - 263 с.

[8] Харари Ю.Н. Homo Deus. Краткая история будущего. - М.: Синдбад, 2019. - 496 с.

[9] Аршинов В.И. Цифровая реальность в оптике постнеклассической парадигмы сложностности //Проектирование будущего. Проблемы цифровой реальности: труды 1-й Международной конференции (8-9 февраля 2018 г., Москва). - М., 2018. - С.147-151 [Электронный ресурс]. Режим доступа: http: //keldysh.ru/future/2018/22.pdf - (Дата обращения: 30.08.2022).

[10] Кравцов Д.В., Леонов Е.А. Разработка автоматизированной системы мониторинга информации в сети Интернет в целях борьбы с распространением идей терроризма и экстремизма. Наука и образование против террора - 2010: сборник работ участников Первого Открытого Конкурса «Наука и образование против террора - 2010». - М: МГТУ им. Баумана, 2011. - С.52-61.

[11] Василенко Л.А. Социология цифрового общества : монография / Л.А. Василенко, Н.Н. Мещерякова ; Томский политехнический университет. – Томск : Изд-во Томского политехнического университета, 2021.

Вторая группа работ раскрывает изменения, происходящие в социальных институтах под влиянием цифровых информационно-коммуникационных технологий (ИКТ). Выделим теоретические подходы к пониманию «электронного (или «цифрового») государства» (Р.Ф. Азизов, А.А. Бочков, А.А. Васильев, В.Д. Зорькин, А.С. Киселев, И.А. Конюхова, Д.А. Ловцов , Л.С. Мамут, Т.Л. Ровинская, А.М. Тарасов, Л.Н. Тимофеева и др.); исследования, раскрывающие изменения в характере властных отношений, процессы цифровизации государственных функций, а также проблемы становления государственного суверенитета в цифровой реальности (работы Ф. Баннистера[1], А.Л. Бредихина[2], А.В. Даниленкова[3], А.А. Ефремова[4], А.Е. Карповой[5], Т.С. Масловской[6], Г.Б. Романовского[7], Л.В. Терентьевой[8], С.В. Хмелевского[9].

Третья группа работ исследует проблемы развития гражданского общества в условиях цифровой реальности. В них анализируются изменения в социальных отношениях под влиянием цифровых информационно-

---

[1] Bannister F., Gronlund A. Information Technology and Government Research: A Brief History //Proceedings of the 50th Hawaii International Conference on System Sciences, 2017. - P.2943-2952 [Electronic resource]. Access mode: https: //scholarspace.manoa.hawaii.edu/bitstream/10125/41512/1/paper0363.pdf. - (Date of access: 30.08.2022).

[2] Бредихин А.Л. Суверенитет как политико-правовой феномен: Монография. - М.: Издательский дом «Инфра-М», 2020. - 128 с.

[3] Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной Сети Интернет //Lex Russica. -2017. - №7 (128). - С.154-165.

[4] Ефремов А.А. Конституционные основы и законодательное обеспечение государственного суверенитета РФ в информационном пространстве //Государственная власть и местное самоуправление. - 2016. - №12. - С.39-43.

[5] Карпова А.Е. Государственный суверенитет в современных условиях //Молодой ученый. - 2016. - №23. - С.334-336.

[6] Масловская Т.С. Цифровая сфера и конституционное право: грани взаимодействия //Конституционное и муниципальное право. - 2019. - №9. - С.18-22.

[7] Романовский Г.Б., Романовская О.В. Проблемы обеспечения цифрового суверенитета. Статья в сборнике материалов Международной научно-практической конференции. Санкт-Петербург, 2023, С.168-172

[8] Терентъева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве //Lex Russica. - 2019. - №7 (152). - С.119-128.

[9] Хмелевский С.В. Государственный суверенитет: понятие, содержание, актуальные теоретические и практические проблемы реализации //Пробелы в российском законодательстве. - 2015. - №4. - С.280-286.

коммуникативных технологий (ИКТ), а также раскрываются новые аспекты проведения демократических процедур (избирательных кампаний, голосований и пр.) в электронном формате (Р.В. Амелин[1], Я.В. Антонов[2], А.Жужлов[3], М.М.Курячая[4], Т.М.Махаматов[5], Ю.Г.Федотова[6], Д.Хорган[7]. Интерес представляют также работы, посвященные исследованию изменений в институтах гражданского общества под влиянием цифровых ИКТ (электронные средства массовой информации (СМИ), блогеры и пр.) (М.В. Жижина[8], Т.Л. Каминская[9], А.Г. Капустина[10], Е.А. Кожемякин[11], П.Ю. Нарушева[12] и др.).

---

[1] Амелин Р.В., Чаннов С.Е. Прямая электронная демократия в Российской Федерации: возможности и перспективы //Конституционное и муниципальное право. - 2017. - №1. - С.27-31.

[2] Антонов Я.В. Конституционно-правовые перспективы развития электронной демократии в современной России //Конституционное и муниципальное право. - 2016. - №9. - С.17-20.

[3] Жужлов А. Гражданское общество и Интернет-технологии //Власть. - 2010. - №8. - С.82-84.

[4] Курячая М.М. Электронное голосование как этап развития непосредственной демократии //Конституционное и муниципальное право. - 2017. - №11. - С.31-35.

[5] Махаматов Т.М. Перспективы демократии и роль гражданского общества в цифровом пространстве //Философское образование. - 2018. - №1 (37). - С.28-33.

[6] Федотова Ю.Г. Электронная демократия как средство обеспечения информационной безопасности государства //Информационное право. -2016. - №3. - С.17-24.

[7] Horgan D., Dimitrijevic B. Frameworks for citizens participation in planning: from conversational to smart tools //Sustainable Cities and Society. - 12 Apr. 2019. - №48 [Electronic resource]. Access mode: https: //doi.org/10.1016/j.scs.2019.101550. - (Date of access: 30.08.2022).

[8] Жижина М.В. Блогер в социальных представлениях молодежи //III Ломоносовские чтения. Актуальные вопросы фундаментальных и прикладных исследований. Сборник статей Международной научно-практической конференции (Петрозаводск, 14.11.2019). - Петрозаводск, 2019. - С.46-50.

[9] Каминская Т.Л. Блогер как актор развития онлайн-журналистики //Медиалингвистика. - 2014. - №53. - С.191-193.

[10] Капустина А.Г. Правовой статус субъектов информационно-коммуникативной деятельности в Интернете //Актуальные проблемы гуманитарных и естественных наук. - 2015. - №11-7. - С.43-46.

[11] Кожемякин Е.А., Попов А.А. Блоги как средство журналистской коммуникации //Научные ведомости Белгородского государственного университета. Серия: гуманитарные науки. - 2012. - №6 (125). - Выпуск 13. -С.148-155.

[12] Нарушева П.Ю. Основные черты блога и его роль в жизни современного человека //Вестник молодых ученых и специалистов Самарского университета. - 2017. - №1. - С.38-43.

Четвертая группа работ посвящена изучению статуса граждан в цифровом обществе, формированию цифровых прав и обязанностей, и акцентирует внимание на понятиях «цифровой гражданин», «цифровое гражданство» (Е.С. Аничкин[1], А.А. Богучарский[2], Е.В. Бродовская[3], Г.В. Градосельская[4], Н.В. Деева[5], А.И. Ковлер[6], В.В. Невинский[7], А.В. Нестеров[8], Э.В. Талапина[9], А.М. Эрделевский[10].

В *пятую группу* входят исследования, посвященные обеспечению безопасности граждан в цифровом пространстве посредством формирования цифрового суверенитета личности (Е.О. Гаврилова[11], И. Ашманова[12], А.

---

[1] Аничкин Е.С. Модернизация конституционно-правового статуса личности в условиях формирования цифрового пространства //Конституционное и муниципальное право. - 2019. - №12. - С.19-22.

[2] Богучарский А.А. Сетевое общество 21 века: влияние информационных технологий и виртуальной социализации на участие граждан в политических процессах политической жизни государства //Экономические и гуманитарные исследования регионов. - 2018. - №2. - С.53-58.

[3] Бродовская Е.В. Цифровые граждане, цифровое гражданство и цифровая гражданственность //Власть. - 2019. - Том 27. - №4. - С.65-69.

[4] Градоселъская Г.В. Сетевые измерения в социологии /Под редакцией Г.С.Батыгина. - М.: Издательский дом «Новый учебник», 2004. - 248 с.

[5] Деева Н.В. Тенденции развития российского гражданского общества в эпоху цифровизации //Гражданин. Выборы. Власть. - 2020. - №1 (15). - С.82-91.

[6] Ковлер А.И. Права человека в цифровую эпоху //Бюллетень Европейского суда по правам человека. - 2019. - №6 (204). - С.146-150.

[7] Невинский В.В. «Цифровые права» человека: сущность, система, значение //Конституционное и муниципальное право. - 2019. - №10. - С.26-32.

[8] Нестеров А.В. О цифровых правах и объектах цифровых прав //Право и цифровая экономика. - 2020. - №1 (07). - С.11-16.

[9] Талапина Э.В. Государственное управление в информационном обществе. Правовой аспект = Public administration in the information society. Legal aspect = L'administration publique dans la société de l'information. L'aspect juridique: монография /Российская академия наук, Институт государства и права. - М.: Издательство «Юриспруденция», 2015. - 188 с.

[10] Эрделевский А.М. О цифровых правах //ЮрФак: изучение права онлайн. - 26.06.2019 [Электронный ресурс]. Режим доступа: https: //urfac.ru/?p=2342. - (Дата обращения: 30.08.2022).

[11] Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой // Вестник КемГУ. Гуманитарные и общественные науки. 2020. - 4(2). - С.146-152.

[12] Ашманов И. Битва за рунет. Как добиться цифрового суверенитета? // E-news. 01.11.2019. Режим доступа:https://e-news.su/in-russia/303970-bitva-za-runet-kak-dobitsya-cifrovogo-suvereniteta-igor-ashmanov.html (дата обращения: 20.09.2022).

Черникова[1], Л. Ю. Черняк[2], А.А. Ефремова[3], И. М. Конобеевская[4]). Во многих работах акцентируется внимание на создании и управлении своими цифровыми идентичностями в цифровом пространстве (У. Дер, С. Йенихена, Я. Сюрмели[5]., К. Леонг, Т. Чи-ханг и др.[6]). В некоторых исследованиях (А. Фраес, М. Грейнер и др.)[7] представлены попытки сформировать концепцию и модель цифрового суверенитета как в рамках технологического подхода через суверенитет данных, технологический суверенитет, так и через выделение различных его уровней (физический уровень, уровень кода и т.д.)

Таким образом, несмотря на достаточно широкую теоретическую изученность вопросов, связанных с цифровизацией всех сфер жизни общества, анализ феномена цифрового суверенитета личности является фрагментарным в социологической науке и не полностью осознанным в обществе. Остаются недостаточно исследованным вопросы формирования цифрового суверенитета личности, его уровней и структуры и практические возможности его защиты в цифровом пространстве.

Объект исследования – личность как субъект социальных отношений и взаимодействий в цифровой среде.

---

[1] Черников А. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома // Vc.ru. 28.01.2020. Режим доступа: https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma (дата обращения: 20.09.2022).

[2] Черняк Л. Ю. К вопросу о понятии информационного суверенитета: теоретический и сравнительно-правовой аспекты // Сибирский юридический вестник. - 2012. - № 3. - С. 117-122.

[3] Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал высшей школы экономики. - 2017. - № 1. - С. 201-215.

[4] Конобеевская И. М. Цифровые права как новый объект гражданских прав // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. - 2019. - Т. 19. - № 3. - С. 330-334.

[5] Der, Uwe et al. “Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution.” *ArXiv* abs/1712.01767 (2017)

[6] Kheng Leong, Tan, Chi-Hung, Chi, and Kwok-Yan, Lam. Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization . 2022 Режим доступа // https://arxiv.org/abs/2202.10069

[7] Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., Wendeborn, T. Towards a Layer Model for Digital Sovereignty: A Holistic Approach. In: Hämmerli, B., Helmbrecht, U., Hommel, W., Kunczik, L., Pickl, S. (eds) Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723. Springer, Cham. 2023. Режим доступа: https://doi.org/10.1007/978-3-031-35190-7_9

Предмет исследования – цифровой суверенитет личности в социологическом дискурсе.

Цель исследования заключается в анализе формирования цифрового суверенитета личности, раскрытии его уровней, структуры и выработки эффективного механизма по обеспечению прав, обязанностей и ответственности личности в цифровом пространстве.

Задачи исследования:

- раскрыть методологические исследовательские подходы к определению сущности цифрового суверенитета личности;
- обосновать суверенную идентичность как условие формирования цифрового суверенитета личности;
- рассмотреть и проанализировать риски и угрозы цифровому суверенитету личности и социальному самоопределению граждан в цифровой среде;
- дать характеристику цифрового статуса личности как основы цифрового суверенитета личности;
- выявить уровни и структуру цифрового суверенитета личности;
- обосновать концептуальную модель цифрового суверенитета личности, предложить рекомендации к ее практическому применению.

Гипотеза научного исследования заключается в предположении, что процессы цифровизации, виртуализации и сетевизации создают новые возможности для формирования цифрового суверенитета граждан и обусловливают необходимость защиты прав и свобод индивидов в современном цифровом обществе. Такое понимание охватывает не только индивидуальный уровень как способность и возможность осознанно управлять своими данными и защищать конфиденциальность, но и организационный и государственный уровни, которые играют ключевую роль в обеспечении цифрового суверенитета личности. Исследование цифрового суверенитета через выявление уровней создаст возможность предусмотреть организационные и государственные меры в условиях постоянно меняющейся

цифровой среды. Обоснование суверенной идентичности, разработка структуры цифрового суверенитета направлено на развитие адаптационной способности к ответственному самоопределению и возможности индивида принимать независимые и обоснованные решения, контролируя свою идентичность.

Новизна научного исследования:

1. Предложено новое понятие «цифровой суверенитет личности», под которым понимается способность и возможность индивида предпринимать сознательные, преднамеренные и независимые действия, принимать самостоятельные решения в отношении всех элементов цифровой жизни (персональных данных, цифровых профилей в социальных сетях и Интернет-сервисах, аппаратного и программного обеспечения, цифровых процессов, электронных услуг и гибридной инфраструктуры), а также совокупность прав, обязанностей и ответственности, возникающих в результате реализации такой способности. Новацией данного подхода является акцент на осознанности и самоконтролируемости действий в цифровом пространстве, ответственности и обязанностях индивида, который не только имеет право на контроль над своими данными и цифровыми профилями, но и несет ответственность за свои поступки.

2. Раскрыта сущность и выделены основные принципы формирования цифровой суверенной идентичности как состояния, при котором индивид осознает и контролирует свою социальную идентификацию, самостоятельно действует и взаимодействует в цифровой среде, сохраняет легитимный контроль над своей идентичностью, автономно управляет персональными данными в различных информационных сервисах и несет ответственность за свои действия. Концепция цифровой суверенной идентичности подчеркивает активную роль индивида в формировании и управлении своей идентичностью как особого типа идентификационного поведения в условиях цифрового взаимодействия, что увеличивает осознанные адаптационные возможности для самовыражения и

взаимодействия, но также накладывает ответственность за самоконтролированное обеспечение своей конфиденциальности и безопасности в цифровом пространстве.

3. Определены основные риски и угрозы цифровому суверенитету личности, которые могут привести к нарушению идентичности, прав и свобод человека в цифровом пространстве и потере контроля над конфиденциальной, приватной и чувствительной информацией. Сделан вывод, что принудительное вовлечение граждан в цифровую среду, снижение правовой защиты в Интернете, возникновение цифрового неравенства, социальное и психологическое давление становятся важными конфликтогенными факторами, влияющими на нормы и правила взаимодействия в цифровом пространстве.

4. Выделены базовые компоненты цифрового статуса как основы адаптационного потенциала личности и ее цифрового суверенитета. Цифровой статус личности представляет собой совокупность отношений, прав, обязанностей и ответственности индивида, возникающих при действиях и взаимодействиях в цифровом пространстве, а также при реализации доступа к Интернету посредством свободного, открытого, равного и недискриминационного обмена информацией, общением и культурой. Подчеркнуто значение права человека на защиту своего цифрового статуса, а также отмечена роль личной ответственности как ключевого фактора обеспечения цифрового суверенитета.

5. Выявлены структура и уровни цифрового суверенитета личности. Выявление трех уровней формирования цифрового суверенитет личности: государственного, организационного и индивидуального - определяет возможности и способы его защиты, на основе которых разработана концептуальная модель цифрового суверенитета личности, включающая три базовых уровня (государство, организация и личность) со своими элементами. Ключевой идеей представленной модели выступает принцип синергетического взаимодействия личности, организации и государства в

цифровой среде, что коренным образом влияет на формирование, динамику и регулирование социальных отношений в условиях цифровой среды. Каждый уровень цифрового суверенитета включает соответствующие механизмы формирования: государственный уровень нацелен на развитие государственной политики в информационной сфере, обеспечение гражданских прав и свобод человека в цифровом пространстве, защиту персональных данных и др.; организационный уровень обеспечивает реализацию политики в отношении суверенитета данных в организации, внедрение технологических стандартов, обучение сотрудников организации новым технологиям и др.; индивидуальный уровень основан на свободном самоопределении в цифровом пространстве, самостоятельном регулировании собственной конфиденциальности, безопасности и прав в цифровом пространстве и др.

Теоретико-методологическую основу диссертационного исследования составили идеи, концепции, теории исследователей, связанные с объектом и предметом работы, в которых отражены методология научного знания и осмысления социальных процессов: С.А. Кравченко, И. Лакатоса, Г.В. Осипова, связанные с развитием цифровой реальности и цифрового пространства.

Основополагающими для диссертационного исследования цифрового суверенитета личности стали теория «социального капитала» Пьера Бурдье, которая позволяет выявить влияние социального капитала на возможности индивидов определять качество социальных связей в цифровом пространстве; теория «сетевого общества» Мануэля Кастельса о способах воздействия сетевых структур на доступ к информации и самовыражение людей в цифровом пространстве; идеи С.А. Кравченко о становлении новой «социо-цифро-природной реальности», которые позволили раскрыть риски и угрозы социальной деятельности в цифровом пространстве. Обоснование воздействия цифровизации на общественное сознание и социальные отношения основано на идеях Л.А. Василенко о становлении цифрового общества.

Автор в своем исследовании опирается на следующие основные теоретико-методологические подходы: междисциплинарный, социологический, социально-психологический, философский, правовой.

Источниковая база исследования представлена законодательными и нормативными правовыми актами Российской Федерации: Конституцией Российской Федерации; федеральными законами Российской Федерации; указами Президента Российской Федерации; постановлениями Правительства Российской Федерации; материалами и результатами реализации государственных программ, национальных и федеральных проектов национальных проектов, федеральных программ и проектов («Цифровая экономика», «Цифровая трансформация», «Развитие науки, промышленности и технологий» и др.).

Для аргументации тезисов диссертационного исследования, а также сделанных заключений, выводов и гипотезы использовались данные Всероссийского центра изучения общественного мнения (далее - ВЦИОМ), а также материалы научно-практических конференций, диссертационные исследования, монографии и статьи, другие документы и материалы, посвященные проблеме исследования.

Эмпирическая база диссертации.

В научной работе использованы следующие методы: социологический опрос, фокус-группа, вторичный анализ данных социологических исследований.

Исследования, проведенные непосредственно автором диссертации:

«Цифровой суверенитет личности». Метод исследования – экспертный опрос; время проведения - май-сентябрь 2024 года. В качестве экспертов выступили: сотрудники ИТ-структур (36% от общей численности), высших учебных заведений (19%), финансовых организаций (21%), служащие государственных и муниципальных органов (14%), общественных организаций (6%), представители частного бизнеса (4%). Всего опрошено 217

экспертов. Руководитель проекта: доктор социологических наук, доцент Е.А. Литвинцева. Индекс в диссертации: ЭО ЦСЛ-2024.

«Цифровой суверенитет личности». Время проведения: февраль – март 2024 г. Метод исследования: фокус-групповая дискуссия. Участники: первая группа (9 человек) – профессорско-преподавательский состав Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), проводящие занятия по дисциплинам «Социология», «Цифровое право», «Социология цифрового общества», «Информационно-коммуникативные технологии в государственном и муниципальном управлении»; вторая группа (10 человек) – специалисты в сфере информационных технологий и защиты персональных данных из государственных структур, бизнес-организаций, а также из организаций – лидеров цифровой трансформации в Российской Федерации (ПАО Сбербанк, ПАО ВТБ, ПАО Мегафон, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации) . Руководитель проекта: доктор социологических наук, доцент Е.А. Литвинцева. Индекс в диссертации: ФГ ЦСЛ-1, ФГ ЦСЛ-2.

Для вторичного анализа использованы материалы социологических исследований, отражающие проблематику цифрового суверенитета личности:

«О восприятии россиянами Интернета и о возможности его ограничения»[1]. Проведено Всероссийским центром изучения общественного мнения 6 апреля 2021 г. Метод опроса — телефонное интервью по стратифицированной двухосновной случайной выборке стационарных и мобильных номеров. В опросе приняли участие 1600 россиян в возрасте от 18 лет. В ходе исследования анализировалось отношение респондентов к восприятию Интернета, возможности распространяемой в Интернете информации, отношение к контролю в сети Интернет.

«Цифровой детокс – 2023: о пользовании Интернетом и отдыхе от

[1] https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-vozmozhnosti-ili-ugrozy

него»[1]. Проведено Всероссийским центром изучения общественного мнения 13 мая 2023 года. Метод опроса — телефонное интервью по стратифицированной случайной выборке, извлеченной из полного списка сотовых телефонных номеров, задействованных на территории РФ. В опросе приняли участие 1600 россиян в результаты опроса россиян о пользовании интернетом.

«Интернет без опасности»[2]. Проведено Всероссийским центром изучения общественного мнения 26 апреля 2024 года. Метод опроса — телефонное интервью по стратифицированной случайной выборке, извлеченной из полного списка сотовых телефонных номеров, задействованных на территории РФ. В опросе приняли участие 1600 россиян в возрасте от 18 лет. Представлены результаты мониторингового опроса россиян, посвященного безопасности в Интернете.

Основные положения диссертационного исследования, выносимые на защиту:

- раскрыто содержание понятие «цифровой суверенитет личности как способности и возможности индивида предпринимать сознательные, преднамеренные и независимые действия, принимать самостоятельные решения в отношении всех элементов цифровой жизни, а также совокупности прав, обязанностей и ответственности, возникающих в результате реализации такой способности;
- обосновано значение и принципы суверенной идентичности как состояния, при котором индивид осознает и контролирует свою социальную идентификацию, самостоятельно действует и взаимодействует в цифровой среде, сохраняя легитимный контроль над своей идентичностью;
- сформулированы и систематизированы риски и угрозы цифровому суверенитету личности. Такая систематизация может послужить фундаментом

[1] https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovoi-detoks-2023-o-polzovanii-internetom-i-otdykhe-ot-nego
[2] https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-bez-opasnosti

для практической оценки цифрового суверенитета личности и выработки конкретных направлений по его формированию, где индивиду как владельцу данных необходимо предоставить возможность реализовать свои права и нести ответственность за использование и обмен персональными данными с высоким уровнем безопасности;

– выделены базовые компоненты цифрового статуса как основы адаптационного потенциала личности и ее цифрового суверенитета, в частности, права, обязанности и ответственность индивида, возникающие при действиях и взаимодействиях в цифровом пространстве, а также при реализации доступа к технологиям и Интернету посредством свободного, открытого, равного и недискриминационного обмена информацией, общением и культурой;

– выявлены уровни цифрового суверенитета личности, существующие в синергийном взаимодействии. Цифровой суверенитет формируется индивидом с его мотивами и потребностями, знаниями и навыками в сфере ИТ-технологий, поддерживается (или не поддерживается) организациями с их технологическими возможностями и зависит от проводимой государством информационной политики, реализующей защиту прав граждан в цифровом пространстве и обеспечивающей национальную безопасность и технологический суверенитет;

– разработана концептуальная модель формирования цифрового суверенитета личности с выделением трех базовых уровней (государство, организация и личность) со своими элементами и с представлением их в соответствующие реляционные структуры. Для представления и описания модели разработана графическая нотация в виде диаграммы Венна, помогающая выявить общие черты и различия между данными уровнями формирования цифрового суверенитета личности;

– предложены рекомендации к практическому использованию концептуальной модели на каждом уровне модели и межуровневом взаимодействии, такие как совершенствование национальной цифровой

инфраструктуры, развитие государственных цифровых платформ для безопасного обмена информацией и предоставления государственных услуг, разработка механизмов обеспечения прозрачности в вопросах обработки и хранения персональных данных сотрудников и клиентов, осознанное индивидуальное поведение в цифровой среде через регулярный аудит личных цифровых следов, разработка системы индикаторов для мониторинга уровня цифрового суверенитета на каждом из трех уровней.

Теоретическая и практическая значимость диссертационного исследования состоит в развитии социологического знания о цифровом суверенитете личности. Предложенные выводы и рекомендации автора вносят вклад в теорию социологии цифрового общества, предлагая авторское определение понятий «цифровой суверенитет личности», «суверенная идентичность», «цифровой статус личности» и их структурных элементов. Данные определения расширяют существующие теоретические рамки и способствуют более глубокому пониманию взаимодействия между личностью и цифровой средой, а также открывают новые горизонты для социологических исследований в области социологии, социальной психологии, социологии права, связанных с идентичностью и самосознанием в цифровом контексте. Разработка концептуальной модели цифрового суверенитета личности с выделением трех уровней (государственного, организационного и индивидуального) создает основу для дальнейших практических исследований, направленных на изучение взаимодействия между этими уровнями и их влияния на безопасность и права граждан в цифровом пространстве.

Выявленная структура цифрового статуса личности может быть использована для разработки образовательных программ и инициатив, направленных на повышение осведомленности граждан об их правах и обязанностях в цифровом пространстве. Результаты исследования могут служить основой для совершенствования государственной политики в области цифровизации, включая защиту персональных данных, создание безопасной

цифровой инфраструктуры и поддержку прав граждан в Интернете. Концептуальная модель цифрового суверенитета личности может быть использована в деятельности организаций для внедрения лучших практик в области управления данными, повышения уровня защиты информации и обучения сотрудников.

Тема исследования соответствует требованиям **паспорта научной специальности 5.4.4. «Социальная структура, социальные институты и процессы»**, область науки: 5 Социальные и гуманитарные науки, группа научных специальностей: 5.4. Социология. Направления исследований: 6. Динамика и адаптация социальных групп и слоев в трансформирующемся обществе; 27. Процессы цифровизации, виртуализации и сетевизации в современном обществе; 29. Социальная идентификация. Типы идентификационного поведения.

Апробация результатов работы. Основные положения и выводы диссертационного исследования докладывались автором на заседаниях и методологических семинарах кафедры организационного проектирования систем управления Института государственной службы и управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, на международных (Международная конференц-сессия «Государственное управление и развитие России: глобальные тренды и национальные перспективы», (г. Москва, 18.05.2022 г.); Международная конференц-сессия «Государственное управление и развитие России: цивилизационные вызовы и национальные интересы» (г. Москва, 15.05.2023 г.); Международная конференц-сессия «Государственное управление и развитие России: новые горизонты и образ будущего (г. Москва, 20.05.2024 г.); XXII Международная конференция «Афанасьевские чтения» на тему «Личность, семья, общество: ценностная среда развития в контексте современных технологий» (г. Москва, 20.02.2025 г.); всероссийских (XVII Всероссийской межвузовской научной конференции "Наука и образование в

развитии промышленной, социальной и экономической сфер регионов России" (г. Муром, 31.01.2025 г.) научно-практических конференциях.

Материалы настоящего диссертационного исследования были апробированы в следующих формах:

– опубликовано 6 научных статей с основными положениями и выводами диссертационного исследования в рецензируемых научных журналах, в том числе три из них (общим объемом 1,8 п. л.) в ведущих журналах, рекомендованных Высшей Аттестационной Комиссией (ВАК);

— непосредственно в практической деятельности автора в федеральном государственном органе, осуществляющим надзор в сфере информационной безопасности, в частности в Центре информационной безопасности ФСБ России при расследовании преступлений, связанных с незаконным распространением персональных данных.

Настоящая диссертационная работа обсуждена на заседании кафедры организационного проектирования систем управления Факультета Управления персоналом и государственной службы Института государственной службы и управления РАНХиГС.

Структура диссертации определена общей целью и задачами исследования. Настоящая диссертация состоит из введения, двух глав, шести параграфов основной части, заключения, 150 использованных источников и литературы, включающих 5 монографий, 62 зарубежных исследования. В настоящем диссертационном исследовании использовано более 40 научных работ, опубликованных за последние 5 лет, начиная с 2020 года.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ В СОЦИОЛОГИЧЕСКОМ ДИСКУРСЕ

1.1 Цифровой суверенитет личности: методологические исследовательские подходы

В последнее время термин «цифровой суверенитет» стал достаточно популярным в научной литературе, социальном и политическом дискурсе. Его употребляют в разных контекстах и смыслах, связывают с национальным государством и информационной безопасностью, корпоративным сектором и экономикой, с гражданами и их коммуникацией в социальных сетях и Интернете.

Для определения основных методологических подходов к исследованию цифрового суверенитета личности предлагается разбить настоящее исследование на несколько этапов.

Во-первых, исследовать предпосылки возникновения концепций суверенитета, суверенности, идентичности, идентификации и особенностей становления цифрового суверенитета с последующим превращением его в самостоятельную форму суверенитета.

Во-вторых, систематизировать различные контексты использования цифрового суверенитета, выявить его общие и отличительные характеристики.

В-третьих, раскрыть системно-структурные компоненты цифрового суверенитета личности и операционализировать данное понятие.

В-четвертых, предложить авторское определение термина «цифровой суверенитет личности».

Хотя термин суверенитет использовался еще со времен древних римлян, его концептуально-историческое содержание часто ассоциируется с такими авторами, как Н. Макиавелли, Т. Гоббс, Ж. Боден, а позже и К. Шмитт, которые ссылаются на общественный договор между абсолютным сувереном

и народом. Хотя это изначально далеко от интуитивного понимания того, что сегодня подразумевается под цифровым суверенитетом, они раскрывают одну особенность: термин «суверенитет» обладает относительной стабильностью (постоянными характеристиками), которая сохраняется даже в формирующемся в настоящее время цифровом пространстве. А именно, сущность всегда остается суверенной относительно другой сущности или объекта. Это делает полезным рассмотрение различного набора отношений в дальнейшем. В конечном счете, то же самое относится к термину «цифровой суверенитет», представляющего собой не статическую конструкцию, а обретающего свою форму в социальном взаимодействии.

Одно из самых распространенных определений суверенитета содержится в работах Н.Б. Пастуховой, под которым понимается «правовое качество или свойство государства, символизирующее политико-правовую самостоятельность государства, его верховенство в пределах своей территории и независимость в государственных отношениях от других государств»[1].

В Стэнфордской философской энциклопедии определены следующие ключевые принципа суверена: «…1) обладание властью; 2) власть проистекает «из какого-то взаимно признанного источника легитимности» (Бог, конституция или закон); 3) власть является высшей; и 4) власть над территорией…»[2] . При этом отмечается возможность ограничения такой власти посредством международных или региональных договоров, действий транснациональных корпораций или глобальных вызовов, в частности, развитием глобальных коммуникационных и телекоммуникационных

[1] Пастухова Н.Б. Суверенитет и федеративная организация российского государства в условиях глобализации: конституционно-правовые аспекты. Автореферат дисс. доктора. юр. наук., М.: 2010. 46 с

[2] Philpott D. Sovereignty. Stanford Encyclopedia of Philosophy Archive, 31 May 2003. Page 3, Режим доступа: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/.

инфраструктур и Интернета[1]. Также в некоторых исследованиях отмечается усиление дискурса суверенитета при слабой реальной власти и наоборот[2].

По мере того как меняются понятия власти, функций государства и пределов его вмешательства в дела гражданского общества, наполняются новым содержанием понятия права, свободы и ответственности человека. Впоследствии это приводит к тому, что понятие суверенитет начинает проявляться в других контекстах и для других субъектов, выходящих за рамки традиционных представлений о суверенитете и оказывающих влияние на концептуализацию понятия «цифровой суверенитет». Появились такие термины как «продовольственный суверенитет»[3], «суверенитет тела», «технологический суверенитет», «информационно-коммуникативный суверенитет» и т.д.

В условиях, когда социальные взаимодействия все больше опосредуются электронными коммуникациями[4], особую актуальность приобретает вопрос о том, как индивид может сохранять автономию и суверенитет в цифровом пространстве. Сетевые структуры, ставшие основой нового социального порядка, одновременно расширяют возможности самовыражения и доступа к информации, но также создают новые формы зависимости и контроля[5]. Цифровой суверенитет личности становится важнейшим элементом существования в сетевом обществе, позволяющим сохранять индивидуальную свободу и идентичность.

В основе социологии цифровизации, предложенной С.А. Кравченко, лежит понимание амбивалентности современных процессов цифровой

---

[1] Bhandar B. The conceit of sovereignty: toward post-colonial technique. In: Lessard B (ed.) Stories Communities: Narratives of Contact and Arrival in Constituting Political Community. Vancouver, BC, Canada: University of British Columbia Press, 2011. pp. 66–88.

[2] Werner WG and De Wilde JH. The Endurance of sovereignty. European Journal of International Relations 7(3). 2001. P 307

[3] Шестопал С. С., Мамычев А. Ю. Суверенитет в глобальном цифровом измерении: современные тренды // БГЖ. 2020. №1 (30). URL: https://cyberleninka.ru/article/n/suverenitet-v-globalnom-tsifrovom-izmerenii-sovremennye-trendy (дата обращения: 21.08.2023).

[4] Кастельс М. Власть коммуникации. М., 2016. С.16

[5] Там же. С. 18

трансформации. С одной стороны, цифровизация наделяет человека невиданными ранее возможностями познания и преобразования мира, с другой – создает сложные вызовы, на которые наука пока не дала исчерпывающих ответов[1]. В этом контексте особенно актуальным становится вопрос о сохранении личностной автономии в цифровом мире, что напрямую связано с концепцией цифрового суверенитета.

Одним из ключевых аспектов социологии цифровизации С.А. Кравченко является концепция «цифрового тела», формирующегося у современного человека в процессе социализации. Это «цифровое тело» наделяет его новыми способностями познания и преобразования мира, но одновременно создает основу для новых форм зависимости и уязвимости. Личная идентичность в гибридной среде расширяется за счет цифровой или сетевой составляющей[2], что усложняет вопросы самоидентификации и сохранения целостности личности.

С.А. Кравченко полагает, что смешение реального и виртуального миров порождает парадоксальное сосуществование реальных и инсценированных рисков[3], формируя новые вызовы для индивида. В этих условиях цифровой суверенитет личности становится не просто желательным, а необходимым условием сохранения психологического благополучия и автономии в принятии решений.

В целом, использование понятия «цифровой суверенитет» в научной литературе является широким и разнообразным, и можно выделить несколько контекстов его применения, каждый из которых отражает отдельные характеристики, в частности:

---

[1] Кравченко, С. А. Социология цифровизации : учебник для вузов / С. А. Кравченко. - Москва : Издательство Юрайт, 2021. - 236 с. - (Высшее образование). - ISBN 978-5-534-14307-2.

[2] Василенко Л.А., Мещерякова Н.Н.. Гибридность цифрового общества. Философия науки и техники 2023. Т. 28. № 1. С. 48–65

[3] Кравченко, С. А. Социология цифровизации : учебник для вузов / С. А. Кравченко. - Москва : Издательство Юрайт, 2021. С. 67

- суверенитет киберпространства, связанный со степенью и характером государственного контроля интернета и регулированием коммуникаций (суверенный интернет);

- цифровой суверенитет государства, связанный с контролем органами государственной власти различных элементов цифрового мира, включая регулирование коммуникаций как средства передачи значимой для государства информации;

- цифровой суверенитет коренных народов и местных общин, возникший вследствие необходимости восстановления суверенитета над землей, культурой и традициями;

- цифровой суверенитет социальных движений, связанный с общественным контролем над технологиями, коммуникациями и цифровой инфраструктурой;

- цифровой суверенитет организаций, связанный со способностью отдельных лиц и компаний функционировать в цифровом мире;

- цифровой суверенитет личности, связанный с контролем человека над своими данными, коммуникациями, устройствами, программным обеспечением и другими технологиями;

Проанализируем некоторые направления и выделим особенности использования термина «цифровой суверенитет» в социологическом дискурсе.

На ранних этапах развития интернета возникла идея независимого от государств цифрового или суверенного пространства, которое должно быть создано вне территориальных границ, свободно от государственного регулирования и вмешательства, со своими правилами, правами и ответственностью пользователей. Интернет как особый способ коммуникации является континуальным и бесконечным процессом общения, где сами границы коммуницирования сложно определить. Такой подход угрожал разрушить национально-государственную, территориально ограниченную и суверенную государственную систему.

Подобные идеи, связанные с суверенитетом в коммуникативном киберпространстве, актуальны и в настоящее время. Так, М. Мюллер отмечает, что именно люди и их индивидуальные коммуникации являются основными носителями суверенитета в киберпространстве[1] .

Под цифровым суверенитетом государства, как правило, понимают «право и возможность правительства самостоятельно и независимо определять внутренние и геополитические национальные интересы в цифровой сфере, вести самостоятельную внутреннюю и внешнюю информационную политику, распоряжаться собственными информационными ресурсами, формировать инфраструктуру национального информационного пространства, гарантировать электронную и информационную безопасность государства»[2], а также «осуществлять регулирование информационных отношений в рамках соответствующего информационного пространства» [3].

Китайский исследователь Т. Ху отмечает связь появления термина «цифровой суверенитет государства» с развитием вычислительных облаков и возрождением суверенной власти в сфере данных[4]. Сегодня государства и правительства действительно много говорят о цифровом суверенитете и контроле коммуникативных потоков данных между государствами. В одном из первых размышлений, опубликованном в 2012 году французским бизнесменом П. Белланже, цифровой суверенитет определяется как «…контроль над нашим настоящим и нашей судьбой в том виде, в каком они проявляются и ориентируются посредством использования технологий и

[1] Mueller M. Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Malden, MA: Polity. 2017

[2] Перова М. В., Волковская И. В., Максимова А. М. Цифровой суверенитет как приоритет государственной политики на современном этапе // Вызовы современности и стратегии развития общества в условиях новой реальности: сборник материалов VI Международной научно-практической конференции, Москва, 21 февраля 2022 года / редколлегия: Л. К. Гуриева, З. Ш. Бабаева [и др.]. Москва: ИП Овчинников Михаил Артурович (Типография Алеф), 2022. С. 118—122.

[3] Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал высшей школы экономики. 2017. № 1. С. 201-215

[4] Hu TH. A Prehistory of the Cloud. Cambridge, MA: The MIT Press. 2015

компьютерных сетей…»[1]. Данный автор выступает за цифровой суверенитет как способ противодействия тотальному «экспорту частной жизни» граждан и предлагает разработать национальные облака, в которых должны храниться данные о государстве и его гражданах. Эта аргументация согласуется со многими современными заявлениями о том, что государства должны установить контроль над своими данными, коммуникационными и телекоммуникационными сетями по отношению к другим странам, особенно к США.

Исследователь Э. Вудс выделяет такие ключевые элементы цифрового суверенитета как верховный контроль; контроль над территорией; независимость от других суверенов[2]. Также Э. Вудс отмечает необходимость исключительного контроля над данными со стороны государства в пределах государственной границы, а также принуждение к соблюдению норм и требований органов государственной власти и контроль средств соблюдения.

В некотором противоречии с государственным суверенитетом находится *цифровой суверенитет социальных движений*. Данная категория используется для подтверждения автономии социальных сообществ посредством общественного контроля над технологиями, коммуникациями и цифровыми инфраструктурами и касается таких аспектов, как бесплатное программное обеспечение, сервисы с открытым исходным кодом и т.д. Так, А. Хаше подчеркивает, что цифровой (технологический) суверенитет относится к «технологиям, разработанным гражданским обществом и для него».[3] Гражданское общество, по его мнению, - это граждане и коллективы, действия которых в первую очередь мотивированы не соблазном получения прибыли, а скорее реакцией на желания и потребности, вызванные, в том числе социальными и политическими трансформациями, а также цифровизацией.

---

[1] Bellanger P. De la souveraineté numérique. 2012. Le Débat 170(3): 149–159. P. 154

[2] Andrew Keane Woods, Litigating Data Sovereignty, 2018, 128 YALE L.J. P. 360

[3] Haché A. La souveraineté technologique. Dossier Ritimo. 2014. Режим доступа: https://www.ritimo.org/IMG/pdf/dossier-st1.pdf P. 11

В данном контексте Л.А. Василенко отмечает, что «в цифровом обществе становится жизненно важным адекватное построение социально-ориентированного управления и внедрение механизмов регуляции, направленных на изменение поведенческих практик и уровней общественных взаимодействий». Все это, соответственно, ведет к изменениям в коммуникативных взаимодействиях, в сборе, анализе и систематизации информации.[1]

Суверенность означает наличие возможностей для реализации самостоятельных действий. Так, Т. Нито отмечает, что быть суверенным в отношении своих личных данных – это значит обрести автономию и свободу действий в информационно-коммуникационном пространстве [2]. Благодаря силе и возможностям технологических корпораций государство зачастую не может в полном объеме поддерживать безопасность коммуникаций своих граждан в Интернете, а это означает, что теперь на последних лежит необходимость защиты собственного личного цифрового суверенитета[3]. В этом контексте суверенитет социальных движений в некоторой степени противоречит государственному подходу к цифровому суверенитету.

В контексте деятельности местных общин и малых народов цифровой суверенитет связывают с такими характеристиками гражданина, как культура, идентичность и его неразрывность с суверенитетом соответствующей коренной нации или местной общины[4]. Коммуникативный аспект в данном формате означает изменения в процессах передачи эмоционального и интеллектуального содержания общения.

---

[1] Василенко Л.А. Социология цифрового общества : монография / Л.А. Василенко, Н.Н. Мещерякова ; Томский политехнический университет. – Томск : Изд-во Томского политехнического университета. 2021.

[2] Nitot T. Numérique : reprendre le contrôle. Paris: Framasoft. 2016. Режим доступа: https://framabook.org/docs/NRC/Numerique_ReprendreLeControle_CC-By_impress.pdf P.3

[3] Литвинцева Е.А., Васекин А.С. Формирование цифрового суверенитета личности: коммуникативный аспект Коммуникология. 2024. Т. 12. № 3. С. 116-127.

[4] Couture, S., & Toupin, S. What does the notion of «sovereignty» mean when referring to the digital? New media and society, 2019, 21(10), 2305–2322.

Существует небольшое количество исследований, относящихся к *цифровому суверенитету организации*, в их числе работы И. Хартманна, Леманна и т.д. В исследованиях Хартманна цифровой суверенитет организации сравнивается с цифровым суверенитетом личности и предлагаются возможности его измерения с точки зрения степени субъектности и контроля в цифровом пространстве[1]. В этом смысле Леманн и Дёрр понимают цифровой суверенитет организаций как способность самостоятельно получать информацию о соответствующих коммуникациях, технологиях, новых технических решениях и иметь возможность выбора между несколькими вариантами информационно-коммуникационных технологий для определения стратегии развития организации»[2].

Подчеркнем, подавляющее большинство исследований изучают либо индивидуальную, либо государственную направленность цифрового суверенитета. В литературе слишком мало внимания уделяется тому факту, что организации являются частью экосистем, и поэтому дискуссии о цифровом суверенитете, как нам представляется, должны быть сосредоточены на всей цепочке социальных взаимодействий: государство, личность, организация. На наш взгляд, в настоящее время организации не уделяют достаточное внимание собственному цифровому суверенитету. Для них представляют больший интерес такие концепты как технологический суверенитет и суверенитет данных. Например, зависимость организации от поставщика программного обеспечения или доступность цифровых сервисов и т.д.

Как И. Хартманн и А. Пентенридер, рассматривая цифровой суверенитет в контексте организационных структур, выделяют такую характеристику, как

1 Hartmann, E.A. Digitale souveränität: soziotechnische bewertung und gestaltung von anwendungen algorithmischer systeme. In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten II, 2022, pp. 1–13. Springer, Heidelberg . Режим доступа: https://doi.org/10.1007/978-3-662-64408-9_1

2 Lehmann, C., Dörr, L. Digital souveräne gestaltung von services – ein marktfähiger mehrwert? In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten II, 2022, pp. 14–24. Springer, Heidelberg P. 14. Режим доступа: https://doi.org/10.1007/978-3-662-64408-9_2

способность, осуществляя коммуникации, анализировать новые технические решения, чтобы иметь возможность выбирать лучшие из различных цифровых технологий[1]. И данная характеристика предполагает наличие взаимосвязи между способностью организаций к инновациям и цифровым суверенитетом. Например, Богенштaль и Зинке фокусируются на таких тенденциях в развитии организации как интеллектуальные алгоритмы, большие данные, искусственный интеллект (машинное обучение) или Интернет вещей[2].

Развитие цифрового суверенитета личности во многом связано с ускорением цифровой трансформации и появлением более совершенных информационно-коммуникационных технологий. Учитывая доминирующее положение крупных технологических гигантов в области облачных вычислений и социальных сетей (Yandex, Google и тд.), данные практически каждого человека и организации в каком-то виде хранятся и обрабатываются неизвестным образом в облаке этих компаний, что может потенциально привести к нарушению фундаментальных прав человека и угрозе суверенитету человека в цифровом пространстве, приватности его персональных данных и конфиденциальности индивидуальных коммуникаций.

Широкое применение умных устройств, технологий мобильности и связи, использование цифровых профилей и аккаунтов, содержащих чувствительную и конфиденциальную информацию в различных сферах общественной жизни, поднимает вопрос о надлежащей защите цифровых прав человека как одного из ключевых элементов цифрового суверенитета личности.

Таким образом, само понятие личности в цифровую эпоху приобретает новое содержание и становится более сложным. Личность современного человека, имеющего хотя бы одно цифровое устройство, начинает

---

[1] Pentenrieder, A., Bertini, A., Künzel, M.Digitale Souveränität als Trend? Digitalisierung souverän gestalten. 2021. Режим доступа: https://doi.org/10.1007/978-3-662-62377-0_2

[2] Bogenstahl, C., Zinke, G. Digitale Souveränität - ein mehrdimensionales Handlungskonzept für die deutsche Wirtschaft. Digitale Souveränität, 2017 . p. 65

приобретать свое цифровое содержание[1]. Цифровая личность рассматривается как процесс и результат постоянной «оцифровки» личности, а все индивидуальные учетные записи и аккаунты и другие реквизиты, являясь средствами коммуникации, дополняют личность и являются ее «донастройками».

Так, рассуждая о цифровом суверенитете личности, Л. Флориди начинает с раскрытия индивидуального суверенитета, который он определяет как «собственность на самого себя или самопринадлежность, особенно над собственным телом, выбором и данными»[2], а затем расширяет до «цифрового суверенитета», который он определяет как «управление данными, программным обеспечением, стандартами и протоколами, оборудованием, услугами и инфраструктурой».

Важно отметить, что такое понимание не ограничивает претензии государств на суверенитет, оно, в определенном смысле, позволяет различным организациям, общественным объединениям и даже отдельным лицам сохранять суверенитет.

По мнению Гурова О.Н. и Петруниной А.А., цифровой суверенитет представляет собой «достижение и поддержание независимости при осуществлении цифровых процессов индивидуальными пользователями и юридическими лицами, действующими в киберпространстве, от любого нежелательного вмешательства со стороны органов управления данным цифровым сегментом Интернета и/или их агентов влияния»[3]. Они отмечают отсутствие самодостаточности этого понятия и тесную взаимосвязь с понятием культурного суверенитета.

---

[1] Василенко Л.А.. Социология цифрового общества : монография / Л.А. Василенко, Н.Н. Мещерякова ; Томский политехнический университет. 2021 – Томск : Изд-во Томского политехнического университета. С.90

[2] Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, 33 PHILOSOPHY AND TECHNOLOGY 369, 371 (2020)

[3] Гуров О. Н., Петрунина М. А. Цифровая трансформация: человеческое измерение // Гуманитарный вестник. 2020. №2 (82). С. 6. URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-chelovecheskoe-izmerenie (дата обращения: 09.11.2023).

Таким образом, анализируя основные контексты применения термина «цифровой суверенитет личности», можно выделить ряд общих характеристик и различий, присущих этому понятию.

Во-первых, несмотря на то, что данный термин исторически использовался и продолжает использоваться главным образом для решения вопросов государственного контроля над технологиями, в настоящее время он активно применяется и другими субъектами, в частности, бизнесом, организациями гражданского общества, общественными объединениями, коренными народами, местными сообществами и отдельными индивидуумами. В некотором смысле наблюдается переход от коллективного восприятия (государства и общества) к более индивидуальному подходу, ориентированному на личность.

Во-вторых, концепция цифрового суверенитета связана с такими понятиями, как контроль, независимость и автономия несколькими способами. В первую очередь, речь идет о способности общества, государства, группы, социальных движений к инновациям или внедрению технологических решений. Это может проявляться, например, в виде поддержки национальных инноваций в рамках экономического национализма со стороны государства или разработки свободного программного обеспечения и автономной инфраструктуры для организаций гражданского общества.

В-третьих, важным аспектом является безопасность и неприкосновенность частной жизни как отдельных граждан, так и коллективов. Это также касается владения и контроля над информационными данными, относящимися к обществу или государству.

В-четвертых, за концепцией цифрового суверенитета нередко стоит стремление создать противовес крупным транснациональным ИТ-компаниям. Дискурс о суверенитете, как правило, становится более актуальным в ситуациях, когда наблюдается слабость власти над объектом.

Несмотря на эти сходства, существуют и фундаментальные различия между существующими концепциями цифрового суверенитета. Например,

авторитарные государства используют концепцию государственного цифрового суверенитета для легитимизации своих властных методов, включая наблюдение и цензуру данных и коммуникаций в пределах своей юрисдикции. В то же время социальные движения рассматривают цифровой суверенитет как способ защиты от такого государственного контроля. Также стоит отметить, что индивидуумы рассматриваются как носители суверенитета исключительно в контексте своей частной жизни, а не как сотрудники компаний.

Рассмотрев основных субъектов, активно применяющих цифровой суверенитет, проанализируем содержательные характеристики этого понятия.

1. *Упрощение термина «цифровой суверенитет» и сведение к одному конкретному смыслу*. В некоторых научных публикациях цифровой суверенитет предлагают интерпретировать в рамках определенных условий и подходов. Например, в таких конструкциях, как «правительства выразили обеспокоенность по поводу цифрового суверенитета, когда государственные данные перемещаются в облако …» возникают вопросы об обеспечении конфиденциальности общедоступных информационных активов, находящихся в облаке и их хранении, в том числе за границей и т.п...»[1]. В этом контексте термин цифровой суверенитет сводится к условиям и методам его использования без необходимости всеобъемлющего определения.

2. *«Цифровой суверенитет» как способность или возможность*. Исследователи отмечают эти особенности цифрового суверенитета, не анализируя условия, в которых он реализуется. Например, «…мы рассматриваем цифровой суверенитет как способность пользователя полностью контролировать свои данные»[2], и «установление суверенитета данных (то есть контроль и проверка геолокации данных) имеет ключевое

[1] Irion K. Government cloud computing and national data sovereignty. 2012. Policy & Internet 4(3–4): 40–71. P . 41

[2] Alboaie S and Cosovan D. Private data system enabling self-sovereign storage managed by executable choreographies. 2017.Lecture Notes in Computer Science LNCS 10320: 83–98. P. 86

значение»[1], или «цифровой суверенитет одновременно включает в себя две ключевые компоненты: возможности независимого применения цифровых технологий в собственных интересах и способности их использования» [2].

3. *«Цифровой суверенитет» как право*. В некоторых работах цифровой суверенитет трактуется как право субъекта совершать определенные действия. Например, «суверенитет данных - это право нации собирать свои собственные данные и управлять ими»[3] или «суверенитет над данными коренных народов - это право коренных народов и наций управлять сбором, владением и применением данных об их народах, землях и ресурсах»[4]. По мнению Кочеткова А.П., «цифровой суверенитет предполагает право национальных государств на независимое управление своими цифровыми ресурсами, надзор и контроль за деятельностью собственных цифровых платформ»[5].

В таком же контексте данное понятие определятся в Концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации, в соответствии с которой цифровой суверенитет подразумевает «право человека полностью или частично отказаться от вовлечения в цифровое взаимодействие, иметь возможность осуществлять свои права с государством и обществом вне цифрового пространства»[6].

---

[1] Esposito C, Castiglione A and Choo KKR. Encryption-Based Solution for Data Sovereignty in Federated Clouds. 2016. IEEE Cloud Computing 3(1): 12–17. P. 14

[2] Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. 2020. № 4. С. 3–11.

[3] Rainie SC, Schultz JL, Briggs E, et al. Data as a strategic resource: Self-determination, governance, and the data challenge for indigenous nations in the United States. 2017. International Indigenous Policy Journal 8(2). P 5-6

[4] Garrison NA, Hudson M, Ballantyne LL, et al. Genomic research through an indigenous lens: Understanding the expectations. 2019. Annual Review of Genomics and Human Genetics 20: 495.

[5] Кочетков Александр Павлович, Маслов Константин Вадимович Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. №2.

[6] Проект Концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации // https://rocit.ru/uploads/4f68dc0a2487678a7675ad7589280277050b4004.docx?t=1639585614

В отдельных работах нет прямого отождествления цифрового суверенитета с правом, однако отмечается связь между ними. Например, «развитие суверенитета данных коренных народов как движения, возглавляемого коренными народами, и как области исследований подчеркнуло четкие права и интересы, которые коренные народы, имеют в отношении своих данных»[1].

4. *«Цифровой суверенитет» как правовая норма*. Например, есть такая точка зрения, что «цифровой суверенитет - это концепция, согласно которой информация, преобразованная и сохраненная в двоичной форме, подчиняется законам страны, в которой она находится»[2]. Применительно к рынку облачных услуг, суверенитет данных понимается как «правила, определяющие, как и где должны храниться определенные наборы данных в пределах национальных границ, и определяющие права правительств на доступ к этим данным, когда им это необходимо»[3]. Другие подчеркивают в большей степени аспекты, связанные с обороной и национальной безопасностью. Так, термин «суверенитет данных» относится к национальному законодательству о защите государства от внешних угроз, таких как государственные субъекты и негосударственные организации[4]. Суверенитет данных касается степени и ограничений контроля над данными и облаком, которые на первый взгляд являются предметом «конкурирующих требований суверенной власти» со стороны нескольких стран и осложняются «экстерриториальными эффектами»[5] попыток регулирования интернета.

5. *Цифровой суверенитет как преимущество «богатства данных».* Обеспечение цифрового суверенитета заключается в том, что он более

---

[1] Kukutai T and Cormack D. Census 2018 and implications for M_aori. New Zealand Population Review 44, 2018. 131–151. P. 145

[2] Hippelainen L, Oliver I and Lal S. Towards dependably detecting geolocation of cloud servers. In: Yan Z, et al. (eds) Network and System Security. Cham: Springer, 2017, pp.643–656. P. 645

[3] Courtney M. Regulating the cloud crowd. 2013.Engineering & Technology 8(4): 60–63. P. 60

[4] Nugraha Y, Kautsarina K and Sastrosubroto AS. Towards data sovereignty in cyberspace. In: 2015 3rd international conference on information and communication technology (ICoICT), Nusa Dua, Indonesia, 27–29 May 2015, pp.465–471.

[5] Woods AK. Litigating data sovereignty. Yale Law Journal 128(2), 2018, 328–406. P. 335

благоприятен для инноваций и гибок, чем жесткие законы о защите данных. В этой связи многие исследователи призывают заменить понятие «защиты данных» понятием «суверенитета данных». Минимизация данных не может оставаться руководящим принципом государственной политики и будет угрожать международной конкурентоспособности страны. Так, П. Кениг считает, что «…вместо стремления к минимизации и экономии данных необходимо установить менталитет «богатства данных», напрямую связывая распространение данных с желаемыми экономическими результатами…» [1].

6. *Цифровой суверенитет как расширение термина государственный суверенитет.* Заметные различия также касаются отношения между цифровым суверенитетом и суверенитетом в классическом понимании. Так, К. Ирион отмечает, что «…национальный суверенитет зависит от адекватного суверенитета данных… если в стране нет эффективных средств контроля за публичной информацией, она частично становится недееспособной»[2]. Данный автор также рассматривает суверенитет данных как расширение суверенитета: «цифровой суверенитет представляет актуальную проблему государственной политики для правительств во всем мире, потому что это важнейшее измерение национального суверенитета, которое предполагает наличие национального государства»[3]. В частности, суверенитет данных является необходимым условием реализации национального суверенитета. «На национальном уровне способность накапливать, обрабатывать и использовать огромные объемы данных станет новым ориентиром силы страны. Информационный суверенитет страны в киберпространстве станет еще одним пространством игры великих держав, помимо суши, моря, воздуха и космоса»[4].

---

[1] Keonig PD. The place of conditionality and individual responsibility in a “data-driven economy”. 2017, Big Data & Society 4(2): 205395171774241.

[2] Irion K. Government cloud computing and national data sovereignty. 2012, Policy & Internet 4(3–4): 40–71. P. 53

[3] Там же P. 42

[4] Jin X, Wah BW, Cheng X, et al. Significance and challenges of big data research. 2015, Big Data Research 2(2): 59–64. P. 60

Также, по мнению А.П. Кочеткова, «…отрицание цифрового суверенитета национального государства означает отказ от государственного управления на национально-территориальном уровне и переход к глобальному цифровому управлению в масштабах всего мира…»[1].

Таким образом, можно отметить отсутствие единых подходов к пониманию цифрового суверенитета как в отечественной, так и в зарубежной литературе. При этом одна принципиальная проблема заключается в том, что авторы часто несколько уклончивы в отношении специфики своего понимания цифрового суверенитета и того, как этот термин соотносится с альтернативными концепциями. Одни авторы понимают суверенитет как право, тогда как другие считают, что это возможность. Это различие, по-видимому, важно, поскольку оно затрагивает обязательства относительно того, является ли цифровой суверенитет чем-то, что уже существует и чем-то, чем мы обладаем, или же он больше похож на цель, то есть на то, к чему мы должны стремиться. Конечно, эти варианты не являются строгими альтернативами, и есть место для их взаимной совместимости. В рассмотренных публикациях иногда упоминается, что могут быть некоторые противоречия, например, между суверенитетом данных отдельных лиц и суверенитетом данных населения, общества или государства.

Многоаспектность и наличие множества коннотаций понятия «цифровой суверенитет» заставляет нас обратиться к поиску ключевых свойств, характеристик и элементов данного термина.

В исследовании П. Хаммела и др.[2] подсчитывается частота использования термина «цифровой суверенитет» в научной и академической зарубежной литературе совместно с другими понятиями. Он выделил наиболее часто встречаемые и получил следующие результаты:

---

[1] Кочетков Александр Павлович, Маслов Константин Вадимович Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. №2.

[2] Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock. Data sovereignty: A review Big Data & Society 2021 8:1

1) контроль и власть (0.12; 85);

2) безопасность и непричинение вреда (0.09; 32);

3) автаркия (0,08 ;18);

4) автономия (0,07; 16);

5) представление и включение (0,06;19)[1].

Рассмотрим некоторые из них более подробно.

1. Легитимный контроль. Границы цифрового суверенитета личности выходят далеко за пределы суверенитета человека над его данными, а скорее охватывают все цифровое измерение его жизни. Возможно, это связано с тем, что зачастую обеспечить суверенитет данных можно только с учетом процессов, стандартов и других элементов цифровой системы. Контроль над этими дополнительными характеристиками цифровой среды оказывает огромное влияние на способность человека к самоуправлению в соответствии со своими собственными соображениями и желаниями, что является воздействием на его автономию и индивидуальный суверенитет.

Как отмечает Л. Флориди, для обеспечения цифрового суверенитета личности особенно важно наличие легитимного контроля, поскольку он представляет нормативный облик цифрового суверенитета[2]. Контроль над цифровым пространством является проявлением цифрового суверенитета только в том случае, если этот контроль является законным. Именно это делает суверенитет нормативным понятием и отличает его от простого фактического контроля.

Реализация легитимного контроля в цифровой среде связана с пониманием того, что в государстве считается легитимным контролем, и в каких случаях этот контроль не нарушает индивидуальные границы и не вмешивается в личную жизнь индивидов.

---

[1] Формат в скобках (частота использования: количество работ)

[2] L. Floridi The fight for digital sovereignty: What it is, and why it matters, especially for the EU Philosophy & Technology, 33, 2020, p. 372, pp. 369-378

В целом, под легитимностью суверенитета личности понимается способность взрослого человека контролировать себя и свою жизнь. Если использовать нормативный язык, то предполагается, что взрослые люди обладают рядом прав на управление самим собой[1].

Так, по мнению бывшего генерального секретаря ООН Кофи Аннана «…индивидуальный суверенитет - под которым я подразумеваю фундаментальную свободу каждого человека, закрепленную в Уставе ООН и последующих международных договорах - был усилен обновленным и распространяющимся осознанием прав личности. Когда мы сегодня читаем Хартию, мы более чем когда-либо осознаем, что ее цель состоит в защите отдельных людей, а не в защите тех, кто жестоко обращается с ними…»[2].

Подобную точку зрения высказывает С. Кутюр, который отмечает, что «цифровой суверенитет социальных групп неразрывно связан с их автономией посредством коллективного (а иногда и индивидуального) контроля над технологиями и цифровой инфраструктурой»[3].

Представляется, что цифровой суверенитет личности подразумевает легитимный контроль человека над цифровыми элементами своей жизни. Вопрос возникает о границах реализации данного легитимного контроля. Х. Конрад справедливо задается вопросом о границах законности такого контроля, направленного на уважение индивидуального суверенитета рассматриваемого лица[4]. Другими словами, какие границы контроля позволяют индивидууму управлять собой, осуществлять свою автономию. Подчеркнем тот факт, что как только будет установлен такой контроль, любые

[1] A. Peters Humanity as the A and Ω of sovereignty European Journal of International Law, 20 (3). 2009, pp. 513-544

[2] Kofi Annan, Two Concepts of Sovereignty, The Economist, 18 September, 1999.

[3] S. Couture, S. Toupin What does the notion of “sovereignty” mean when referring to the digital? New media and society, 21 (10) . 2019, pp. 2305-2322

[4] Niël Henk Conradie, Saskia K. Nagel. Digital sovereignty and smart wearables: Three moral calculi for the distribution of legitimate control over the digital. Journal of Responsible Technology. Volume 12, December 2022

попытки вернуться назад будут нелегитимными, поскольку нарушают индивидуальный суверенитет.

В данном контексте важно соблюдение определенной пропорции между государственным легитимным контролем и самоконтролем личности. Исследователи отмечают опасность «цифровой колонизации» как деятельности, при которой соблюдаются легитимные права государства и государственных органов, но при этом игнорируются права личности: «цифровая колонизация» подразумевает доминирующую культуру, обеспечивающую власть и влияние на культуры меньшинств, а также принимает форму суверенитета данных и пренебрежения правом собственности на цифровые данные и конфиденциальностью.

Вместе с тем, в некоторых исследованиях, например, И. Хартмана, эти аспекты социально-цифрового суверенитета рассматриваются через такие аспекты контроля, как эффективность и дивергенция. Данный автор подчеркивает социальную составляющую и выводит понятие социально-цифрового суверенитета, поскольку взаимодействие человека с цифровыми системами встроено в социальную среду[1].

2. *Конфиденциальность и ограничение информационных потоков*. Эти понятия также относятся к ограничению доступа к информации и персональным данным для третьих лиц и обеспечению защиты от форм потери контроля вместо полного отказа от технологии или услуги, предоставляемой технологическими гигантами [2].

3. *Многосубъектность.* Содержание понятия «цифровой суверенитет» должно быть определено в результате обсуждения различных заинтересованных сторон. Необходимо участие различных институтов

[1] Hartmann, E.A.: Digitale souveränität in der wirtschaft – gegenstandsbereiche, konzepte und merkmale. In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten, pp. 1–16. Springer, Heidelberg . 2021. https://doi.org/10.1007/978-3-662-62377-0_1

[2] Князева А.С. Биометрические персональные данные: интересы личности в контексте цифрового суверенитета В сборнике: IX Студенческий юридический форум "Парадигма права на современном этапе развития общества: от теории к практике". Сборник статей форума. В 4-х томах. Под общей редакцией А.В. Сладковой. Москва, 2023. С. 203-206.

гражданского общества, которые совместными усилиями разрабатывали бы принципы и методы использования информации, в том числе изучали бы способы, методы и принципы доступа и хранения данных, порядок их уничтожения и пр.

4. *Право собственности*. Цифровой суверенитет прямо связан с технологиями владения данными. Например, суверенитет медицинских записей: врач, создающий медицинские данные, или больница, хранящая их, не являются владельцами этой информации. Вся медицинская информация принадлежит пациенту, который контролируют свои данные и доступ к этой информации. Цифровой суверенитет – это, прежде всего, персональные данные, которые принадлежат пользователю, а не поставщику или социальным сетям в Интернете. Для использования этих данных третьими лицами необходимо согласие пользователя, и пользователь должен иметь возможность контролировать/отслеживать, как распространяется его информация.

5. Автономия действий. Существует связь между цифровым суверенитетом и автономией. На первый взгляд, между обоими понятиями есть определенные параллели. Они подразумевают особый вид свободы от внешнего вмешательства и позитивную свободу действовать по своему усмотрению.

Например, Дж. Дворкин понимает автономию как свободу от внешних ограничений плюс аутентичность, т.е. возможность определенного выбора, основанного на предпочтениях более высокого порядка[1]. В другом определении Т. Бошам и Дж. Чайлдресс[2] выделяют в автономии интенциональность, т. е. соответствие представлению агента о действии, понимание того, что он собирается сделать, и отсутствие контролирующих влияний, определяющих его действие.

[1] Dworkin G. Autonomy and behavior control. The Hastings Center Report 6(1), 1976, 23–28.
[2] Beauchamp TL and Childress JF. Principles of Biomedical Ethics. Oxford and New York: Oxford University Press. 2013, P. 104-105

В исследовании Ф. Никера и др.[1] отмечаются несколько иные условия автономии: принцип автономии требует, чтобы человек обладал возможностью самостоятельных действий (самоуправлением) посредством, во-первых, критического осмысления своих поступков и, во-вторых, чтобы его решения не подвергались чрезмерному внешнему влиянию. Таким образом, акцент на критическом осмыслении индивидуальных действий указывает на то, что автономия может быть формой руководства.

Подчеркнем, что для автономии важно отсутствие неправомерного внешнего влияния, давления, манипуляции, идеологического давления и всех иных подобных методов.

Кроме того, индивид должен осознавать последствия своих действий в сети, включая возможность утечки личной информации, кибербуллинга и других форм цифрового насилия, что требует от него активного подхода к защите своей конфиденциальности и безопасности, а также понимания рисков, связанных с использованием различных онлайн-сервисов. Индивид несет ответственность за формирование своего цифрового имиджа и репутации. В современном обществе информация о человеке может быть доступна широкой аудитории, и его действия в цифровом пространстве могут оказывать влияние на личные и профессиональные отношения. Поэтому важно осознавать, что каждое действие, каждое сообщение или публикация могут иметь долгосрочные последствия. Ответственность в цифровом пространстве также включает в себя активное участие в формировании и поддержании безопасной цифровой среды, что может проявляться в виде участия в общественных инициативах, направленных на защиту прав пользователей, а также в обучении других пользователей основам цифровой безопасности и грамотности.

Таким образом, анализ научных и практических подходов к термину цифровой суверенитет позволяет говорить о том, что цифровой суверенитет -

[1] F. Niker, G. Felsen, S.K. Nagel, P.B. Reiner Autonomy, evidence-responsiveness, and the ethics of influence The law and ethics of freedom of thought, Palgrave-Macmillan, Cham, 2021.

это сложное, многомерное и мультидисциплинарное понятие с широким спектром потенциальных коннотаций, связанное с конфиденциальностью и защищенностью персональных данных, легитимным контролем над персональной и приватной информацией, автономией деятельности граждан в цифровом пространстве и повышением их роли как потребителей и индивидуальных пользователей цифровых технологий и услуг, а также со свободой доступа к различным источникам информации и коммуникации.

В этой связи, представляется целесообразным предложить следующее определение цифрового суверенитета личности как способности и возможности индивида предпринимать сознательные, преднамеренные и независимые действия, принимать самостоятельные решения в отношении всех элементов цифровой жизни (персональных данных, цифровых профилей в социальных сетях и многочисленных интернет-сервисах, аппаратного и программного обеспечения, цифровых процессов, электронных услуг и гибридной инфраструктуры), а также совокупность прав, обязанностей и ответственности, возникающих в результате реализации такой способности. Новацией данного подхода является акцент на осознанности и самоконтролируемости действий в гибридном цифровом пространстве, ответственности и обязанностях индивида, который не только имеет право на контроль над своими данными и цифровыми профилями, но и несет ответственность за свои поступки.

Таким образом, цифровой суверенитет личности не только предоставляет индивидам права и возможности, но и требует от них активного и ответственного поведения в условиях постоянно меняющегося цифрового ландшафта.

1.2 Суверенная идентичность как основа цифрового суверенитета личности

Взаимосвязь людей, сервисов и технологий является определяющим аспектом цифровизации различных сфер современной жизни человека. Процессы цифровой трансформации возвели данные и информацию на небывалую высоту, сделали их основой любых инновационных проектов и технологий. Зачастую эти данные носят приватный и конфиденциальный характер, что обусловливает необходимость контроля человеком уровня их обмена, доступности и раскрытия.

Важнейшим элементом контроля над личными данными является управление идентификацией личности. Человек реализует идентификационные поведенческие паттерны через социальное самоопределение, защищенность его цифровой или онлайн-идентичности, цифрового профиля, что ведет к необходимости сохранения или достижения цифрового суверенитета. Чтобы реализовать общественные запросы в онлайн-идентификации, правительствами различных стран предлагается создавать цифровые удостоверения личности, позволяющие гражданам иметь большую конфиденциальность и безопасность при использовании цифровых платформ и сервисов.

Личностная и социальная идентификация в частных доменах и крупных цифровых платформах, таких как Yandex, Google и др., создает большую концентрацию персональных данных и онлайн-активности, что оказывает прямое влияние на цифровой суверенитет людей. В этом контексте безопасность данных, а также возможность отдельного человека контролировать уровень их доступности и раскрытия являются важными сдерживающими факторами обмена и раскрытия информации.

Чтобы снизить риски потери цифровой идентичности, существуют методы и технологии интеллектуального анализа данных с сохранением и повышением конфиденциальности. Такие методы скрывают конфиденциальную информацию о владельце данных и тем самым выборочно предоставляют информацию для использования. В большинстве случаев они не согласуются с желаемым и комфортным уровнем обеспечения

конфиденциальности, так как зачастую могут содержать идентифицируемые личные данные или тайну личной жизни и отслеживаться в Интернете.

Представляется, что цель цифрового суверенитета личности состоит не в том, чтобы отдельные данные о человеке были закрыты в разрозненных труднодоступных бункерах с ограниченным доступом и полезностью, а в том, чтобы предоставить человеку, как законному владельцу данных, право контролировать и решать их судьбу.

Подчеркивая желание и потребность людей взять под контроль и заявить о своем суверенитете над управлением цифровой идентичностью и любой информацией, позволяющей идентифицировать цифровое «я» человека в Интернете, в научном сообществе была предложена *категория «суверенная идентичность»* (self sovereign identity), которая стала «продолжением концепции суверенного самоуправления (self sovereign authority) - возможности независимого (суверенного) самоуправления как «врожденной» отличительной черты человеческого естества»[1], существующей вне рамок государственного администрирования. В цифровом контексте это перекликается с вестфальской моделью суверенитета, перенесённой на уровень индивидуума.

Данный термин требует анализа составляющих элементов, в частности:

- само: индивидуальный, собственный, личный, ориентированный на пользователя;

- суверенный: независимый, самоуправляемый, контроль, власть, автономия, наделение полномочиями, не спрашивая разрешения;

- идентичность: отличительный характер, индивидуальность, атрибуты и поведение, по которым можно узнать человека или вещь.

Уделим особое внимание идентичности - понятию, широко используемому в социологии. Согласно социологическому словарю Коллинза:

[1] E. Digital, « EIT Digital Report on European Digital Infrastructure and Data Sovereignty » . [Online]. 2020, Режим доступа: https://www.earto.eu/eitdigital- report-on-european-digital-infrastructure-and-data-sovereignty/

«Идентичность - это чувство «я» и преемственность «я», которое первоначально оформляется в детстве как отличение от родителей и семьи и обретение своего места в обществе»[1]. При этом формирование идентичности - это «постоянно возобновляемый процесс самоопределения и соотнесения с социальной реальностью, люди конструируют идентичности посредством социального взаимодействия и что эти взаимодействия всегда структурно укоренены»[2].

По мнению Н.Л. Поляковой «социальная идентичность - это такие аспекты индивидуальной «я-концепции», которые проистекают из членства в различных группах и оформляются в связи с идентификацией с такими социальными категориями как раса, гендер, религия, профессия, а также с другими, которые могут и не проявляться в означенных социальных контекстах»[3]. В отличие от социальных идентичностей, личностные идентичности считаются ключевыми, «действующими внутри и за пределами ролевых и социальных/групповых идентичностей, на которые претендуют люди, а также ситуаций, в которых эти ролевые и социальные/групповые идентичности встроены» [4].

С понятием «социальная идентичность» связаны также психологические концепции самосознания. В них это понятие определяется как выражение «множественной интегрированной идентичности», в которую включаются личностная и социальная идентичности, выступающие регуляторами социального поведения и самосознания[5].

Люди участвуют в социальных взаимодействиях, активируют и развивают собственные идентичности, реализуют эти идентичности таким

---

[1] Collins dictionary of sociology. 2005. Glasgow p.288

[2] Полякова Н.Л. «Идентичность» в современной социологической теории. 2016. Вестн. Моск. Ун-та. Сер. 18. Социология и политология. № 4

[3] Полякова Н.Л. «Идентичность» в современной социологической теории. 2016. Вестн. Моск. Ун-та. Сер. 18. Социология и политология. № 4. С. 57

[4] Stets, Jan E. and Peter J. Burke. "The Development of ldentity Theory." 2014, Advances in Group Processes 31:57-97

[5] См. подробнее: Психология самосознания. Хрестоматия. Самара: Издательство «Издательский дом «БАХРАХ-М», 2000.

образом, чтобы вызвать обратную связь, подтверждающую идентичность (что приводит к положительному эффекту); или опровергающую идентичность (что приводит к негативному эффекту)[1]. Эти процессы хорошо теоретически обоснованы, и исследователи продолжают проверять их эмпирически.

Тем самым, идентичность – это уникальное человеческое свойство. Это невыразимое «Я» самосознания, нечто, что понимается во всем мире каждым человеком, живущим в каждой культуре. Однако современное общество смешало эту концепцию идентичности. Сегодня страны и корпорации заменяют водительские права, карты социального страхования и другие выданные государством удостоверения личности с идентичностью. В этом может быть проблема, человек может потерять идентичность, если государство удалит его удостоверяющие данные и т.д.

Становление идентичности личности в цифровом мире происходит еще сложнее; и также подвергается централизованному контролю, который очень разбалансирован. В контексте цифрового общества идентичность становится не просто отражением социального положения, но и самостоятельным ресурсом, который может быть использован для накопления социального капитала. Идентификационное поведение, выраженное через профили в социальных сетях, цифровую репутацию и присутствие на различных платформах, становится важным компонентом социального капитала в его современном понимании.

Управление цифровой идентичностью требует определенных навыков и знаний, которые сами по себе становятся формой культурного капитала. Способность эффективно представлять себя в цифровом пространстве, управлять своим цифровым присутствием и защищать свои данные становится важным фактором социального успеха и доступа к ресурсам.

В этой связи теория социального капитала Бурдье приобретает новое измерение в условиях цифровизации. Социальные сети и цифровые

[1] Stets, Jan E. and Peter J. Burke. "Emotions and Identity Non-Verification." 2014, Social Psychology Quarterly 77:387-410. P.390

платформы создают новые формы «устойчивых сетей институционализированных отношений», которые Бурдье рассматривал как основу социального капитала. Однако характер этих отношений, механизмы их формирования и поддержания существенно изменились[1].

Взаимосвязь между теорией социального капитала Бурдье и концепцией цифрового суверенитета личности проявляется в нескольких ключевых аспектах. Во-первых, цифровой суверенитет можно рассматривать как необходимое условие для эффективного формирования и использования социального капитала в цифровой среде. Способность контролировать свои данные, управлять своей цифровой идентичностью и определять параметры своего цифрового присутствия непосредственно влияет на возможности накопления социального капитала.

Во-вторых, сам цифровой суверенитет становится формой капитала, который может быть конвертирован в другие формы капитала, включая социальный. Знания, навыки и ресурсы, необходимые для поддержания цифрового суверенитета, становятся ценным активом в информационном обществе и могут быть использованы для расширения социальных связей и доступа к ресурсам.

Цифровое неравенство, выражающееся в различном доступе к цифровым технологиям, навыкам и ресурсам, создает новые формы социальной дифференциации, которые влияют на распределение социального капитала. Как отмечал Бурдье, объем социального капитала зависит не только от размера сети связей, но и от объема других форм капитала[2]. В цифровую эпоху экономический капитал (доступ к технологиям) и культурный капитал (цифровые навыки) становятся важными факторами, определяющими возможности накопления социального капитала.

---

[1] Бурдье, П. Формы капитала / П. Бурдье // Экономическая социология. – 2002. – № 5. – С. 60–75.

[2] Бурдье, П. Формы капитала / П. Бурдье // Экономическая социология. – 2002. – № 5. – С. 67.

При этом «цифровые идентичности» разрознены и различаются в зависимости от цифровых платформ. Поскольку цифровой мир становится все более важным для мира физического, он открывает новые возможности, в частности, предлагает возможность переопределить современные концепции идентичности и позволить вернуть идентичность под контроль человека.

В этой связи концепт «суверенная идентичность», где пользователь играет центральную роль в управлении своей цифровой личностью («цифровой идентичностью»), приобретает особое значение. Это требует не только совместимости идентичности пользователя в нескольких местах (на разных цифровых платформах) с его согласия, но и реального контроля над собственными данными, создавая автономию действий пользователя[1].

Этот же факт отмечает С. Аллен: создавая суверенную идентичность, необходимо проявлять осторожность и защищать личность от финансовых и других потерь, предотвращать нарушения прав человека со стороны государства, регулирующих органов или транснациональных компаний и обеспечивать фундаментальные права человека[2].

Представляется, что концепция суверенной идентичности возникла не столько из научных текстов, сколько из социальных сетей, сообщений в блогах, журналах и интернет-форумах. Такие форумы определяли суверенную идентичность как набор этических принципов и идеалистическое видение, согласно которому люди становятся «владельцами своей собственной идентичности»[3].

В академической литературе М. Чизман определяет «владение» идентичностью и расширение прав и возможностей личности как элементы суверенной идентичности, направленные на «устранение необходимости в

---

[1] Васекин А.С. Суверенная идентичность как основа развития цифрового суверенитета личности: социологический ракурс В сборнике: Государственное управление и развитие России: цивилизационные вызовы и национальные интересы. Сборник статей Конференц-сессии ИГСУ РАНХиГС. Москва, 2024. С. 174-176.

[2] Allen, C. «The Four Kinds of Privacy». Life With Alacrity blog. /2015/04/the-four-kinds-of-privacy.html

[3] Allen, C. «The Path to Self-Sovereign Identity», Life With Alacrity, 2016.

мощных, централизованных институциональных структурах, предоставляя людям контроль и владение своей идентификационной информацией»[1]. Далее автор отмечает, что, поскольку различные способы использования людьми технологий цифровой идентификации не могут быть определены заранее, концепция суверенной идентичности потенциально может расширить не только возможности людей, лишенных гражданских прав, но и усилить контроль за ними регулирующих органов.

Терминология суверенной идентичности предполагает своеобразную концепцию суверенитета, а самосуверенитет, в свою очередь, связан с другими неформальными понятиями, такими как суверенитет данных, владение цифровой идентификацией и персональными данными[2].

Также интерес представляет исследование Х. Леонга, который провел частотный анализ статей в англоязычных источниках, где встречается термин суверенная идентичность. Так, наиболее часто встречающиеся и родственные слова в определении суверенной идентичности, включают в себя: «индивидуум, контроль, данные, пользователь, цифровой, принципы, согласие, учетные данные, способность, раскрытие, полномочия, автономия, безопасность, личное, право собственности, переносимость, прозрачность, минимум, корреляция, экосистема» и т. д[3].

Представляется, что суверенная идентичность трансформирует индивидуальную автономию, предоставляя инструменты для контроля над персональными данными и цифровым присутствием. Это влияние проявляется через такой ключевой аспект, как перераспределение власти, а именно перенос управления идентичностью с институтов (государство, транснациональные корпорации, организации) на самого индивида. Это позволяет ему не только

---

[1] Cheesman, M. «Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity», Geopolitics, 2020, pp. 1–26

[2] Ishmaev, G., «Sovereignty, privacy, and ethics in blockchain-based identity management systems», Ethics and Information Technology, 2020, pp. 1–14.

[3] Kheng Leong, Tan, Chi-Hung, Chi, and Kwok-Yan, Lam. Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization, 2022. Режим доступа // https://arxiv.org/abs/2202.10069

самостоятельно решать, кому и в каком объёме предоставлять доступ к персональным данным, но и укрепить суверенность психологического пространства как способность защитить физические, социальные и ценностные границы.

Таким образом, суверенная идентичность усиливает индивидуальную автономию, но ставит вопросы о балансе между личной свободой, социальной ответственностью и технологическими ограничениями.

Автором совместно с преподавателями кафедры организационного проектирования систем управления ИГСУ РАНХиГС была проведена фокус-групповая дискуссия, целью которой было определение особенностей формирования цифрового суверенитета личности. В первую группу экспертов входил профессорско-преподавательский состав Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), проводящий занятия по дисциплинам «Социология», «Цифровое право», «Социология цифрового общества», «Информационно-коммуникативные технологии в государственном и муниципальном управлении»[1], «Информационная безопасность», а вторую группу представляли специалисты в сфере информационных технологий и защиты персональных данных из государственных структур, бизнес-организаций, а также из организаций – лидеров цифровой трансформации в Российской Федерации (ПАО Сбербанк, ПАО ВТБ, ПАО Мегафон, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации и др.[2]).

Отметим результаты анализа ответов, полученных в ходе фокус-групповой дискуссии на *вопрос о независимости, автономности и контроле действий людей в цифровом пространстве.*

Так, первая фокус-группа отметила следующие аспекты.

[1] ФГ ЦСЛ-1
[2] ФГ ЦСЛ-2

Во-первых, существуют юридические и этические ограничения свободы действий. Елена, которая представила себя как юрист в сфере цифрового права, подчеркивает важность осознания границ, связанных с публикацией информации, и отмечает, что «многие пользователи осознают юридические и этические рамки, которые могут ограничивать их действия в сети, и в некоторой степени становятся более осторожными в своих действиях, что может быть связано с изменением социальных норм».

Предметом обсуждения стало наличие социальных норм и возможности саморегуляция в цифровом пространстве. Так, участник фокус-группы Екатерина отмечает, что «поведение пользователей в социальных сетях изменилось. И новые пользователи приходят с уже установленными нормами, что может указывать на саморегуляцию и самоуправление, когда пользователи заранее адаптируются к ожиданиям и нормам своих локальных групп, и это в определенной степени может ограничивать их свободу выражения мнения». Упоминание Екатерины о практике увольнения муниципальных служащих за лайки в социальных сетях подчеркивает влияние внешних факторов на поведение пользователей, что создает атмосферу страха и осторожности и ограничивает свободу действий.

Участники первой фокус-группы отмечали, что цифровое пространство создает множество социальных ролей и идентичностей, которые могут быть жестко отделены друг от друга. По мнению Екатерины, это «приводит к чувству дискретности и фрагментации личности и, с одной стороны, затрудняет ощущение цельности, с другой – предоставляет возможность для самовыражения и свободы».

Участник Игорь отмечает большое влияние технологий на повседневную жизнь и вне цифрового пространства. По его мнению, «это не столько бремя, сколько обыденное чувство, но тем не менее это создает ощущение ограничения их свободы действий в различного рода коммуникациях».

Участники второй фокус-группы отмечают, что анонимность в интернете не является абсолютной, их действия могут быть отслежены, и это влияет на их публикации. Так, участник Ольга подчеркивает, что «с развитием технологий и увеличением автоматизации процессов, уровень контроля и наблюдения за действиями пользователей возрос. Это создает ощущение, что свобода действий в цифровом пространстве уменьшилась по сравнению с прошлым».

Тем самым, участники фокус-групп имеют разные взгляды на то, что такое свобода и контроль в цифровом пространстве. Некоторые чувствуют себя свободно, пока соблюдают определенные личные ограничения, в то время как другие ощущают значительные ограничения из-за страха перед последствиями своих действий.

В этой связи можно отметить следующий вывод. С одной стороны, для использования концепции суверенной идентичности требуются цифровые навыки, что создаёт риски исключения маргинализированных групп[1], с другой - усиление контроля над данными может привести к добровольному отказу от анонимности в обмен на доступ к онлайн-платформам.

В этой связи можно выделить несколько ключевых принципов деятельности в цифровом пространстве, позволяющих обеспечить индивидуальный контроль и автономность как основу суверенной идентичности.

1. Существование. Любая суверенная идентичность в конечном итоге основана на существующем «Я»; она не может существовать полностью в цифровом формате, а только делает публичными некоторые ограниченные аспекты индивида.

2. Контроль. Индивиды (пользователи) должны самостоятельно контролировать свои идентичности и знать безопасные алгоритмы. Именно индивид имеет неограниченную власть над своей идентичностью, он может

[1] Майкова Э.Ю, Филиппченкова С.И. Риски автономии личности в социальной траектории. Власть. №3. 2015 С. 59

дать ссылку на идентификатор, обновить или даже скрыть его, выбирать публичный или приватный доступ. Это не означает, что пользователь контролирует все упоминания своей личности в Сети; другие пользователи могут ссылаться на пользователя, но это не должно быть определяющим аспектом в этой идентичности.

3. Доступность. Пользователь всегда должен иметь возможность легко, без посредников и третьих сторон получить все упоминания и другие данные, относящиеся к его идентичности.

4. Прозрачность. Информационные системы и алгоритмы, применяемые для администрирования и использования идентификационного контура, должны быть открытыми и прозрачными в части обновления, управления и функционирования. Алгоритмы должны быть бесплатными, с открытым исходным кодом, хорошо известными и максимально независимыми от какой-либо конкретной архитектуры. И любой должен иметь возможность изучить, как они работают.

5. Устойчивость. Идентичность должна быть долговечной. Предпочтительно, чтобы цифровые профили сохранялись навсегда или, по крайней мере, так долго, как пожелает пользователь. В быстро меняющемся мире Интернета эта цель может быть не совсем разумной, поэтому идентификационные данные должны сохраняться, по крайней мере, до тех пор, пока они не устареют из-за новых систем идентификации. Это не должно противоречить «праву на забвение»; пользователь должен иметь возможность распоряжаться своими идентификационными данными, если пожелает, а упоминания должны быть изменены или удалены по мере необходимости с течением времени. Для этого требуется четкое разделение идентичности и ее требований: их нельзя связывать навсегда.

6. Портативность. Информация и услуги, касающиеся идентичности, должны быть транспортабельными. Идентификационные данные не должны принадлежать отдельному стороннему объекту, даже если это доверенный объект, который, как ожидается, будет работать в интересах пользователя.

Проблема в том, что информация и услуги могут исчезнуть; и в Интернете в итоге так и происходит. Административные режимы могут измениться, пользователи могут переехать в другую юрисдикцию. Переносимые идентичности гарантируют, что пользователь сохраняет контроль над своей цифровой личностью несмотря на любые обстоятельства.

7. Совместимость. Идентичность должна быть максимально доступной для широкого использования. Идентичность не имеет особой ценности, если она работает только в ограниченных нишах. Цель системы цифровой идентификации 21-го века – сделать идентификационную информацию широко доступной, создать глобальную (международную) идентичность, не теряя при этом контроль со стороны пользователей.

8. Согласие. Пользователи должны дать согласие на использование своей идентичности. Любая система идентификации построена на совместном использовании цифровой личности и ее упоминаний. Однако обмен данными должен происходить только с согласия пользователя. Хотя другие пользователи, такие как работодатель, кредитная или страховая организация, могут запрашивать определенную информацию, пользователь все равно должен дать согласие на это. Необходимо обратить внимание, что это согласие не обязательно должно быть интерактивным, но оно все равно должно быть осознанным и понятным.

9. Минимализация. Раскрытие информации должно быть сведено к минимуму, необходимому для выполнения поставленной задачи. Например, если требуется указать только минимальный возраст, то точный возраст не следует раскрывать, а если запрашивается только возраст, то не следует раскрывать точную дату рождения. Этот принцип можно поддержать с помощью выборочного раскрытия, проверки диапазона и других методов с нулевым разглашением и т.д.

10. Защищенность. Права пользователей должны быть защищены. Когда возникает конфликт между требованиями системы идентификации и правами

отдельных пользователей, то цифровая платформа должна быть на стороне сохранения свобод и прав отдельных лиц.

11. Восстановление. Должны быть предусмотрены механизмы для восстановления и подтверждения личности в случае полной утраты учетных данных.

12. Отсутствие платы. Владение идентичностью должно быть бесплатным или с незначительными затратами.

13. Устойчивость. Цифровая инфраструктура и услуги должны быть устойчивыми в экологическом, социально-экономическом и технологическом плане.

Таким образом, анализ концепции «цифровая суверенная идентичность» позволяет сделать несколько выводов, связанных с процессами социальной идентификации и реализацией идентификационного поведения:

- цифровая суверенная идентичность как элемент цифрового суверенитета личности возникает не только благодаря государственным инициативам или действиям крупных сообществ, но и в значительной степени обусловлена внутренними потребностями граждан, связанными с ощущением уязвимости в цифровом пространстве и стремлением к самостоятельному выбору и контролю своих действий в онлайн-среде;

- цифровая суверенная идентичность представляет собой состояние, в котором индивид осознает и контролирует свою личную идентичность в контексте социальных, культурных и цифровых взаимодействий. Это состояние позволяет ему действовать и взаимодействовать в цифровой среде, сохраняя легитимный контроль над своей идентичностью и автономно управляя персональными данными в различных информационных сервисах. Такое состояние также подразумевает свободу выбора для индивида в отношении использования или неиспользования цифровых услуг, особенно в контексте небезопасных ситуаций, что соотносится с идеями С.А. Кравченко о критическом принятии цифровизации и способности критически оценивать и выборочно принимать технологические решения.

- основные принципы формирования цифровой суверенной идентичности включают существование, контроль, доступность, прозрачность, устойчивость, портативность, совместимость, согласие, минимализацию, защищенность и восстановление. Данные принципы подчеркивают важность активного участия индивидов в управлении своей идентичностью в процессах виртуализации и сетевизации в современном обществе.

- концепция цифровой суверенной идентичности подчеркивает активную роль индивида в формировании и управлении своей идентичностью как особым типом идентификационного поведения в условиях цифрового взаимодействия, что увеличивает осознанные адаптационные возможности для самовыражения и взаимодействия, но также накладывает ответственность за самоконтролированное обеспечение своей конфиденциальности и безопасности в гибридном цифровом пространстве.

1.3 Риски и угрозы цифровому суверенитету личности в цифровом пространстве

С развитием технологий цифровое пространство постепенно превращается из аппаратной межсетевой инфраструктуры в виртуальную социальную среду, в которой люди, бизнес и органы государственной власти взаимодействуют с помощью современных информационных и коммуникационных технологий. Как отмечал У. Бек, «… риски нас настигают: нас ими наделяет само развитие цивилизации»[1]. Еще одно важное замечание сделал в свое время И. Бестужев-Лада, отмечая наличие «категорического императива невозможности сохранения существующих тенденций развития человеческого общества на долгосрочную перспективу»[2].

[1] Бек. У. Общество риска. На пути к другому модерну. / Пер. с нем. В.Седельника и Н. Федеровой. М.: Прогресс- Традиция, 2000. С.26.
[2] Бестужев-Лада И. Альтернативная цивилизация: актуальность социологического осмысления // Социология на пороге XX века: Основные направления исследований. / Под ред. С.И. Григорьева (Россия), Ж. Коэтен-Хуттера (Швейцария). М.: РУСАКИ, 1999. С.36.

Как правило, процессы цифровизации инициируются крупными технологическими компаниями, контролирующими онлайн-платформы и большие массивы данных, где информация о пользователях легко доступна и может быть использована для целей анализа, в том числе алгоритмами машинного обучения, для улучшения существующих бизнес-процессов.

Нередко такие данные представляют собой индивидуальную (личную) и приватную информацию, онлайн-профили, действия и поведение человека, то есть «цифрового двойника» человека, связанного с жизнью в цифровом пространстве, в которой он хотел бы сохранить свою конфиденциальность и самостоятельно обеспечивать его доступность.

Отметим в этой связи значение работ С.А. Кравченко о влиянии социокультурного аспекта на социальные риски и безопасность. По его мнению, полипарадигмальный подход к изучению рисков позволяет понять и осмыслить глобальные тенденции развития современного общества[1]. Также он полагает, что смешение реального и виртуального миров порождает парадоксальное сосуществование реальных и инсценированных рисков, формируя девиантный характер сознания и поведения людей[2].

Сегодня современный человек вынужден оставаться в режиме «онлайн», поскольку только так он может оставаться активным членом общества[3]. Эта вынужденная интеграция в цифровое пространство создает риски потери цифрового суверенитета, которые требуют тщательного социологического анализа. Работы С.А. Кравченко предлагают методологическую основу для такого анализа через призму критического осмысления последствий цифровизации.

Существует множество ситуаций, условий и факторов при использовании цифровых технологий, которые приводят к полной/частичной потере контроля человека над конфиденциальной, приватной и

[1] См. Подробнее: Кравченко С.А. Социология риска и безопасности: учебник и практикум для вузов / С. А. Кравченко. — Москва : Издательство Юрайт, 2023. — 272 с.
[2] Кравченко С.А. Социология цифровизации: учебник для вузов. М.: Юрайт, 2021. С. 47
[3] Там же. С. 57

чувствительной информацией и нарушению прав человека в цифровом пространстве. Такие ситуации в настоящем исследовании мы будем называть рисками или угрозами цифровому суверенитету личности.

Перечислим и проведем краткий анализ некоторых из них.

Принудительное вовлечение граждан в цифровую среду.

Данная угроза отмечена в докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека[1]. Авторы доклада отмечают неоправданность принудительной цифровизации в сфере государственных и муниципальных услуг при проектировании и планировании национальных программ и стратегий, а также игнорирование прав граждан на сохранение традиционных способов взаимодействия с государством, а также медицинских, экономических и технологических ограничения некоторых людей.

Снижение правовой защиты в Интернете и ответственности государственных и частных структур.

Социальные платформы и сети оказывают огромное влияние на цифровой суверенитет личности в связи с их неограниченными возможностями по сбору личных и чувствительных данных, по блокировке и фильтрации контента, по манипуляции с уязвимыми группами населения и т.д. Вместе с тем, многие крупные социальные сети самостоятельно определяют политику, нормы и стандарты поведения для пользователей, обеспечивают соблюдение этой политики, регулируют и разрешают конфликты. Существует мнение, что такие сети представляют собой «квазигосударственный институт», обладающий многими основными характеристиками развитой политической системы.[2]

[1]Цифровая трансформация и защита прав граждан в цифровом пространстве: доклад Совета при Президенте РФ по развитию гражданского общества и правам человека(Москва, 2021 г.) [Электронный ресурс]. URL: http://president-sovet.ru/docs/ doc- lad_SPCh.docx

[2] Thorsten Busch, Fair Information Technologies: The Corporate Responsibility of Online Social Networks as Public Regulators 71, 2013. Режим доступа: https://www.alexandria.unisg.ch/228863/

Следовательно, социальные платформы обладают властью, представляющей собой определенную угрозу для реализации гражданских прав и свобод, что может привести к нарушению и цифрового суверенитета личности.

Хотя государство несет ответственность за нарушения прав человека и является основным носителем обязанностей по обеспечению прав личности, социальные платформы и крупные технологические компании в большинстве юрисдикций могут злоупотреблять своей властью. Тот факт, что социальные платформы являются корпоративными образованиями и могут причинить определенный вред правам человека, подтверждает необходимость признания их носителями обязанностей в области этих прав и привлечения к ответственности в случае нарушений.

Интернет-зависимость или проблемное использование Интернета.

По результатам опроса ВЦИОМ, роль Интернета в российском обществе воспринимается скорее неоднозначно: каждый второй опрошенный склоняется к мнению, что Всемирная сеть приносит нам и пользы, и вреда примерно в равной степени (48%).[1]

Амбивалентность цифровизации, о которой пишет С.А. Кравченко[2], проявляется в том, что цифровые технологии одновременно расширяют возможности человека и создают новые формы зависимости. Понимание этой амбивалентности является необходимым условием формирования стратегий сохранения цифрового суверенитета личности. Такие формы поведения в Интернете, как увлечение азартными играми, чрезмерное использование социальных сетей, «киберзапугивание» и «киберхондрия», могут иметь значимые последствия для психического и физического здоровья человека. С точки зрения цифрового суверенитета личности эта угроза может повлиять на

[1] https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-bez-opasnosti
[2] См. Подробнее: Кравченко С.А. Социология риска и безопасности: учебник и практикум для вузов / С. А. Кравченко. — Москва : Издательство Юрайт, 2023. — 272 с.

такие права, как право на здоровье и безопасность, а также права особо уязвимых групп, например, права ребенка.

Психологический дискомфорт, испытываемый пользователями при отсутствии доступа к интернету, может указывать на потерю контроля над своей цифровой идентичностью и взаимодействиями. Так, исследование ВЦИОМ[1] установило, что такие негативные ощущения при лишении доступа к сети, как подавленность и тревожность, испытывали 7% тех пользователей сети, кто вынужденно или по своей инициативе оказывался без интернета на долгий срок.

Цифровой суверенитет подразумевает, что индивид должен иметь возможность управлять своим присутствием в сети. Когда пользователи становятся зависимыми от интернета, они могут терять этот контроль, что приводит к негативным эмоциональным состояниям.

Интернет-зависимость может подрывать автономию личности, что является основным аспектом цифрового суверенитета. Если пользователи чувствуют себя подавленными или тревожными при отсутствии доступа к сети, это может свидетельствовать о том, что их способность принимать самостоятельные решения и контролировать свою жизнь в оффлайн-пространстве ослаблена.

«Культура отмены» и социальная инженерия.

Понятие «культура отмены» относится к акту социальной «отмены» человека, форме непроизвольного социального остракизма, вызванного действиями других, и направленного на то, чтобы обесценить мнения человека-жертвы и фактически его существование в некоторых сферах жизни общества[2]. В специальной литературе это явление обычно упоминается в контексте взаимодействия в социальных сетях (например, публикация верных

[1] ВЦИОМ. Новости: Цифровой детокс — 2023: о пользовании интернетом и отдыхе от него
[2] Шураева Л. Ю., Коринец А. Г. Социальный эффект "культуры отмены" в цифровом пространстве на примере поколений Y и Z // Вестник ГУУ. 2022. №12. URL: https://cyberleninka.ru/article/n/sotsialnyy-effekt-kultury-otmeny-v-tsifrovom-prostranstve-na-primere-pokoleniy-y-i-z (дата обращения: 02.05.2025).

или ложных комментариев о социально предосудительном поведении, таком как жестокое обращение с детьми или гендерное насилие). Что касается агрессии в цифровом пространстве, она является естественным продуктом анонимности Интернета. Культура отмены может влиять на цифровой суверенитет, поскольку она создает давление на индивидов и организации, заставляя их адаптироваться к общественным ожиданиям и нормам. В условиях культуры отмены пользователи могут чувствовать необходимость контролировать свои высказывания и действия в цифровом пространстве, чтобы избежать негативных последствий. Это может привести к самоцензуре и ограничению свободы выражения мнений, что противоречит принципам цифрового суверенитета. Взаимосвязь между культурой отмены и цифровым суверенитетом также поднимает вопросы этики и ответственности. Индивиды должны осознавать, как их действия в цифровом пространстве могут повлиять на других, и стремиться к конструктивному диалогу, а не к осуждению.

С социальной отменой личности могут быть связаны и методы социальной инженерии. Например, за счет использования искусственного интеллекта и информации из социальных сетей для создания клеветнической кампании посредством фейковых новостей в отношении определенного человека.

Риски, связанные с этическими и образовательными аспектами цифрового суверенитета личности.

Отсутствие должного образования в области этики цифрового взаимодействия может привести к серьезным рискам. Пользователи, не обладающие необходимыми знаниями, могут стать жертвами кибербуллинга, утечки данных или неправомерного использования своей информации. Это подчеркивает важность интеграции этических и образовательных аспектов в программы по цифровому суверенитету.

Чтобы обеспечить уважение прав человека, политические рекомендации и правовые нормы должны подкрепляться этическим образованием и обучением для различных целевых групп. Проблемы цифровой эпохи,

касающиеся прав человека, а также моральных и юридических норм, связаны, например, с анонимностью, с одной стороны, и технологическими возможностями сбора данных, с другой. Людей часто соблазняет анонимность, идея «отсутствия идентичности» или новая идентичность, и это влияет на их действия, которые часто отличаются от тех, которые были бы сделаны при личном взаимодействии. В цифровой среде, с соблазном анонимности, важно видеть роль этики, потому что этика или мораль, часто рассматривается как форма регулирования, которая имеет место, даже когда мы практически «одни» и осознаем, что никто не может видеть наши действия, только наша совесть[1].

Связь между цифровым суверенитетом и образовательными аспектами заключается в создании ответственной цифровой среды, где пользователи могут безопасно взаимодействовать, защищая свои права и идентичность. Образование в области этики и социальных норм поможет формировать более осознанное и ответственное общество, способное эффективно справляться с вызовами цифровой эпохи.

Риски для конфиденциальности и безопасности в Интернете, связанные с искусственным интеллектом.

Риски для цифрового суверенитета личности, связанные с искусственным интеллектом (ИИ), становятся все более актуальными в условиях стремительного развития технологий. Системы искусственного интеллекта присутствуют во многих сферах частной и общественной жизни. Например, в здравоохранении развивается роботизированная хирургия, внедряются ультразвуковые исследования сердца, распространяется клиническая диагностика на основе систем машинного обучения. Многие врачебные действия основаны на технологиях искусственного интеллекта с целью улучшения результатов лечения и повышения качества обслуживания пациентов.

[1] Tiina Pajuste (ed.), Specific Threats to Human Rights Protection from the Digital Reality (Tallinn: Tallinn University, 2022) P. 22

ИИ-системы часто требуют больших объемов данных для обучения и функционирования. Это может привести к утечкам персональной информации или ее использованию без согласия пользователей. Если данные не защищены должным образом, это может угрожать цифровому суверенитету личности[1].

Также существует множество юридических и этических проблем, касающихся использования систем искусственного интеллекта, например, в части замены человеческого фактора и доверия к полученным данным, выводам и т.п. Отмечается появление и развитие технологий «доверенного искусственного интеллекта». Обеспечение правовой базы для использования искусственного интеллекта и технологических инструментов – это непростой процесс. За этим скрывается множество рисков, в том числе связанных с защитой цифрового суверенитета личности, поскольку технологии искусственного интеллекта во многих случаях опережают формирование правовой базы, поэтому необходимо активно разрабатывать правовые основы внедрения искусственного интеллекта. В своей Белой книге по искусственному интеллекту Европейская комиссия прямо подчеркнула, что искусственный интеллект должен использоваться в сочетании с законодательством о правах человека, особенно с учетом защиты конфиденциальности и прав на данные.

Риски автоматизированного принятия решений, в том числе связанные с профилированием.

Прогресс в области алгоритмов машинного обучения облегчил использование данных как в государственном, так и в частном секторах для генерации/извлечения знаний, содействия принятию обоснованных решений, а впоследствии и для автоматизированного принятия решений. Автоматизированное принятие решений наряду с социальными и экономическими выгодами, может иметь негативные последствия и риски для

[1] Горбачева Т. А. Искусственный интеллект: риски и проблемы внедрения в Российской Федерации // Инновационная экономика: информация, аналитика, прогнозы. 2025. №1. С. 98

цифрового суверенитета личности, включая нарушения прав на неприкосновенность частной жизни, защиту персональных данных, ограничение свободы выбора, подрыв человеческого достоинства и автономии, увеличение предвзятости и дискриминации, а также социальную сегрегацию[1].

Системы машинного обучения могут принимать решения на основе алгоритмов, что может привести к ситуации, когда пользователи теряют контроль над своими данными и идентичностью. Например, алгоритмы могут автоматически обрабатывать и анализировать данные без участия человека, что может вызвать этические и правовые вопросы. Кроме того, такие системы могут наследовать предвзятости, присутствующие в данных, на которых они обучаются, что может привести к дискриминации определенных групп пользователей и угрожать их правам и свободам. Во многом это связано с непрозрачностью используемых алгоритмов, вероятностного характера рисков, связанных с качеством входных данных и т.п.

Риски конфиденциальности, связанные с воздушным наблюдением и дронами.

С развитием технологий дронов и беспилотных летательных аппаратов появляются различные новые возможности бизнес-моделей, такие как доставка посылок по воздуху, аэрофотосъемка, воздушное такси, дроновая журналистика и т. д. Современные дроны обладают рядом технологических возможностей, связанных с захватом и хранением большого объема данных, перехватом сообщений, автономным отслеживанием цели, распознаванием изображений и звуков, а также могут взаимодействовать с другими устройствами и сетью Интернет. В этой связи персональные и приватные данные, полученные с использованием дронов, не только могут быть легко доступны, но и анонимно собраны в тех областях, где люди обоснованно

[1] Чубукова С. Г. Защита прав субъекта персональных данных при автоматизированном принятии решений // Право и государство: теория и практика. 2020. №3 (183). С. 214 URL: https://cyberleninka.ru/article/n/zaschita-prav-subekta-personalnyhdannyh-pri-avtomatizirovannom-prinyatii-resheniy (дата обращения: 02.05.2025).

ожидают приватности и конфиденциальности[1]. Кроме того, дроны могут быть взломаны и перехвачены, в том числе с возможностью получения данных, хранящихся во внутренней памяти.

В этом контексте дроны как технология, обеспечивающая функциональность другим технологиям (например, камерам, звукозаписывающим устройствам, GPS), и позволяющая их использовать в совершенно новых условиях, предлагает дополнительные возможности наблюдения, что представляют угрозу цифровому суверенитету личности. Представляется, что массовое внедрение дронов в общественную жизнь, несмотря на все их преимущества, может привести к сдерживающему эффекту, когда люди чувствуют себя менее свободными и проявляют самосохранение путем ограничения своего поведения в общественных и приватных локациях.

Цифровая мобильность как угроза цифровому суверенитету личности.

Ряд прямых и косвенных угроз цифровому суверенитету стал очевидным в условиях развития глобального рынка мобильной связи. Мобильность становится быстро развивающимся трендом и одновременно увеличивает потенциальные угрозы цифровым правам и суверенитету личности. Даже во время Covid-19, когда передвижения и социальные контакты были строго ограничены, возникли соответствующие угрозы в отношении цифрового суверенитета личности из-за использования цифровых мобильных приложений.

Цифровые мобильные приложения зачастую используются для отслеживания территориальных передвижений, наблюдения за сотрудниками с помощью систем видеонаблюдения, сбора персональных данных, зачастую без явного согласия пользователей. При этом платформы цифровой мобильности, продвигающие мобильность как услугу, включают в себя широкий спектр транспортных поставщиков, часто базирующихся в разных

[1] Tiina Pajuste (ed.), Specific Threats to Human Rights Protection from the Digital Reality (Tallinn: Tallinn University, 2022) P. 29

странах или даже континентах, предлагающих варианты поездок на такси, автобусе, поезде, велосипеде или электросамокате, что создает проблему юрисдикционной защиты прав человека в зависимости от выбранных технологий. Появление больших баз данных в результате использования облачных сервисов, наряду с искусственным интеллектом, создает новые социальные и этические угрозы, например, общественной «слежки» в сочетании с рисками кибербезопасности. Поскольку большие наборы данных также продаются рекламным организациям за пределами национальных границ через различные платформы, очевидно, что для отдельных пользователей становится практически невозможным полностью обеспечить цифровой суверенитет[1].

Последнее связано с неизбежными трудностями в определении того, кто несет ответственность и должен противодействовать таким угрозам. Некоторые нормативные требования трудно реализовать на практике, особенно в транспортном секторе, например, ответственность при передаче данных мобильных услуг за пределы определенной юрисдикции.

Деплатформирование как принудительная блокировка или удаление пользователя.

Деплатформирование означает исключение пользователя из конкретной технологической платформы или социальной сети путем закрытия его учетных записей, запрета или блокирования использования системы или ее услуг, обычно из-за содержания его высказываний или блогов. В результате деплатформирования деятельность прерывается и ее результаты не могут быть доведены до целевой аудитории[2]. Это рассматривается как некая форма цензурирования, как одностороннее навязывание власти с помощью нерегулируемых «больших технологий». Эта форма ограничения дает

[1] Tiina Pajuste (ed.), Specific Threats to Human Rights Protection from the Digital Reality (Tallinn: Tallinn University, 2022) P. 29

[2] D. D'Orazio. Deplatforming in Theory and Practice: The Ann Coulter Debacle. In E. Macfarlane, eds., Dilemmas of free expression (Toronto: University of Toronto Press, 2022), p. 269.

возможность технологическим компаниям манипулировать общественным дискурсом.

Зачастую информационные платформы (социальные сети, торговые, платежные и сервисные платформы, услуги интернет-инфраструктуры (хостинг и т.п.) оправдывают удаление или блокировку пользователя и его контента нарушениями условий пользовательского соглашения. Представляется, что деплатформирование отрицательно влияет на цифровой суверенитет личности и такие права, как свобода выражения мнений, а также является крайней формой модерации контента и формой наказания за нарушение приемлемого поведения. Деплатформирование оправдано обращением к более широкой дискурсивной стратегии, которая пытается со временем остановить распространение потенциально вредных высказываний и сообщений[1] .

«Цифровой разрыв» как неравный доступ к технологиям, ведущий к росту неравенства.

«Цифровой разрыв» – это возникающая социальная дистанция между теми, кто имеет доступ к современным информационным и коммуникационным технологиям и владеет навыками, позволяющими ими воспользоваться, и теми, у кого нет доступа и соответствующих навыков[2]. «Цифровой разрыв» существует, например, между развитыми и развивающимися странами, городским и сельским населением, молодыми и пожилыми, образованными и менее образованными людьми, мужчинами и женщинами. И хотя доступ к компьютерам и Интернету продолжает расти, «цифровой разрыв» сохраняется, а в некоторых случаях даже увеличивается[3].

[1] D. D'Orazio. Deplatforming in Theory and Practice: The Ann Coulter Debacle. In E. Macfarlane, eds., Dilemmas of free expression (Toronto: University of Toronto Press, 2022), p. 269.

[2] Головенчик Г. Цифровой разрыв: причины возникновения, последствия и пути преодоления // Наука и инновации. 2021. №6 (220). С.33

[3]Цифровая трансформация и защита прав граждан в цифровом пространстве: доклад Совета при Президенте РФ по развитию гражданского общества и правам человека(Москва, 2021 г.) [Электронный ресурс]. URL: http://president-sovet.ru/docs/ doc- lad_SPCh.docx

Цифровой суверенитет личности подразумевает, что индивид имеет право контролировать свою цифровую идентичность и данные. Однако, если у человека нет доступа к интернету или необходимым технологиям, его возможности для реализации этого права значительно ограничены. Люди, находящиеся на «неправильной» стороне цифрового разрыва, могут не иметь возможности управлять своими данными, защищать свою идентичность или участвовать в цифровых взаимодействиях.

Риски суверенитету личности, связанные с умными носимыми устройствами.

Проблемы, которые порождают умные носимые устройства (телефоны, гаджеты и др.), можно разделить на две общие категории с важным замечанием, что границы между ними могут быть размытыми в части наличия угрозы автономии и конфиденциальности. Угроза автономии касается возможности того, что носимые технологии могут повлиять на автономность пользователя (или сопровождающих его лиц) таким образом, что снизят их способность принимать решения, действовать и взаимодействовать в соответствии со своими желаниями и целями. Угроза конфиденциальности связана с риском того, что носимые устройства могут собирать, обрабатывать или хранить данные, относящиеся к их пользователям, в том числе этически неприемлемым способом[1]. Носимые устройства обладают тремя особенностями, которые по отдельности и вместе увеличивают риски для цифрового суверенитета личности. В частности, их присутствие непосредственно на человеке (близость) в сочетании с их легкой доступностью (удобством) и вездесущностью (повсеместностью) может сделать их основными векторами вмешательства, влияющими на автономию пользователя и нарушающими его право на неприкосновенность частной жизни.

[1] Niël Henk Conradie, Saskia K. Nagel. Digital sovereignty and smart wearables: Three moral calculi for the distribution of legitimate control over the digital. Journal of Responsible Technology. Volume 12, December 2022

Пользователь становится социально и психологически зависимым от устройства, поэтому его собственные навыки и способность принимать решения могут атрофироваться, вплоть до такой степени, что автономия оказывается под угрозой. Такое явление часто называют «деквалификацией»[1]. Опасность зависимости возникает в двух случаях: во-первых, когда человек остается с ограниченной автономией в случаях недоступности технологий; во-вторых, когда зависимость приводит к уменьшению контроля других сфер жизни.

Что касается первого случая, то все меньше и меньше людей запоминают телефонные номера, перекладывая эту задачу на свои цифровые устройства, к которым все чаще относятся и будут причисляться умные носимые устройства. Это очень удобно и может быть интерпретировано как высвобождение когнитивных ресурсов для реализации более широких, более ценных и подлинных желаний и целей. Однако, при возникновении ситуации недоступности устройств, пользователи оказываются неспособными вспомнить информацию из-за отсутствия навыков в этой области. Это может варьироваться от легкого раздражения до серьезной опасности в зависимости от ситуации, в которой происходит сбой навыка. Подобный пример - потеря навигационных навыков из-за чрезмерной зависимости от спутниковых навигационных систем. Логика аналогична: когда спутниковая навигация недоступна, пользователь изо всех сил пытается найти дорогу, используя бумажные карты или альтернативные методы навигации.

Первые исследования, касающиеся влияния технологий на контроль других сфер жизни, показали, что растущее использование и зависимость от различных технологий – особенно тех, которые всегда под рукой и используются нерефлексивно – коррелируют с ухудшением способности

[1] McKinlay, R. Technology: Use or lose our navigation skills. Nature, 573–575, 2016. Режим доступа: https://doi.org/10.1038/531573a

концентрации внимания среди подростков[1]. Снижение этих способностей представляет собой угрозу способности агента развивать автономную социальную и психическую жизнь, препятствуя саморефлексивному рассуждению и идентификации подлинных желаний и целей. Это делает желания человека пугающе эндогенными и уязвимым для манипуляций. Такая реальность возлагает на разработчиков и поставщиков этих технологий эпистемический и моральный долг быть добросовестными и проявлять должную осмотрительность в доступе к косвенному влиянию на автономию зависимости от технологии. Это также требует, чтобы развитие цифрового суверенитета было направлено на минимизацию этого воздействия.

В этой связи каждый случай использования таких устройств должен рассматриваться в его собственном контексте. Зачастую отмечается необходимость развития цифрового суверенитета посредством модульных, понятных и удобных пользовательских соглашений, где четко определены линии контроля и автономии.

Приведенная систематизация рисков и угроз цифровому суверенитету личности не окончательна, должна постоянно обновляться в связи с динамичным внедрением процессов цифровизации в различные сферы общественной жизни. Такая систематизация может послужить теоретическим фундаментом для практической оценки цифрового суверенитета личности и выработки конкретных направлений по его формированию, где человеку как владельцу данных необходимо предоставить возможность реализовать свои права и нести ответственность за использование и обмен персональными данными с высоким уровнем безопасности.

Анализируя данные опроса ВЦИОМ «Интернет без опасности»[2] о восприятии рисков и угроз, связанных с использованием Интернета, можно

[1] S.E. Baumgartner, W.A. van der Schuur, J.A. Lemmens, F. te Poel The relationship between media multitasking and attention problems in adolescents: Results of two longitudinal studies Human Communication Research, 44 (1). 2018, pp. 3-30

[2] https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-bez-opasnosti

сделать следующие выводы. Мнения респондентов относительно угроз, связанных с Интернетом, остаются стабильными с апреля 2023 года по апрель 2024 года. Процент тех, кто считает, что Интернет «определенно может» представлять угрозу, не изменился (13%). Процент респондентов, считающих, что Интернет «скорее может» представлять угрозу, немного снизился с 29% до 27%. Это может свидетельствовать о некотором улучшении восприятия безопасности в Интернете или о том, что люди становятся более уверенными в своих способах защиты.

В целом, данные показывают, что восприятие угроз от Интернета остается относительно стабильным, но с небольшими изменениями, которые могут указывать на изменение общественного мнения и уровня осведомленности о безопасности в сети.

Для понимания значимости основных рисков и угроз цифровому суверенитету личности следует обратиться к результатам Экспертного опроса[1].

По мнению экспертов, ключевой проблемой остается обеспечение конфиденциальности и безопасности. Высокий уровень тревоги респондентов по поводу утраты конфиденциальности и персональных данных указывает на важность вопросов информационной безопасности в социальных структурах. Так, 61% экспертов отмечают высокую степень данного риска при действиях в цифровом пространстве. Можно утверждать, что постепенно начинает формироваться мнение, что необходимо повышенное внимание к защите личной информации, и это становится неотъемлемой частью социальной идентичности.

Риск мобильности, связанный с отслеживанием геолокации, отмечают 48% опрошенных. На наш взгляд, это подчеркивает происходящие изменения в восприятии пространства и личной свободы граждан в этом пространстве. Таким образом, мобильность и персональная геолокация, как ключевой аспект современного образа жизни, начинает восприниматься не только как

[1] ЭО ЦСЛ-2024

возможность, но и как источник риска, что может привести к перераспределению социальных ролей и норм. Высокая доля ответов, связанная с оценками возникающего цифрового неравенства (47% ответов респондентов), свидетельствует о том, что в социальной структуре формируются новые линии разлома, связанные с доступом к цифровым технологиям и информации, что может привести в дальнейшем к исключению определённых групп населения из многих социальных процессов и институтов.

Проблема низкой ответственности за распространение фейков (51% ответов) и цифровой буллинг (46% ответов) указывает на необходимость пересмотра роли социальных сетей в современном обществе. В то же время такие результаты являются отражением развития новых социальных институтов, направленных на регулирование и создание ответственности за контент.

Эксперты также отмечают риски, связанные с принудительным вовлечением в цифровую среду (47% ответов) и возникновением интернет-зависимости (43% ответов) как особо значимые в современном обществе. Это доказывает наше мнение, что цифровизация меняет процессы формирования идентичности и личных отношений. Люди начинают сталкиваться с новыми вызовами в построении социальных связей и взаимодействий. Данные экспертного опроса показали, что респонденты не придают большого значения рискам, связанным с деплатформингом (38% респондентов) и умными устройствами (32%). Возможно, это может свидетельствовать об их вовлеченности в эти формы социальной активности (например, онлайн-активизм).

Отметим, что материалы экспертного опроса показывают разницу в оценке рисков для цифрового суверенитета личности между двумя группами: специалисты из ИТ-сферы и работники других профессиональных групп.

Так, наиболее значимые различия между этими группами наблюдаются по рискам, связанным с нарушением конфиденциальности и использованием

персональных данных без согласия: абсолютное большинство (90%) экспертов из первой группы отмечают данные риски. В то время как только 44% респондентов из второй группы разделяют эту озабоченность.

ИТ-специалисты проявляют значительную обеспокоенность рисками, связанными с отслеживанием геолокации (69% против 37%) и принудительным отключением от цифровых платформ (68% против 21%). Сравнение восприятия рисков, связанных с цифровым неравенством и распространением ложной информации, также показывает существенные различия между этими двумя группами. Например, 58% ИТ-специалистов рассматривают цифровое неравенство как значительную проблему, а среди не ИТ-специалистов этот показатель составляет всего 40%.

Представляется, что такие различия во мнениях могут свидетельствовать о том, что знание и опыт в области информационных технологий формируют более высокую чувствительность к определенным угрозам, а также формируют профессиональное убеждение о необходимости внедрения более строгих норм и стандартов защиты данных, активизации деятельности государственных структур, правоохранительных органов и систем защиты прав потребителей по защите индивидов от неправомерной деятельности со стороны технологических компаний и обеспечения прав граждан на свободный доступ к информации и услугам.

Примечательно, что ИТ-специалисты менее обеспокоены рисками, связанными с искусственным интеллектом (38% против 48% у не ИТ-специалистов), а также с цифровым буллингом (28% против 40%). Это может также объясняться тем, что специалисты, работающие с технологиями, более уверены в своих знаниях и способностях справляться с этими рисками, чем их коллеги из других сфер. Однако это также может быть сигналом о необходимости повышения знаний о потенциальных угрозах, связанных с искусственным интеллектом.

Таким образом, возникающие риски цифровому суверенитету личности приводят к нарушению прав человека в цифровом пространстве и потере

контроля человека над конфиденциальной, приватной и чувствительной информацией. Принудительное вовлечение граждан в цифровую среду, снижение правовой защиты в Интернете, возникновение Интернет-зависимости, риски для конфиденциальности и безопасности в Интернете, связанные с искусственным интеллектом, – оказывают значительное влияние на цифровой суверенитет личности.

Результаты анализа Экспертного опроса показывают, что проблемы конфиденциальности, мобильности и цифрового неравенства становятся важными факторами, формирующими новый социальный контекст, в котором необходимо пересмотреть существующие нормы и правила взаимодействия в цифровом пространстве.

ГЛАВА II ХАРАКТЕРИСТИКА БАЗОВЫХ КОМПОНЕНТОВ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ

2.1 Цифровой статус как основа цифрового суверенитета личности

Стремительное развитие цифрового общества и цифрового пространства значительно повлияло на способы построения общественных отношений, сфер жизнедеятельности и социальных институтов, опирающихся на цифровые методы обработки информации. В этих условиях необходимо понимание структуры и содержания цифрового статуса личности, включающего онлайн-идентификацию, репутацию, формируемую через взаимодействие в социальных сетях и других цифровых платформах, а также особенности доступа к различным услугам и возможностям в цифровом мире.

Социальные сети, такие как ВКонтакте, Яндекс Дзен и т.д., играют ключевую роль в формировании цифрового статуса и предоставляют пользователям возможность взаимодействовать, делиться опытом и создавать контент. Подобные платформы способствуют формированию личного бренда и влияют на восприятие индивидов в обществе. Лайки, репосты и комментарии формируют оценку статуса, который может варьироваться от «влиятельного» до «маргинализированного». Важно отметить, что на цифровом уровне статус может быть искажен, так как он зависит от не всегда прозрачных алгоритмов платформ и социальных норм, которые могут варьироваться в зависимости от контекста[1].

Такой статус не только отражает личные достижения, но и служит основой для формирования цифрового суверенитета личности[2]. Для анализа взаимосвязи между цифровым суверенитетом и статусом полезно обратиться к социологическим теориям, таким как теория социального капитала Пьера Бурдье и теория идентичности. Так, теория социального капитала

[1] Зайцева С. А., Смирнов В. А. Аксиологический подход к понятию цифрового следа // Ноосферные исследования. 2021. № 3. С. 79-87

[2] Кислухина А.А. Актуальные проблемы цифрового правового статуса личности Бизнес-трансформация: управление улучшениями. 2023. № 4. С. 160-164.

подчеркивает значимость социальных связей и сетей для достижения успеха[1]. В контексте цифрового суверенитета, социальный капитал может быть представлен в виде подписчиков, взаимодействий и взаимопомощи в сети. Представляется, что люди с высоким уровнем социального капитала имеют больше возможностей для управления своим цифровым суверенитетом, так как они могут использовать свои связи для защиты личных данных и влияния на общественное мнение.

С точки зрения теории идентичности индивиды формируют свое «я» в зависимости от контекста и взаимодействий с другими. В цифровом пространстве идентичность может быть многослойной и изменчивой, что влияет на восприятие статуса. Управляя своим цифровым пространством, люди создают различные аспекты своей идентичности, что, в свою очередь, влияет на их статус и воспринимаемую репутацию.

Одним из конститутивных элементов цифрового статуса как основы цифрового суверенитета личности являются *цифровые права.* Обеспечение цифровых прав и наличие механизмов по их защите являются значимыми для формирования и развития цифрового суверенитета личности.

Так, в докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека отмечено, что «…в своей совокупности «цифровые» права формируют «цифровой суверенитет» личности, в основе которого лежит понимание, что человек не равен «цифровому вектору», то есть набору цифровых коэффициентов, вычисленных цифровыми платформами и помещённых в тот или иной реестр…»[2]

В этой связи целесообразным представляется рассмотрение основных прав человека, содержащихся в международном и российском

[1] Бурдье П. Практический смысл / Пер. с фр.: А. Т. Бикбов, К. Д. Вознесенская, С. Н. Зенкин, Н. А. Шматко; Отв. ред. пер. и Послесл. Н. А. Шматко. — СПб.: Алетейя, 2001 г. — 562 с.
[2] Цифровая трансформация и защита прав человека в цифровом пространстве . Доклад Совета при Президенте РФ по развитию гражданского общества и правам человека, М. 2021 https://ifap.ru/pr/2021/n211213a.pdf

законодательстве, и их реализации в информационном пространстве и Интернете.

В ст. 17 Конституции Российской Федерации отмечено, что «…в Российской Федерации признаются и гарантируются права и свободы человека и гражданина согласно общепризнанным принципам и нормам международного права…». Проведем сравнительный анализ основных прав и свобод человека, содержащихся в международных документах по основным правам и Конституции Российской Федерации (таблица 1, таблица 2).

Таблица 1. Международный пакт о гражданских и политических правах и Конституция РФ

Статьи Международного пакта о гражданских и политических правах	Будапештская конвенция 2001 года о киберпреступности	Хартия прав человека и принципов для Интернета 2011	Конституция Российской Федерации
Право на судебную защиту (статья 2)	Статья 15	Статья 18	Статья 46
Гендерное равенство (статья 3)	Статья 15	Статья 2c	Статья 19
Право на равенство перед законом (статья 14)	Статья 15		Статья 19
Право на неприкосновенность частной жизни (статья 17)	Статья 15	Статья 8	Статья 23
Свобода мысли, совести и религии (статья 18)	Статья 15	Статья 6	Статья 28
Свобода мнений и их выражения (статья 19)	Статья 15	Статья	Статья 29
Запрет пропаганды (статья 20)	Статья 15	Статья 5(e)	Статья 29
Право на мирные собрания (статья 21)	Статья 15	Статья 5(a), 6	Статья 31

Свобода объединений (статья 22)	Статья 15	Статья 6	Статья 30,
Права детей (статья 24)		Статья 12	
Право на участие в ведении государственных дел (статья 25)		Статья 15	Статья 32
Права меньшинств (статья 27)		Статья 2(b)	

Таблица 2. Статьи международного пакта об экономических, социальных и культурных правах и Конституция РФ

Статьи Международного пакта об экономических, социальных и культурных правах	Конституция Российской Федерации	Хартия прав человека и принципов для Интернета 2011
Гендерные права (статья 3)	Статья 19	Статья 2(c)
Право на труд (статья 6)	Статья 37	Статья 14
Справедливые условия труда (статья 7)	Статья 37	
Социальное обеспечение (статья 9)	Статья 39	Статья 4, Статья 17
Права детей (статья 10)		Статья 12
Право на образование (статья 13/14)	Статья 43	Статья 10
Право на участие в культурной жизни и пользование научным прогрессом (статья 15)	Статья 44	Статья 11

Первое упоминание о цифровых правах связано с Конвенцией о защите физических лиц в отношении автоматической обработки персональных данных[1], принятой Советом Европы в 1981 году, основной задачей которой была защита права на неприкосновенность частной жизни, как указано в статьях 11 и 12(2).

Конвенция о киберпреступности, подписанная в 2001 году (также известная как Будапештская конвенция), стала первым международным

[1] Council of Europe. Additional Protocol to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows. 2001. Режим доступа: https://www.refworld.org/docid/3dde11814.html

документом, целью которого является борьба с преступностью в киберпространстве[1]. Данный документ был ратифицирован сорока девятью государствами. Российская Федерация подписала Международный пакт о гражданских и политических правах (МПГПП), однако ее основное возражение против Будапештской конвенции связано не столько с правами человека, закрепленными в МПГПП, сколько с разрешением на «односторонний трансграничный доступ к данным, находящимся в распоряжении другой стороны, без уведомления властей государства, обладающего соответствующей информацией».

Позже была предложена Хартия прав человека и принципов для Интернета[2], которая значительно расширила понятие цифровых прав. В этой хартии доступ к Интернету и киберпространству признаётся правом человека. Глобальный опрос пользователей Интернета, проведённый в 2012 году, показал, что восемьдесят шесть процентов респондентов согласились с тем, что Интернет следует рассматривать как основное право человека.

Хартия подчеркивает, что доступ к Интернету и его использование становятся всё более необходимыми для реализации прав человека, включая право на свободу выражения мнения, право на образование, право на свободу мирных собраний и ассоциаций, право на участие в управлении страной, право на труд, а также право на отдых и досуг. Право на доступ к Интернету напрямую связано со всеми перечисленными правами человека.

Это право должно быть обеспечено для всех без каких-либо ограничений, за исключением случаев, предусмотренных законом и необходимых в демократическом обществе для защиты национальной безопасности, общественного порядка, общественного здоровья, нравственности, а также прав и свобод других лиц. Право на доступ к

---

[1] ETS No. 185. Convention on Cybercrime, Council of Europe, 2001 [online] Режим доступа: https://www.refworld.org/docid/47fdfb202.html

[2] Internet Rights & Principles Coalition. *The Charter of Human Rights and Principles for the Internet, 2014* Режим доступа: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf.

Интернету включает в себя такие аспекты, как качество обслуживания, то есть уровень предоставляемых услуг должен развиваться в соответствии с технологическим прогрессом; свободу и возможность выбора систем и программного обеспечения, включающую использование совместимых коммуникационных инфраструктур и протоколов; обеспечение охвата цифровыми технологиями, то есть возможность использовать разнообразные цифровые средства массовой информации, коммуникационные платформы и устройства для управления и обработки информации.

В этом документе отмечается, что интернет является общим достоянием. Его архитектуру следует защищать и развивать, чтобы она служила средством свободного, открытого, равного и недискриминационного обмена информацией, общения и культурой.

Споры о том, является ли право на интернет основным правом человека, продолжаются до сих пор. Сторонники этой позиции часто приводят в доказательство статью 19 Всеобщей декларации по правам человека (далее – ВДПЧ): «Каждый имеет право на свободу мнений и их выражения; это право включает свободу беспрепятственно придерживаться своих убеждений, а также свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от границ».

Можно сказать, что первоначальные конвенции по правам человека не устарели в эпоху цифровых технологий. Например, в Замечании общего порядка № 16, изданном в 1966 году о конфиденциальности, не хватает явного упоминания современных проблем, в том числе: «запрет нецелевого массового наблюдения, массового сбора и хранения метаданных; доступ спецслужб/правоохранительных органов к коммуникационным данным, хранящимся у сторонних провайдеров и интернет-компаний, в том числе в «облаке»; отношения между частными компаниями и правительствами; сбор биометрических данных (например, с помощью отпечатков пальцев, программного обеспечения для распознавания лиц) и трансграничный доступ к закрытым для общественности данным в обход требований договоров о

взаимной правовой помощи»[1]. Тем не менее, было бы невозможно явно учесть и предвидеть все эти проблемы до их возникновения. Таким образом, на усмотрение политиков ООН и государств необходимо тщательно интерпретировать и интегрировать современные проблемы с фундаментальными правами в соответствии с этими конвенциями.

Статья 19 ВДПЧ часто используется в качестве инициатора признания Интернета правом человека, но она не единственная. Согласно статье 27 ВДПЧ, люди имеют право пользоваться своей культурой, религией, языком и участвовать в научных достижениях и их результатах. Эта часть показывает дальновидность, которой обладали первоначальные авторы ВДПЧ.

Резолюция Совета ООН по правам человека «Интернет и права человека», принятая в 2012 году, включает «поощрение, защиту и реализацию прав человека в Интернете», но не упоминает Интернет как право. В свою очередь Дж. Томальти [2] предлагает четко разграничивать права человека между «законными правами человека», например, сформулированными во ВДПЧ, МПГПП и МПЭСКП, и естественными правами, например, «моральными правами»[3]. Естественные права являются базовыми и присущими человечеству, независимо от общества или эпохи. Согласно этой логике, доступ к Интернету как коммерческому продукту не является естественным правом, поскольку доступ не может быть универсальным для всех людей.

Как указано ранее, доступ к Интернету и его использование предполагает несколько естественных прав, включая свободу выражения мнений, ассоциаций, информации и образования. Интернет, несомненно,

---

[1] Watt, E. The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7), 2017, pp.773-799. P.788

[2] Tomalty, J. Is There a Human Right to Internet Access?. *Philosophy Now*, [online] (118), 2017, pp.6-8. Режим доступа: https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access

[3] Tomalty, J. Is There a Human Right to Internet Access?. *Philosophy Now*, [online] (118), 2017, pp.6-8. Режим доступа: https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access.

является важным средством реализации существующих прав человека и, следовательно, способствует улучшению условий жизни человека. Однако доступ к Интернету - это просто средство реализации прав[1]. Скорость изменения технологий делает невозможным прогнозирование технологических разработок и того, как эти разработки повлияют на гражданские права и права человека.

В Хартии по цифровым правам в Интернете перечислены несколько важных прав, включая право на конфиденциальность в сети, которое включает в себя следующие аспекты:

а) Национальное законодательство о конфиденциальности. Государства обязаны разработать и внедрить комплексные регуляторы для защиты конфиденциальности и личных данных граждан. Эти рамки должны соответствовать международным стандартам прав человека и защиты потребителей, а также обеспечивать защиту от нарушений конфиденциальности со стороны как государственных, так и частных учреждений.

б) Политики и настройки конфиденциальности. Политики конфиденциальности и настройки всех онлайн-сервисов должны быть легко доступны, а управление настройками конфиденциальности должно быть интуитивно понятным и удобным для пользователя.

в) Стандарты конфиденциальности и целостности ИТ-систем. Право на неприкосновенность частной жизни должно поддерживаться стандартами конфиденциальности и целостности информационных технологий, которые обеспечивают защиту от несанкционированного доступа к системам.

г) Защита виртуальной идентичности. Каждый человек имеет право на защиту своей виртуальной идентичности. Это включает в себя защиту цифровых подписей, имен пользователей, паролей, PIN-кодов и TAN-кодов от

[1] Урсу В.А. Права и свободы человека как элемент конституционно-правового статуса личности в цифровой телекоммуникационной среде В сборнике: Россия - Евразия - мир: интеграция - развитие - перспектива. Материалы XIV Евразийского экономического форума молодежи. В 4-х томах. Екатеринбург, 2024. С. 158-160.

использования или изменения без согласия владельца. Важно уважать виртуальную идентичность человека, однако это право не должно использоваться во вред другим.

д) Право на анонимность и использование шифрования. Каждый имеет право на анонимное общение в Интернете и на использование технологий шифрования для обеспечения безопасного, конфиденциального и анонимного взаимодействия.

е) Свобода от наблюдения. Каждый имеет право общаться без произвольного наблюдения или перехвата, включая поведенческое отслеживание, профилирование и киберпреследование. Любое соглашение о доступе к онлайн-сервисам, содержащее согласие на слежку, должно четко обозначать характер этого наблюдения.

ж) Свобода от клеветы. Никто не должен подвергаться незаконным посягательствам на свою честь и репутацию в Интернете. Каждый имеет право на защиту закона от таких вмешательств. Однако защита репутации не должна использоваться как предлог для ограничения свободы слова за пределами допустимых рамок.

К цифровым правам личности также можно отнести *право на забвение*. Существует несколько точек зрения на право на забвение. В одних случаях, в зависимости от юрисдикции, такое право признается судом, в других отмечается, что истинная информация не может быть удалена. Однако разделяется мнение о том, что концепция права на забвение вызывает серьезные опасения в отношении цифрового суверенитета личности.[1]

В контексте социологии концепция права на забвение представляет собой важный аспект взаимодействия между индивидуумом и обществом, особенно когда речь идет о доступности информации. Право на забвение касается информации, доступной общественности, и в этом контексте необходимо учитывать право общества на получение адекватной информации по вопросам, имеющим общественный интерес. Это право становится важным

[1] Jones, M. L. Ctrl + Z: The Right to Be Forgotten, NYU Press. 2016, pp.1-3.

фактором, поскольку «неактуальная» информация может восприниматься по-разному. То, что для одного человека может казаться незначительным, для другого может иметь критическое значение.

Кроме того, право на забвение предоставляет индивиду возможность требовать удаления информации, которая, хотя и является правдивой и легально опубликованной, может быть в настоящее время некорректной для конкретного человека[1]. Это поднимает вопрос о том, как мы можем сбалансировать индивидуальные интересы с общественными. Необходимо рассмотреть, должны ли мы игнорировать право общества на получение информации в пользу переоценки идентичности человека в цифровом пространстве.

Следует также отметить, что право на забвение может быть использовано как инструмент цензуры. Оно может затруднить поиск важной информации о конкретных лицах, что может иметь серьезные последствия для общественного дискурса. Операторы поисковых систем, как правило, определяют, какие запросы на удаление информации удовлетворять, а какие отклонять, зачастую без четких и прозрачных стандартов. Например, Google разработала руководство для реализации права на забвение, которое основывается на интерпретациях национального законодательства, но отсутствие единых критериев может привести к произвольным решениям.

Таким образом, предоставление частным компаниям роли арбитров в вопросах свободы слова и права на забвение представляет собой риск. Это сочетание может ограничить свободу выражения мнений, поскольку операторы поисковых систем могут не иметь достаточной подготовки для выполнения этих функций. В результате, необходимо разработать четкие стандарты и критерии, которые позволят найти баланс между правом на

[1] Мушаков В. Е.. Совершенствование российского законодательства о цифровых правах человека: публично-правовой аспект. Научный вестник Омской академии МВД России, 2022

забвение и свободой слова, чтобы обеспечить как индивидуальные права, так и общественные интересы.

Представляется, что перечень цифровых прав, связанных с киберпространством и Интернетом, постепенно расширяется. Принимаются новые хартии и конвенции, и в каждой из них упоминается все больше прав для обеспечения дополнительной защиты цифрового суверенитета личности.

В этом контексте заслуживают внимания результаты анализа Экспертного опроса.[1] Так, ответы респондентов на вопрос «На ваш взгляд, какие из нижеперечисленных прав и свобод должны соблюдаться в сети Интернет?» можно разбить на следующие группы: «высокая поддержка» (более 70 %), «средняя поддержка» (50-70%) и «низкая поддержка» (менее 50%).

Таким образом, высокий уровень поддержки прав на безопасность и защиту персональных данных (83.8% опрошенных отметили данную позицию) свидетельствует о том, что респонденты осознают важность защиты своей личной информации в цифровом пространстве, что может быть связано как с растущими угрозами кибербезопасности и утечками данных, так и неясными законодательными инициативами и мерами по защите данных со стороны органов государственной власти. Также респонденты поддержали право на неприкосновенность частной жизни в цифровом пространстве (74.6%), что указывает на то, что респонденты ценят свою приватность и стремятся к защите от вмешательства со стороны государства и частных компаний. Это может говорить о растущем недоверии к технологиям и платформам, которые собирают и обрабатывают личные данные.

Высокий уровень поддержки права равенства перед законом (76.9%) подчеркивает важность для экспертов справедливости и равенства в цифровом пространстве, что может указывать на осознание респондентами необходимости защиты своих прав в ситуациях, когда цифровые технологии могут создавать неравные условия для различных групп населения.

[1] ЭОЦСЛ-2024

Вторая группа прав, которые можно отнести к правам «со средним уровнем поддержки», включает право на защиту потребителей в Интернете (68.6% экспертов отметили данную позицию), право на доступ в Интернет (соответственно 65.8%), свободу совести и религии (58% выбрали данное право). Это говорит о том, что респонденты считают эти права важными, но не столь критичными для своего цифрового суверенитета.

Наименьшую поддержку у экспертов получили такие права, как свобода мысли, мнений и их выражения (50.6%), право на труд (42.8%), право на образование и право на мирные собрания (40.5%). Это может свидетельствовать о том, что респонденты, возможно, менее осведомлены о значении этих прав в контексте цифрового суверенитета личности или считают их менее актуальными в условиях современного цифрового взаимодействия.

Если проводить анализ ответов на данный вопрос в разрезе профессиональной деятельности, то можно отметить некоторое отличие восприятия цифровых прав у ИТ-специалистов от других специальностей. Это относится, прежде всего, к таким правам, как право на справедливое судебное разбирательство, право на труд, свобода совести и религии (рис. 1).

Как показало исследование, восприятие и понимание прав личности в цифровом пространстве различается у представителей разных профессий. Для ИТ-специалистов более значимы право на защиту потребителей в Интернете, право на безопасность и защиту персональных данных, равенство перед законом и неприкосновенность частной жизни. То есть для данных специалистов наиболее значимы права, связанные с их профессиональными действиями. А для представителей иных профессиональных групп важными являются право безопасность и защиту персональных данных, право на доступ в Интернет, равенство перед законом, неприкосновенность частной жизни. При этом, для всех профессиональных групп менее значимы право на мирные собрания и свободу объединений, право на труд.

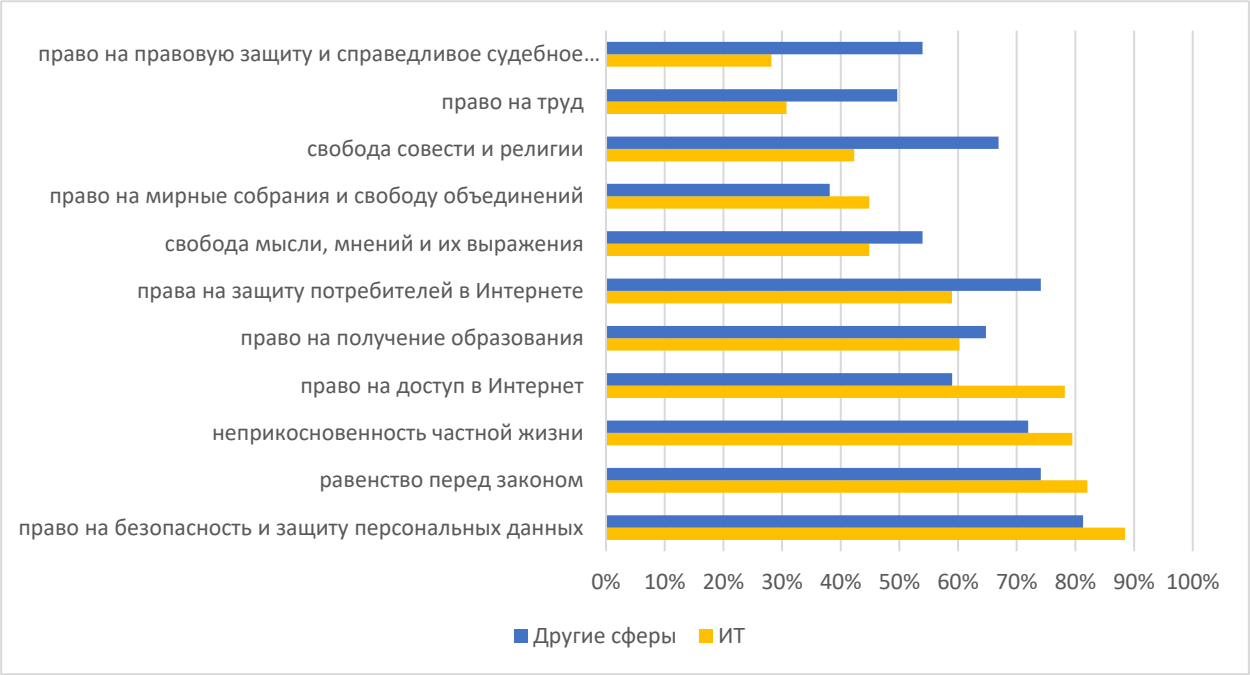

Рисунок 1. Ответы респондентов по вопросу о цифровых правах

Еще одним значимым элементом цифрового статуса как основы формирования цифрового суверенитета личности являются *обязанности и ответственность граждан в Интернете*. Так, в статье 29 ВДПЧ отмечено, что «каждый человек имеет обязанности перед обществом, только в котором возможно свободное и полное развитие его личности»[1].

На наш взгляд, основные обязанности каждого перед сообществом включают следующие положения:

а) Уважение прав других: каждый обязан и несет ответственность уважать права всех людей в онлайн-среде.

б) Ответственность обладателей власти перед другими пользователями: обладатели власти должны ответственно осуществлять свою власть, воздерживаться от нарушения прав человека и уважать их, защищать и реализовывать их в максимально возможной степени.

Так, анализ результатов Экспертного опроса[2] на вопрос «Какие обязанности могут быть у человека в сети интернет?» позволяет сделать

[1] Всеобщая декларация прав человека - Декларации - Декларации, конвенции, соглашения и другие правовые материалы // https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
[2] ЭОЦСЛ-2024

несколько выводов о характере ответственности и обязанностей при деятельности в цифровой среде. Ответы респондентов целесообразно разделить на несколько групп по степени важности. Наибольшую поддержку среди респондентов получили обязанности, касающиеся уважения прав и свобод других людей (82.9% экспертов отметили данную позицию), что говорит о высоком уровне осознания ими важности этических норм в цифровом пространстве. Респонденты понимают, что соблюдение прав других является основой для безопасного и справедливого взаимодействия в сети.

Обязанность не распространять недостоверную и ложную информацию (88.4%) также получила значительную поддержку, что указывает на растущее беспокойство о влиянии фейковых новостей, дезинформации и психологического воздействия на общественное мнение и личность. Респонденты осознают, что их действия в сети могут иметь серьезные последствия. Высокий уровень поддержки получила обязанность не использовать персональные данные других пользователей без их согласия (83.8%), что подчеркивает важность конфиденциальности и защиты личной информации и может отражать растущее недовольство по поводу практик сбора данных со стороны компаний и платформ.

Вторая группа обязанностей, отмеченных в ходе экспертного опроса, связана с требованиями соблюдения государственной политики информационной безопасности (70%), недопущением распространения противозаконных идей (74.1%), а также с необходимостью «не оскорблять других людей и не клеветать» (73.2%). Они получили несколько меньшую поддержку, что может указывать на неоднозначное отношение респондентов к государственному регулированию в сфере цифровых технологий.

Низкая поддержка обязанностей, связанных с соблюдением авторских прав (57,6%) и обязательной авторизацией в сети (18.4%), может указывать на низкую осведомленность респондентов о важности этих аспектов в части формирования цифрового суверенитета и на общее недовольство по поводу

сложных, часто непонятных правил, установленных цифровыми платформами.

Интерес представляет мнение экспертов, которые входили в состав 2-х фокус-групп, относительно наличия обязанностей при взаимодействии в цифровой среде[1].

Представитель первой фокус-группы «Преподаватели»[2] Елена отмечает, что хотя в Конституции провозглашается право на свободу информации, на практике это право ограничено различными законами, включая законодательство о дипфейках и защите репутации. Это подчеркивает важность понимания того, что права в цифровом пространстве не являются абсолютными и могут быть ограничены. Участник Екатерина подчеркивает, что ее восприятие прав и обязанностей зависит от социальных ролей. «Ощущение наших возможностей, прав и обязанностей сильно зависит от того, какую социальную роль мы сейчас проигрываем». В этой связи можно сделать вывод о том, что права и обязанности в цифровом пространстве могут восприниматься иначе в зависимости от социальной ситуации. Многие участники не видят значительной разницы между правами и обязанностями в реальной жизни и в цифровом пространстве, что может указывать на то, что для них цифровое пространство является продолжением реальной жизни, и они применяют те же моральные и социальные нормы.

Участник Людмила говорит о цифровом разрыве, особенно третьего порядка, что подчеркивает важность цифровой грамотности и способности формировать свою цифровую реальность, а также подчеркивает существование неравенства в доступе к цифровым ресурсам и возможностям. Участники фокус-группы активно обсуждали новые формы контроля в цифровом пространстве и то, как это влияет на их ощущение гражданства, и как права и обязанности могут изменяться в зависимости от того, как люди взаимодействуют с цифровыми технологиями.

[1] ФГ ЦСЛ-1, ФГ ЦСЛ-2
[2] ФГ ЦСЛ-1

Анализируя ответы второй фокус-группы «Специалисты ИТ»[1] на вопрос о правах, обязанностях и ответственности в цифровом пространстве, можно выделить несколько ключевых тем и тенденций, отражающих мнения участников.

Большинство участников согласны с тем, что права и обязанности в цифровом пространстве аналогичны тем, что существуют в реальной жизни. Они подчеркивают, что юридические нормы и моральные обязательства должны быть одинаковыми в обоих контекстах. Однако было высказано мнение, что в цифровом пространстве эти права и обязанности могут быть менее формализованы и защищены. В процессе дискуссии ИТ-специалистами отмечалось, что размещение информации в интернете делает её публичной, и это требует более серьезного подхода к публикациям, комментарии и посты могут быть доступны широкой аудитории, что накладывает дополнительные обязательства на их авторов.

Некоторые участники данной фокус-группы указывали на технические аспекты цифрового пространства, которые влияют на соблюдение прав и обязанностей. Например, возможность блокировки пользователей в мессенджерах рассматривается как преимущество цифрового общения, в то время как в реальной жизни такая возможность отсутствует. Участники отмечали ответственность владельцев социальных сетей и платформ за контент, размещаемый пользователями, и подчеркивали, что с недавних пор законодательство стало более строгим в отношении ответственности за информацию, размещаемую на публичных площадках. Несмотря на наличие прав, участники выражали сомнения в их реальном соблюдении в цифровом пространстве и указывали на сложности с защитой персональных данных и на то, что пользователи могут столкнуться с трудностями в случае нарушения их прав. Многие участники считают, что необходимо создать более четкие правила и нормы для цифрового пространства, чтобы обеспечить защиту прав пользователей и повысить ответственность за нарушения.

[1] ФГ ЦСЛ-2

Представляется, что важным фактором формирования цифрового суверенитета личности являются возможности и наличие *государственного контроля над цифровым контентом*. Так, одним из распространенных инструментов государственного регулирования в России является выделение и блокировка так называемых неблагонадежных сайтов, а также формирование «черного списка» веб-сайтов. Число подобных веб-сайтов с годами неуклонно растет, и особенно явная положительная динамика наблюдалась после начала специальной военной операции.

Поправки к федеральному законодательству предоставили Роскомнадзору и другим ведомствам право принимать решения относительно того, какой контент является основанием для блокировки веб-сайта. Роскомнадзор ведет список заблокированных веб-сайтов, которые содержат изображения насилия над детьми, контент, связанный с наркотиками, информацию о самоубийствах, нарушениях авторских прав, информацию о несовершеннолетних жертвах преступлений, а также призывы к публичным акциям или митингам.

Одновременно были приняты более строгие законы, ограничивающие анонимность в Интернете, в частности, путем блокировки VPN и требования к другим телекоммуникационным приложениям связывать пользователей с их личной информацией в соответствии с поправкой 2018 года к Закону об информации, информационных технологиях и информационной безопасности (см. Таблицу 3).

Таблица 3. Развитие регуляторов в России

Регулятор	Дата закона/постановления	Цель/актуальность
Закон об иностранных агентах	Июль 2012 г.	Зарегистрированные НПО, которые получают определенное иностранное финансирование и участвуют в деятельности, считающейся политической, подлежат проверкам и отмечаются как иностранные агенты в официальных заявлениях.
Закон об информации, информационных технологиях и информационной безопасности (поправки)	Февраль 2014	Позволяет без суда блокировать сайты, провоцирующие массовые беспорядки, экстремистские или террористические действия. Расширяет рамки первоначального закона, который боролся с детской порнографией. Последняя поправка требует, чтобы зарубежные интернет-сервисы хранили пользовательские данные в России.
Закон о блоггерах	август 2014 г	Все интернет-издания, включая блоги и персональные страницы социальных сетей с более чем 3000 читателями в день, должны зарегистрироваться в Роскомнадзоре
Закон о средствах массовой информации (поправки)	Январь 2016 г.	Запрещает иностранным гражданам и организациям владеть более чем двадцатью процентами акций любого российского СМИ.
Закон о новостных агрегаторах	январь 2017 г.	Требует, чтобы поисковые системы Интернета с более чем одним миллионом пользователей в день проверяли правдивость информации, считающейся общественно важной, перед ее распространением. Новости, признанные ложными, должны быть удалены с веб-сайтов, иначе им грозят финансовые санкции, что приводит к самоцензуре в частных компаниях и свободному потоку онлайн-информации.
Закон Яровой (пакет поправок)	Июль 2018 г.	Обязывает онлайн-сервисы предоставлять ключи шифрования для Интернета, требует от телекоммуникационных провайдеров хранить записи в течение шести месяцев и предоставлять любую информацию, запрашиваемую на федеральном уровне, вводит тюремное заключение сроком до семи лет за призывы к терроризму в Интернете или его оправдание.
Федеральный закон о персональных данных	Март 2023	Введение новых правил, которые касаются: уничтожения персональных данных; новых полномочий Роскомнадзора при передаче персональных данных за границу; оценки вреда утечки персональных данных.
Закон об информации, информационных технологиях и информационной безопасности (поправки)	Июль 2023 г.	С 1 октября у владельцев соответствующих информационных ресурсов появятся новые обязанности, в частности: не допускать применение рекомендательных технологий, нарушающих права и законные интересы граждан и организаций, или использовать их для предоставления информации с нарушением законодательства; не допускать предоставление информации с применением рекомендательных технологий без информирования пользователей об их применении на информационном ресурсе
Закон об информации, информационных технологиях и информационной безопасности (поправки)	Июль 2023 г.	Запрет регистрации на российских сайтах с помощью иностранной электронной почты. Авторизацию можно будет пройти по номеру телефона российского оператора, через Госуслуги, Единую биометрическую систему или другую российскую информсистему.

В этой связи целесообразно привести результаты опроса ВЦИОМ[1] «Интернет: Возможности или угрозы?». Так, увеличение числа респондентов, которые «совершенно не согласны» с утверждением о том, что регулирование ущемляет их свободу (с 15% до 26%), может указывать на растущее понимание того, что регулирование может быть необходимым для защиты их цифрового суверенитета. Пользователи могут осознавать, что определенные меры регулирования могут помочь им сохранить контроль над своими данными и защитить их от злоупотреблений. Увеличение числа тех, кто «совершенно согласен» с тем, что регулирование может ущемлять свободу (с 9% до 13%), может быть связано с опасениями по поводу чрезмерного контроля и слежки со стороны государства или корпораций.

Связь между восприятием регулирования Интернета и цифровым суверенитетом личности подчеркивает важность осознания пользователями своих прав и свобод в цифровом пространстве. Это также указывает на необходимость создания эффективных механизмов регулирования, которые будут защищать личные данные и права пользователей, не ущемляя их свободы.

Несмотря на множество различных угроз защите прав человека со стороны цифровой среды, тенденция цифровизации продолжится и ее воздействие на социальный статус человека представляется значительным.

Таким образом, результаты анализа цифрового статуса как основы адаптационного потенциала личности и ее цифрового суверенитета подчеркивают сложность и многогранность определения прав и обязанностей в цифровом пространстве, важность выделения социальных норм и типов идентификационного поведения, а также необходимость учитывать вопросы доступа и контроля в контексте цифровых прав. Это может служить основой для дальнейших исследований в области социологии личности в информационной пространстве и формирование адекватной модели цифрового суверенитета личности.

[1] https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-vozmozhnosti-ili-ugrozy

2.2 Уровни и структура цифрового суверенитета личности

Наличие множества коннотаций и возможностей использования термина цифровой суверенитет диктует необходимость применения системного подхода к определению уровней и структуры цифрового суверенитета личности.

Из имеющихся подходов в зарубежной литературе можно отметить исследования В. Витпаля, который выделил три уровня цифрового суверенитета для системного понимания этого термина[1]. А именно:

Гражданский уровень, в том числе:

- Цифровой суверенитет в социальных сетях;

- Цифровое участие в бизнесе (например, открытые инновации) и науке (например, открытая наука/гражданская наука);

- Социально-цифровой суверенитет как суверенное отношение и компетентность людей в отношении социально и культурно укоренившихся цифровых технологий.

Общественный уровень (сообщества и организации):

- Цифровой суверенитет как технологический суверенитет в области цифровых технологий, например, в контексте Индустрии 4.0, в отношении оценки, использования и производства таких технологий;

- Защита данных и конфиденциальность в цифровом мире труда;

Государственный уровень:

- Противоречия между большими данными/наукой о данных и традиционной статистикой в описании и анализе политической и социальной реальности;

- Действия государства по поддержанию и развитию цифрового суверенитета в контексте «сфер» личности, организации/компании,

[1] Wittpahl, V. (Hrsg.): Digitale Souveränität. Bürger, Unternehmen, Staat. Springer Vieweg Open, Berlin, 2017.

национального государства и межправительственных/ международных/ транснациональных субъектов;

- Обучение цифровым навыкам как главное требование цифрового суверенитета на всех уровнях.

Дж. Поле также предполагает[1], что существуют индивидуальное, государственное и экономическое измерения, пересечение которых и попадает под понятие цифрового суверенитета. Организация BITKOM, представляющая ИТ-отрасль в Германии, использует многоуровневый подход к описанию цифрового суверенитета, но позиционирует его как многосубъектные отношения между потребителями, корпоративными пользователями и государством[2] .

По мнению И. Фрайса, цифровой суверенитет представляет собой системный всеобщий процесс, охватывающий государство, организацию и личность во взаимном интерактивном и межреляционном контексте, с учетом широты концепции и междисциплинарного подхода. Он отмечает, что различные уровни цифрового суверенитета нельзя рассматривать изолированно друг от друга[3].

Представляется, что многомерный подход к цифровому суверенитету лучше отражает его конститутивные признаки и мультипредметность.

И. Хартман использует социотехнический подход к описанию цифрового суверенитета личности с учетом характеристик рабочей среды[4], выделяя три подсистемы, а именно:

---

[1] Pohle, J.: Digitale Souveränität. Handbuch Digitalisierung in Staat und Verwaltung . 2020. Режим доступа:https://doi.org/10.1007/978-3-658-23669-4_21-1

[2] BITKOM: Digitale Souveränität. Datenschutz und Datensicherheit - DuD 42(5), 294–300 2018. https://doi.org/10.1007/s11623-018-0944-y

[3] Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., Wendeborn, T. Towards a Layer Model for Digital Sovereignty: A Holistic Approach. In: Hämmerli, B., Helmbrecht, U., Hommel, W., Kunczik, L., Pickl, S. (eds) Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723. Springer, Cham. 2023, Режим доступа: https://doi.org/10.1007/978-3-031-35190-7_9

[4] Ulich, E.: Arbeitssysteme als soziotechnische Systeme – Eine Erinnerung. J. Psychol. Alltagshandelns 6(1), 2013, pp.4–12

- человек с его мотивами и потребностями, а также его знаниями и навыками, которые можно приобрести посредством формального, неформального и неофициального обучения;

- технология в ее сложной структуре, состоящей из разнородных (механических, электронных, оптических, жидкостных, аппаратных и программных) подсистем, функционирующей в сложной сети самых разнообразных, пространственно-распределенных систем;

- организация с возможностями разделения и совмещения задач, структурной и процессной организации, с сосуществованием формальных и неформальных организационных структур, а также организационной и корпоративной культуры.

Он предлагает объединение этих трех социотехнических подсистем с тремя критериями цифрового суверенитета организации, относящихся к контролю прозрачностью, дивергенцией и эффективностью (таблица 4)

Таблица 4. Цифровой суверенитет и контроль

Аспект контроля	Человек	Технология	Организация
Прозрачность	Базовые цифровые знания/цифровая грамотность	Прозрачность/объяснимость	Прозрачность задач и полномочий по принятию решений
Эффективность	Специальные знания, связанные с выполнением задач (цифровые)	Техническая надежность, прочность, отказоустойчивость	Разделение и совмещение задач, социальная поддержка
Дивергенция	Междисциплинарные (цифровые) специальные знания, компетенции как склонности к самоорганизации.	Возможности вмешательства в систему на выбираемых уровнях регулирования.	Простор для принятия решений, активности и действий

Что касается людей, то прозрачность рабочей среды, характеризуемой алгоритмическими системами, зависит от базовых знаний индивидов в

области ИТ, которые позволяют понять основы работы. Глубокие профессиональные, в том числе специфические, связанные с информационными технологиями, знания и навыки определяют степень эффективности и безопасности действий сотрудников. Наконец, дивергенция зависит от широких, а возможно, и междисциплинарных квалификаций, которые позволяют следовать несколькими качественно различными путями к определенным целям.

Организация во всех ее формальных и неформальных аспектах может способствовать прозрачности контроля за счет ясности в отношении задач, ролей и полномочий. Степень социальной поддержки других факторов, которая, в свою очередь, зависит как от организационной структуры, так и от корпоративной культуры, влияет на эффективность индивидуальных и коллективных действий.

Технологии могут в той или иной степени способствовать прозрачности как через свою внутреннюю структуру, так и через интерфейс человека и технологии. Вклад технологий в повышение эффективности отражается в высокой технической надежности, прочности и устойчивости. В конечном счете, дивергенция оказывает положительное влияние на технологии, например, если она предлагает варианты выбора.

При работе с понятием цифрового суверенитета на любом уровне возникает вопрос о его измерении. Для оценки цифрового суверенитета доступны различные методы и критерии.[1] Например, Д. Байшев и П. Крун предлагают три направления оценки: конфиденциальность, кибербезопасность и стратегия[2]. В некоторых работах для решения данной задачи использовалась методология оценки надежности систем

[1] Jenderny, S., Foullois, M., Kato-Beiderwieden, A.-L., Bansmann, M., Wöste, L., Lamß, J., Maier, G. W., Röcker, C.: Development of an instrument for the assessment of scenarios of work 4.0 based on socio-technical criteria. In: PETRA '18: Proceedings of the 11th PErvasive Technologies Related to Assistive Environments. Conference June 2018

[2] Baischew, D., Kroon, P., Lucidi, S., Märkel, C., Sörries, B.: Digital sovereignty in Europe: a first benchmark. Wik-consult report, Bad Honnef, 2020. Режим доступа: http://hdl.handle.net/10419/251539

искусственного интеллекта (ALTAI), которая разделена на семь областей критериев с соответствующими группами подкритериев[1]. Так, для оценки цифрового суверенитета личности можно, например, использовать следующие из них, в частности:

- Человеческая деятельность и возможность контроля (человеческая активность и автономия, индивидуальный контроль и надзор);
- Конфиденциальность и управление данными;
- Прозрачность (прослеживаемость, объясняемость);
- Разнообразие, недискриминация и справедливость.

При исследовании такого комплексного феномена как цифровой суверенитет личности был использован методологический подход Г.В. Осипова, характеризующийся системностью и многоуровневым анализом социальных явлений. Предложенная им структуризация предоставляет методологический и практический каркас для исследования цифрового суверенитета личности, позволяя рассматривать его одновременно на макроуровне общественных отношений и на микроуровне индивидуальных практик взаимодействия с цифровой средой.

Важным аспектом методологии Г.В. Осипова является внимание к социальной структуре и социальным отношениям, социально-территориальным общностям, социально-политической организации общества и социальным институтам[2]. Применительно к проблематике цифрового суверенитета личности данный подход позволяет анализировать, как различные социальные институты и структуры взаимодействуют в процессе формирования и регулирования цифровой среды, влияя на степень суверенитета отдельной личности.

---

[1] AI HLEG: High-level expert group on artificial intelligence: the assessment list for trustworthy artificial intelligence (ALTAI). https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment, 2020.

[2] Рабочая книга социолога / Под общ. ред. и с предисл. Г. В. Осипова. Изд. 5-е. — М.: Книжный дом «ЛИБРОКОМ», 2009. — 480 с. Источник: https://www.isras.ru/publ.html?id=6535

Также для исследования цифрового суверенитета личности целесообразно использовать концепцию научно-исследовательских программ, предложенную Н. Лакатосом[1], согласно которой, любая такая программа состоит из «жесткого ядра» (фундаментальных предположений) и «защитного пояса» (вспомогательных гипотез), а также включает положительную и отрицательную эвристику. Применительно к изучению цифрового суверенитета личности «жестким ядром» может выступать представление о фундаментальном праве личности на автономию в цифровом пространстве и контроль над своими данными. «Защитный пояс» может включать различные концепции реализации этого права в зависимости от культурного, политического и технологического контекста.

Методология Лакатоса позволяет интегрировать различные теоретические подходы к цифровому суверенитету, оценивая их прогрессивность и регрессивность с точки зрения способности объяснять и предсказывать новые факты. Это создает основу для формирования целостной научно-исследовательской программы изучения цифрового суверенитета личности, способной развиваться и адаптироваться к меняющимся реалиям цифровой эпохи.

Для проверки основной гипотезы исследования автором был проведен экспертный опрос, в котором приняли участие 217 человек из различных сфер общественной жизни (таблица 5). Из представителей ИТ блока, в том числе занимающихся вопросами информационной безопасности и защитой персональных данных - 78 человек[2].

Таблица 5 . Место работы и сфера деятельности респондентов

Сфера	Количество человек	Процент
ИТ структура	78	36%
ВУЗ	41	19%
финансовая организация, страховая организация, бизнес-организация	45	21%

[1] Sfetcu, Nicolae, Imre Lakatos, the Methodology of Scientific Research Programmes - An Overview (February 22, 2019). Режим доступа: https://ssrn.com/abstract=4693820
[2] ЭОЦСЛ-2024

государственный и муниципальный орган	31	14%
общественная организация	13	6%
частная организация, индивидуальный предприниматель	9	4%

Для проведения социологического исследования цифрового суверенитета личности важно было разработать вопросы, которые позволяют выявить уровни и механизмы формирования цифрового суверенитета личности и влияние основных акторов: личности, организации и государства – на формирование этого суверенитета.

Анкета, посвященная исследованию цифрового суверенитета личности, включает в себя несколько ключевых переменных и смыслов, которые можно выделить для социологического исследования. Вот основные из них:

- *Определение цифрового суверенитета*.

Вопросы 1 и 2 направлены на выявление мнений респондентов о том, что составляет основу цифрового суверенитета личности. Предполагались как готовые определения из научных источников (вопрос «По вашему мнению, что входит в основу цифрового суверенитета личности?», так и возможность собственной формулировки (*вопрос «Продолжите предложение: Я буду обладать цифровым суверенитетом, если: «)*.

- *Восприятие цифрового суверенитета* (*вопрос «Как вы, в целом, оцениваете защищенность вашего личного цифрового суверенитета?»*).

Вопрос 3 позволяет оценить, как респонденты воспринимают свою защищенность в цифровом пространстве, что может отражать уровень доверия к существующим системам защиты и осознание рисков в цифровой среде. Оценка защищенности в цифровом пространстве отражает не только личные ощущения респондентов, но и их уровень информированности о существующих угрозах и мерах защиты. Это может помочь выявить пробелы в знаниях и осознании рисков.

- *Права и свободы в интернете*.

Вопросы 5 и 6 касаются прав и обязанностей пользователей в интернете, что позволяет понять, какие права респонденты считают важными и какие обязанности они готовы на себя взять. Исследование прав и обязанностей пользователей в интернете помогает выявить, как респонденты воспринимают баланс между свободой и ответственностью в цифровом пространстве, а также проанализировать их взгляды на этические нормы и социальные контракты, существующие в онлайн-среде.

- *Риски для цифрового суверенитета личности.*

Вопрос 15 позволяет оценить, как респонденты воспринимают риски, связанные с Интернетом и доступом к технологиям. Оценка таких рисков позволяет понять восприятие респондентами уровня угроз для своего цифрового суверенитета и может быть связана как с их личным опытом, так и с общими трендами государственной информационной политики, информационной безопасности, а также с готовностью респондентов принимать меры для минимизации этих рисков.

- *Влияние человека на свой цифровой суверенитет* (*вопрос «Что конкретно может сделать человек для защиты своего цифрового суверенитета?»*).

Вопросы 4 и 12 исследуют, какие действия респонденты готовы предпринять для сохранения своего цифрового суверенитета. Анализ индивидуальных действий позволяет понять, насколько респонденты осознают свою ответственность за защиту своего цифрового суверенитета. Это может включать в себя как проактивные меры (например, использование сложных паролей), так и реактивные (например, реагирование на утечки данных). Важно также оценить, насколько респонденты готовы обучаться и повышать свою цифровую грамотность.

- *Влияние организации на цифровой суверенитет личности* (*Вопрос «Что конкретно должны сделать информационные платформы и организации для сохранения цифрового суверенитета личности?»*).

Вопросы 9, 10 исследуют наличие систем защиты цифрового суверенитета в организациях, где работают респонденты. Вопрос 11 касается контроля за

рабочей деятельностью, что может указывать на уровень доверия между работниками и работодателями, а также на восприятие приватности. Анализ организационных мер защиты позволяет понять, как работодатели и организации воспринимают свою роль в обеспечении цифрового суверенитета сотрудников. Результаты такого анализа позволят оценить, насколько организации готовы инвестировать в защиту данных и соблюдение прав своих сотрудников.

- Влияние государства на цифровой суверенитет личности (Вопрос «Что должно, на ваш взгляд, сделать государство для защиты цифрового суверенитета личности?»).

Вопрос 14 исследует, какие меры могут быть предприняты государством для защиты цифрового суверенитета личности. Оценка восприятия респондентами роли государства в защите цифрового суверенитета может помочь выявить ожидания граждан от государственных структур и включать в себя как поддержку и защиту прав пользователей, так и регулирование технологий и платформ, что важно для формирования доверия к государственным институтам.

Анкета охватывает широкий спектр вопросов, связанных с цифровым суверенитетом личности, включая индивидуальные, организационные и государственные уровни, и позволяет получить комплексное представление о восприятии и понимании цифрового суверенитета, его формировании и защиты, что в дальнейшем позволило разработать Модель цифрового суверенитета личности.

Анализ результатов анкеты.

По мнению респондентов, основу цифрового суверенитета должны составлять следующие элементы:

«защищенность от отслеживания персональной геолокации» (88%),

«установление ответственности за разглашение и утечку персональных данных» (86%),

«защищенность от мошенников, использующих персональные данные, применяющих цифровой буллинг, распространяющих фейки (ложную информацию) (83%).

Наименьшее число экспертов высказались за «возможность независимо и самостоятельно высказывать свое мнение в цифровом пространстве» (69%), возможность выбора информационного контента в Интернете (77%), обязательное согласие человека при использовании его цифрового профиля и персональных данных (78%).

Тем самым, по мнению респондентов, в основе цифрового суверенитета преобладающими являются принципы безопасности, защищенности и конфиденциальности, что свидетельствует о необходимости развития социальных институтов, отвечающих за защиту прав граждан в цифровом пространстве, за адаптацию к новым вызовам, связанным с цифровизацией.

Низкий интерес респондентов к возможности независимо и самостоятельно высказывать свое мнение в цифровом пространстве и к выбору информационного контента указывает на то, что в обществе, возможно, не сформировалось понимание возможности существования автономного и независимого цифрового пространства и Интернета.

Представляется, что такое отсутствие баланса между вопросами безопасности и автономией говорит о недостаточной работе социальных институтов по этому направлению.

Интересны также результаты анализа открытого вопроса респондентам в части условий обладания цифровым суверенитетом. Представляется целесообразным провести анализ данного ответа с помощью частотного анализа и модели LDA, используемой в машинном обучении (LDA - Латентное размещение Дирихле).

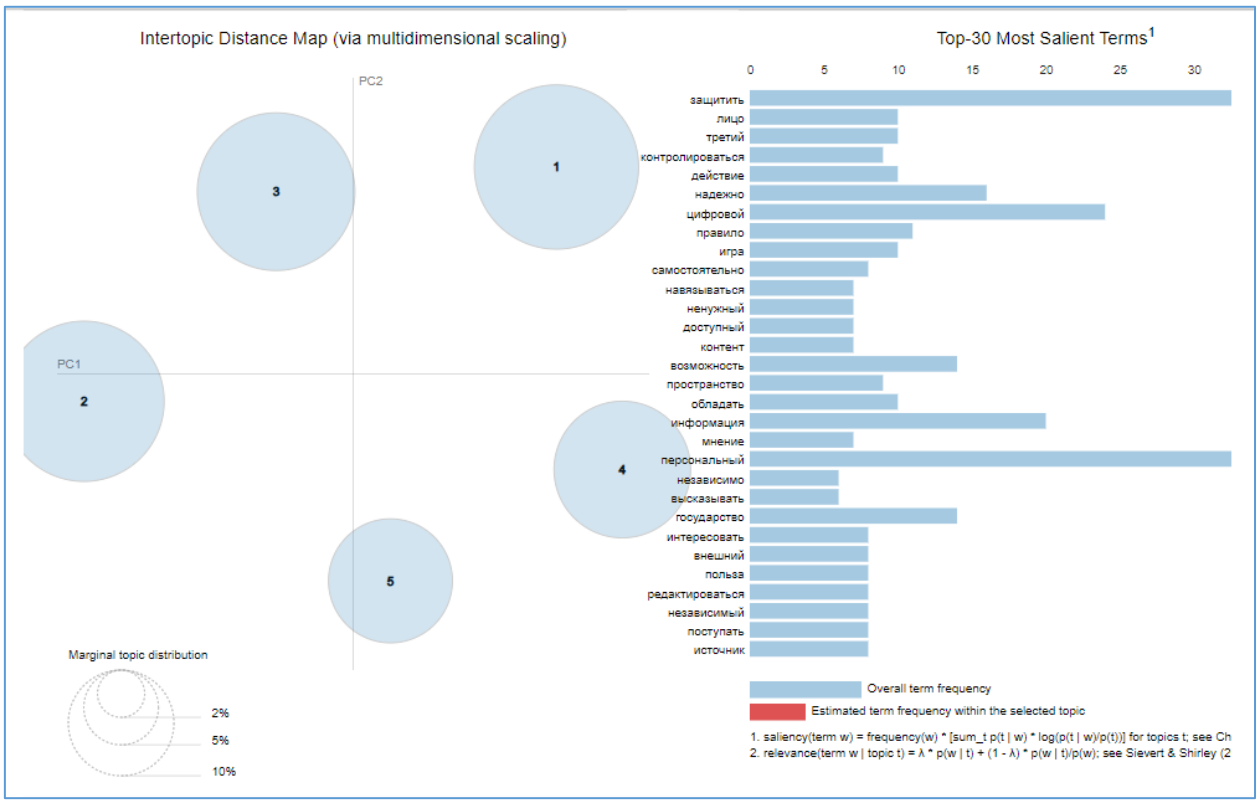

Рисунок 2 - Алгоритм LDA-анализа вопроса анкеты «Я буду обладать цифровым суверенитетом, если»

Результаты частотного анализа позволяют выделить наиболее используемые слова, употребляемые респондентами: защитить и защищенность (35 ответов), персональная информация (32 ответов), контроль (9 ответов), доступность (10 ответов) и т.д.

Также алгоритм LDA позволил выделить пять блоков ответов о понимании цифрового суверенитета опрошенными экспертами, которые мы классифицировали следующим образом, в частности:

1. Доступ к информации. Многие участники опроса (24.2 %) отметили важность доступа к интересующей информации и независимости источников, что указывает на стремление к свободе слова и доступу к качественным информационным ресурсам.

2. Защита персональной информации от утечек и мошенничества (23%). Респонденты акцентировали внимание на необходимости защиты от

утечек персональных данных, в которой особую роль должно играть государство.

3. Регулирование взаимодействий в цифровой среде, включая необходимость формирования понятных «правил игры» в цифровом пространстве (22,3%). Респонденты ожидают, что государство будет обеспечивать защиту персональных данных и создавать правовые рамки для их защиты, что подчеркивает важность законодательных инициатив в области цифрового суверенитета личности.

4. Контроль над персональными данными и самостоятельность принятия решений в цифровом пространстве (16,7%). Многие респонденты выразили желание контролировать свои персональные данные, обеспечивать их безопасность и принимать самостоятельные решения об их использовании, что подчеркивает важность личной ответственности и осведомленности в вопросах кибербезопасности.

5. Анонимность и конфиденциальность. Каждый десятый участник Экспертного опроса выразил желание сохранять анонимность в интернете и уверенность в конфиденциальности своих данных.

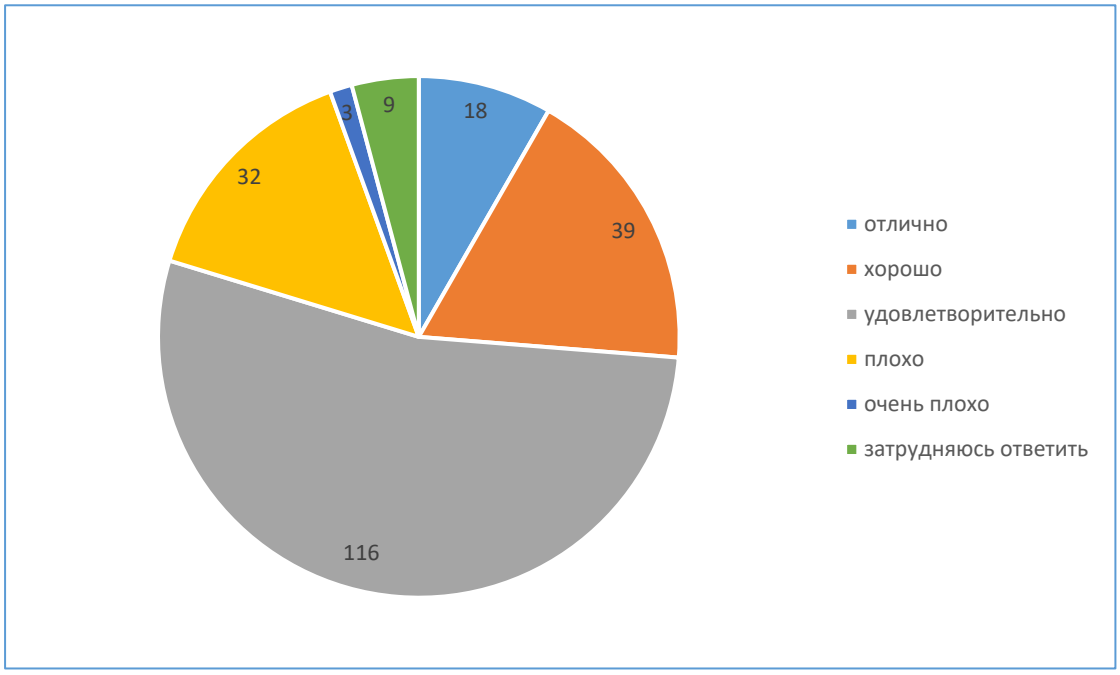

Рисунок 3. Диаграмма ответов респондентов на вопрос «Как вы, в целом, оцениваете защищенность вашего личного цифрового суверенитета?»

Также можно выделить дополнительные блоки, которые можно связать с неопределенностью и сомнениями о возможности существования цифрового суверенитета личности и его элементов. Некоторые участники выразили нежелание иметь цифровой суверенитет, что может, возможно, свидетельствовать о недоверии к цифровым технологиям или о предпочтении традиционных форм взаимодействия. С этими выводами коррелируют результаты анализа вопроса «*Как вы, в целом, оцениваете защищенность вашего личного цифрового суверенитета?*»[1]. Так, большинство респондентов (70%) оценивают свой суверенитет как удовлетворительный (рисунок 3).

Интересно распределение ответов респондентов на этот вопрос по двум группам: «ИТ-специалисты» и «специалисты из других сфер деятельности».

[1] ЭОЦСЛ-2024

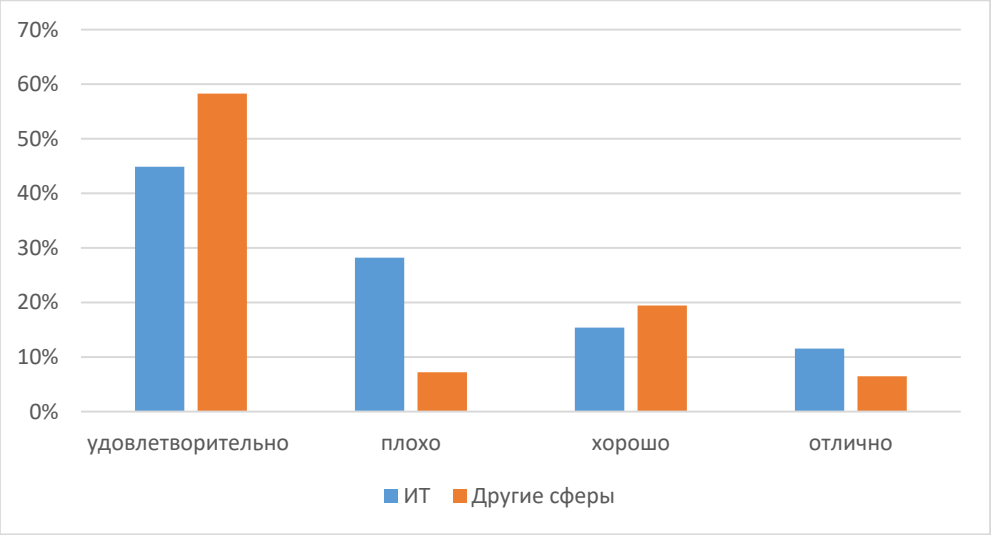

Рисунок 4. Распределение ответов респондентов на вопрос «Как вы, в целом, оцениваете защищенность вашего личного цифрового суверенитета?» в разрезе специальностей

Примечательно, что ИТ-специалисты в целом хуже оценивают свой цифровой суверенитет – за вариант «плохо оцениваю» высказалось 28% опрошенных.

Следующий блок вопросов касался действий индивида в части сохранения цифрового суверенитета («*Что может сделать человек для сохранения своего цифрового суверенитета?*»). Представляется, что ответы на этот вопрос целесообразно разбить на три группы: высокая, средняя и низкая степень значимости.

Что касается первой группы, респонденты в первую очередь подчеркивают важность осознания личной ответственности за свои действия в цифровом пространстве (81.1 %) и повышения цифровой грамотности (69%). В этой связи, можно сделать вывод об осознании человеком прямой зависимости между своим поведением в Интернете и обеспечением конфиденциальности.

Вторая группа факторов включает контроль за использованием персональных данных (53.4%), осознание рисков, связанных с умными устройствами (56.7%), и указывает на растущее беспокойство человека к негативному и угрожающему влиянию технологий на личную безопасность и

приватность. Многие респонденты уделяют особое внимание также знанию нормативных актов в части защиты своих прав и интересов в цифровом пространстве. (51.1%).

Последняя группа факторов, связанных с выполнением требований цифровых платформ, имеет меньшую значимость в ответах респондентов (37.7%), что, возможно, связано с непониманием значимости правил и регламентов взаимодействия с цифровыми платформами.

Представляется, что результаты анализа мнения респондентов по этому вопросу подчеркивают важность личной ответственности и цифровой грамотности как ключевых факторов для обеспечения цифрового суверенитета личности.

На выявление степени личной ответственности за технологические аспекты защищенности цифрового суверенитета личности был направлен вопрос: *«Какие технологические аспекты обеспечения своего цифрового суверенитета вы используете?».*

Как показывает анализ ответов на данный вопрос, люди много собственных усилий вкладывают в защиту своего суверенитета, прежде всего, в части использования антивирусного программного обеспечения (75,5%), проверенных сайтов и надежных источников (65,4%), регулярного обновления систем безопасности (56,2%), полагаясь на деятельность специализированных организаций (20,2 % ответа) и органов государственной власти. С другой стороны, это несколько противоречит их инертности в отношении изучения и применения новых возможностей и мер по защите личного цифрового суверенитета (33,1%).

Важным для понимания сущности цифрового суверенитета личности является анализ ответов экспертов на вопрос: «*Как вы думаете, насколько защищены ваши персональные данные?».*

Так, результаты анализа показали высокий уровень доверия к государственным организациям (76,5% опрошенных выбрали уровень не ниже среднего) и особенно к банкам и кредитным организациям (88,4%), что может

свидетельствовать о восприятии данных учреждений как более надежных в вопросах защиты персональных данных, а также более строгое регулирование и контроль данных организаций со стороны органов государственной власти и их обязательств по соблюдению стандартов безопасности. При этом, наивысший уровень доверия (более 90 %) отмечен респондентами к организациям, в которых работают респонденты, что может указывать на то, что люди чувствуют себя более защищенными в рамках своей профессиональной среды, а также связано с особенностями корпоративной культуры, акцентирующей внимание на защите данных сотрудников.

Низкий уровень доверия к интернет-магазинам (60 % опрошенных отметили низкую защищенность) отражает опасения людей относительно безопасности своих финансовых данных и личной информации при онлайн-покупках, что, возможно, связано с их недостаточной осведомленностью о мерах безопасности, принимаемых этими платформами, а также с негативным опытом, который могли иметь респонденты в прошлом в подобных ситуациях.

Также низкие оценки свойственны, по мнению экспертов, уровню защищенности персональных данных в личной переписке (42%) и социальных сетях (51,1%), что, на наш взгляд, указывает на растущее беспокойство о конфиденциальности в цифровом пространстве. Представляется, что частые утечки данных, скандалы вокруг использования личной информации и недостаточная прозрачность в политике конфиденциальности онлайн-платформ стали ключевыми факторами, влияющими на безопасность взаимодействий в Интернете.

Тем самым, результаты анализа ответов показывают, что, в целом, доверие к защите персональных данных варьируется в зависимости от контекста. Люди более склонны доверять традиционным и регулируемым организациям, в то время как в цифровом пространстве они проявляют настороженность. В этой связи необходимо подчеркнуть важность деятельности по повышению доверия людей к цифровым платформам, необходимость разработки более прозрачных и надежных механизмов защиты

персональной информации, а также развития цифрового просвещения и совершенствования навыков индивидуальной работы в цифровой среде.

С этими выводами коррелируют результаты анализа ответов на вопрос *о наличии в организации системы защиты персональных данных работников*. Большинство респондентов (58,5%) отметило существование в своей организации соответствующей системы.

Из 12 предложенных мер защиты персональных данных, используемых организациями, респонденты отметили высокое внимание к контролю доступа и наличию технических средств для защиты информации (по 79,2 % мнений соответственно), а также к ответственности работников за утечку персональных данных (72,3%) и контроль за обработкой и использованием персональных данных (76%). По мнению экспертов, самой значимой мерой является принятие политики информационной безопасности и норм электронного взаимодействия (73%), что подчеркивает важность формализации процессов, создания четких правил поведения для сотрудников и необходимость правового и этического подхода к обработке данных.

Отметим, что наименьшее количество ответов получила такая мера защиты, как регулярное обучение сотрудников новым информационным технологиям (51,6%), что, на наш взгляд, может свидетельствовать о достаточно изначально высоком уровне знаний в сфере информационных технологий, либо, наоборот, что данное направление защиты не является приоритетным для организации. Представляется, что именно обучение сотрудников является ключевым фактором в предотвращении утечек данных, так как многие инциденты происходят из-за человеческого фактора.

Некоторые вопросы экспертного опроса касались исследования степени контроля организации за действиями своих сотрудников в сфере информационных технологий. Анализ ответов респондентов на вопрос «*Какие элементы вашей рабочей деятельности контролируются в организации?*» позволил сделать следующие выводы**.** Наибольшее количество респондентов (67,7%) выбрало вариант «контент на компьютерах», что указывает на

большое внимание организации к защите информации на корпоративных компьютерах и наличию требований к соблюдению корпоративных стандартов в этой сфере. Вторым по популярности вариантом (52,5%) стало «использование рабочего времени» и «выполнение задач» (48,8%) и это связано, на наш взгляд, с необходимостью повышения эффективности и ответственности работы сотрудников и оптимизации рабочего процесса. Значительно меньший выбор экспертами ответов «контроль активности в интернете» (38,2% респондента) и «использование «умных» устройств» (35,4%) указывает, по нашему мнению, на то, что данная деятельность контролируется организацией из-за влияния на рабочий процесс.

Характерно, что личная переписка (7,8% ответов) и использование социальных сетей (12%) значительно меньше контролируется в организациях. Это может быть объяснено тем, что сотрудники имеют установленную степень свободы во время работы.

Как мы ранее утверждали, цифровой суверенитет представляет собой определенное состояние, при котором возможно достижение и поддержание независимости деятельности в цифровой среде. Цифровой суверенитет формируется различными субъектами, в частности, государством, организациями и отдельными индивидуумами. Уровень защищенности цифрового суверенитета личности во многом определяется тем, насколько сам индивид, организация, в которой он работает, и государство заинтересованы в защите цифровых прав пользователей. В этой связи интерес представляет мнение экспертов относительно степени вовлеченности личности, общества и государства в формирование цифрового суверенитета личности.

Влияние личности на собственный цифровой суверенитет.

Респонденты акцентируют повышенное внимание на практических и технических мерах защиты, таких как использование проверенных сайтов (77%) и надежных паролей (70%). Это еще раз подтверждает наш вывод о том, что большинство людей воспринимают защиту своих личных данных как приоритетную задачу, требующую конкретных действий, а не абстрактных

знаний или принятия рисков. Меры защиты, связанные с осознанием личной ответственности и знанием нормативных актов, получили значительно меньшее количество упоминаний (соответственно 39,6% и 36% ответов). Возможно, это указывает на недостаточную осведомленность респондентов о правовых аспектах защиты данных и их прав как пользователей, либо отражает общее недоверие к правовым системам, либо отсутствие информации о том, как эти системы могут помочь в защите личных данных в информационном пространстве.

Наименее популярны среди экспертов меры, касающиеся «повышения цифровой культуры и грамотности» (26,7%). Таким образом, респонденты не считают это важным аспектом защиты своего цифрового суверенитета. На наш взгляд, многие пользователи не осознают важность образования и информированности в области информационной безопасности и не понимают связи между уровнем своей цифровой грамотности и защитой личных данных. Также эксперты отмечают появление рисков использования «умных» устройств и необходимость обращения в специализированные компании по защите своего цифрового профиля (соответственно 16,5% и 15,6%). Это связано с тем, что у них появилось понимание необходимости в профессиональной помощи в столь сложных вопросах, а также в осознание неуверенности в своих знаниях и навыках, чтобы самостоятельно справляться с рисками и угрозами действий в цифровой среде.

Однако отметим, что экспертами не поддерживается такая сторона защиты, как соблюдение этических норм работы в Интернете (всего 13,3% экспертов отметили данную позицию), что, вероятно, связано с общим снижением уровня доверия к другим пользователям и платформам, а также с отсутствием четких этических норм деятельности в цифровом пространстве.

Влияние организации на цифровой суверенитет личности.

Анализ результатов Экспертного опроса[1] показал высокие требования к организациям для защиты цифрового суверенитета личности. По мнению

[1] ЭОЦСЛ-2024

респондентов, организации должны развивать политику информационной безопасности (67,7% выделили данную позицию), контролировать утечки данных (56,2%), устанавливать ответственность за разглашение информации (52,5%). Все это свидетельствует о необходимости создания в организациях более строгих регуляторов и правил, способствующих защите прав граждан в цифровой среде.

Корпоративное обучение сотрудников основам информационной безопасности и новым технологиям также является значимым для экспертов (38,2%), это подчеркивает важность повышения уровня осведомленности о рисках и методах защиты данных. Внедрение передовых стандартов и технологий, таких как системы фильтрации (36%) и ответственный подход к использованию искусственного интеллекта (27,2%), указывает на необходимость интеграции новых технологий в существующие социальные процессы.

Менее всего эксперты поддержали такие меры защиты цифрового суверенитета в организациях, как развитие открытых технологий (всего 4,1% ответов) и прозрачность (2,3%), что указывает на недостаточный уровень осведомленности или недоверия к таким подходам и в некоторой степени является препятствием для развития более открытых и доступных систем управления данными и, в целом, может замедлить прогресс в области цифрового суверенитета личности при выборе программного и аппаратного обеспечения.

Влияние государства на цифровой суверенитет личности.

Одним из значимых субъектов защиты цифрового суверенитета личности являются государство и государственные структуры, которые ответственны за формирование государственной политики в информационной сфере и обеспечение контроля за соблюдением цифровых прав граждан.

На основе представленных респондентами ответов можно сделать следующие выводы о вкладе государства в защиту персональных данных и цифрового суверенитета личности.

Наиболее популярны меры, связанные с развитием государственной политики в информационной сфере и блокировкой ненадежных социальных сетей (соответственно 66,3% и 55,3% экспертов выделили эти меры). Это, как нам кажется, указывает, во-первых, на высокую степень доверия респондентов к государству как к основному институту, способному обеспечить защиту их прав в цифровом пространстве, и, во-вторых, на высокие ожидания граждан в части активного вмешательства государства в регулирование информационной среды.

Выделим также обозначенный в исследовании запрос на разработку технических средств противодействия угрозам (54,3%) и установление ответственности за распространение фейков и утечку данных (53%), что подчеркивает важность не только принятия законодательных мер, но и необходимость государственной поддержки технологических решений. Это может привести к развитию новых социальных институтов, таких как омбудсмен в области кибербезопасностью и защиты данных и т.д.

Ответы, касающиеся снижения зависимости от глобальных информационных систем и разработки отечественных платформ (39,6%), указывают на высокую экспертную поддержку растущего стремления России к национальному цифровому суверенитету в части развития новых отечественных технологий и стартапов, а также необходимости укрепления национальной идентичности в цифровом пространстве.

Характерно, что в экспертном опросе отмечен достаточно низкий уровень интереса к развитию моральных и этических норм работы в Интернете (всего 9,2% выбрали данную позицию) и расширению возможностей для получения электронных услуг (соответственно 13,3%), что может говорить о том, что респонденты не видят в этом первоочередных задач, и указывает на недопонимание гражданами важности этических аспектов в цифровом взаимодействии и требует дополнительного внимания со стороны образовательных и государственных институтов.

Таким образом, анализ данных экспертного опроса показывает необходимость системного подхода к анализу уровня и структуры цифрового суверенитета личности. Формирование цифрового суверенитета личности представляет собой системный всеобщий процесс, охватывающий государство, организацию и личность во взаимном интерактивном контексте. Различные уровни цифрового суверенитета нельзя рассматривать изолированно друг от друга. Цифровой суверенитет формируется самим индивидом с его мотивами и потребностями, знаниями и навыками в сфере ИТ-технологий, поддерживается (или не поддерживается) организациями с их возможностями разделения и совмещения задач с сосуществованием формальных и неформальных организационных структур и зависит от проводимой государством информационной политики, реализующей защиту прав граждан в цифровом пространстве и обеспечивающей национальную безопасность и технологический суверенитет.

Исследование показало, что респонденты видят формирование и защиту цифрового суверенитета как совместную ответственность между индивидуумом, организациями и государством, что указывает на необходимость комплексных мер, включающих как государственные меры, так и активное участие гражданского общества и образовательных учреждений.

2.3 Формирование концептуальной модели цифрового суверенитета личности

Концептуальные модели в исследовании социальных процессов представляют собой определенные теоретические (абстрактные) представления, которые не только помогают понять и анализировать сложные социальные явления, но и выполняют роль инструмента для систематизации

знаний, упрощения анализа и визуализации взаимосвязей между различными элементами социальных систем[1].

Преимущества использования концептуальных моделей включают возможность выявления ключевых факторов, влияющих на социальные процессы, а также упрощение коммуникации между исследователями и практиками. Представляется, что концептуальная модель может помочь в исследовании цифрового суверенитета личности, позволяя определить не только структуру, но и взаимодействие различных аспектов цифровой идентичности, цифрового статуса и контроля над личными данными.

Чтобы системно описать цифровой суверенитет личности, нами предложена многоуровневая концептуальная модель с выделением категорий государства, организации и личности с представлением их в соответствующие реляционные структуры и включением родственных понятий, таких как суверенитет данных, суверенитет цифрового текста и т.д.

Структура концептуальной модели представлена в таблице 6.

Таблица 6. Концептуальная модель цифрового суверенитета личности

	Государство	Организация	Личность
Цифровой суверенитет личности	Государственная политика в информационной сфере	Технологические стандарты и свобода выбора	Цифровая социализации и грамотность
	Государственные услуги и электронное правительство	Нормативная и правовая база организации	Возможность самостоятельного (суверенного) действия
	Обеспечение гражданских прав и свобод человека в цифровом пространстве	Обучение сотрудников организации новым технологиям	Знание нормативных актов и самоопределение в цифровом пространстве

[1] Е Б. Хорольцева,А В. Федорова. Эффективные организационные практикаи управления социальным капиталом в условиях высокой неопределенности и рисков. Вестник Поволжского института управления, 2024. С. 76

	Регуляторы и международные стандарты в сфере информационной безопасности	Взаимодействие между цифровым и аналоговым форматом в бизнес-процессах организации	Осознание рисков использования «умных» устройств
	Экономическая стратегия и финансирование исследований и инноваций	Права на участие в управлении организацией	Самоопределение в информационном пространстве
	Государственная политика в отношении монополистических ИТ структур	Прозрачность деятельности организации	Доверие к используемым сайтам и платформам
	Защита персональных данных	Технологическая универсальность	Развитие цифровой культуры и этики
	Образование и доступ к технологиям	Политика в отношении суверенитета данных в организации	Осознание личной ответственность за свой цифровой суверенитет

Для более информативного отображения модели цифрового суверенитета личности с тремя уровнями: государство, организация и личность, можно использовать графическую нотацию, которая визуализирует взаимосвязи и элементы на каждом уровне. Одним из подходов является диаграмма Венна, помогающая выявить общие черты и различия между социальными явлениями, что способствует лучшему пониманию их взаимодействия. Так, можно использовать диаграмму для анализа пересечений структурных элементов на различных уровнях формирования цифрового суверенитета личности.

Рисунок 5. Диаграмма Венна концептуальной модели цифрового суверенитета личности

Каждый уровень цифрового суверенитета личности (государство, организация, личность) представлен отдельным кругом. Эти круги могут пересекаться, чтобы показать общие элементы и взаимосвязи между уровнями (рисунок 5). Внутри каждого круга размещены ключевые элементы, соответствующие каждому уровню.

Так, например, для уровня «Государство» - государственная политика в информационной сфере, для «Организации» - технологическая универсальность, взаимодействие цифрового и аналогового формата деятельности, для уровня «Личность» - социализация, возможность суверенного действия в цифровом пространстве и т.д.

В местах пересечения кругов можно указать элементы, которые являются общими для двух или всех трех уровней. Например, элемент «технологические стандарты и свобода выбора используемой технологии» может быть важным как для личности, так и для организации, а «государственная политика в отношении монополистических ИТ структур» может пересекаться с интересами как государства, так и организаций.

Выбранный размер кругов диаграммы Венна призван подчеркнуть значимость уровней при формировании цифрового суверенитета личности. По мнению автора, уровень личности должен быть в центре этой модели. Государственный уровень также играет важную роль в обеспечении защиты гражданских прав и свобод человека в цифровом пространстве, в том числе защиты персональных данных. Организационный уровень создает необходимые условия для обеспечения информационно-психологической безопасности при выборе и использовании новых технологий и реализует политику обеспечения суверенитета данных сотрудников.

Подписи и легенда диаграммы Венна представлены на рис.6

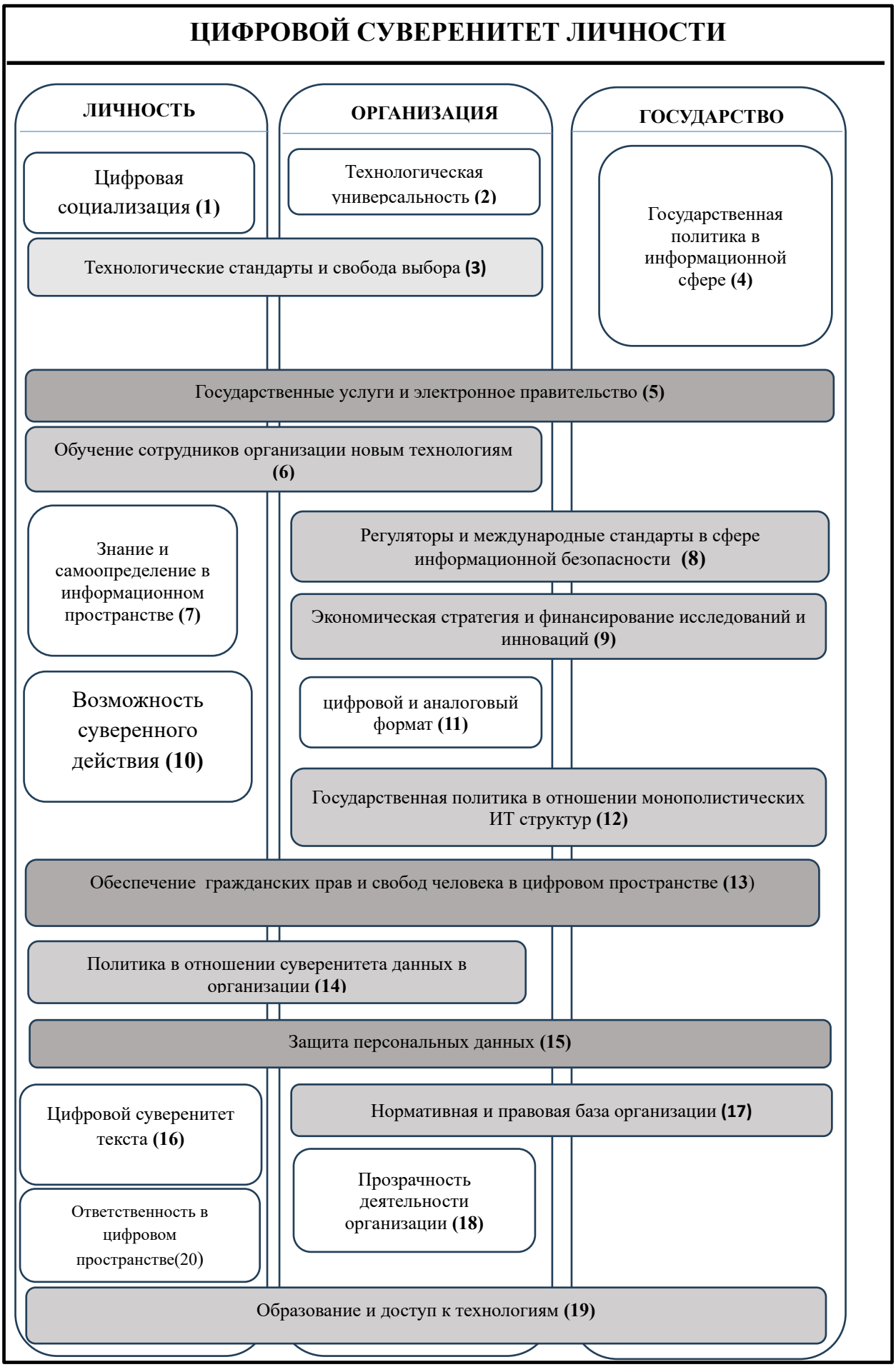

Рисунок 6. Структура концептуальной модели цифрового суверенитета личности

Основные элементы концептуальной модели цифрового суверенитета личности.

1. Уровень государства.

Цифровой суверенитет государства тесно связан с такими элементами информационной безопасности, как устойчивость критических информационных инфраструктур, конфиденциальность и защита персональных данных, контроль над экономическими экосистемами, доверие к нормам права и свободам человека, автаркия, функциональная совместимость с международными стандартами, мобильностью и открытыми стандартами.

Способы влияния государства на цифровой суверенитет личности:

- *Реализация государственной политики в информационной сфере.*

Тематика информационной безопасности и цифрового суверенитета затрагивается все чаще в выступлениях высших должностных лиц различных государств. Так, в 2021 Президент Российской Федерации В.В. Путин на одном из заседаний Совета Безопасности Российской Федерации отметил, что «мы выступаем за незыблемость цифрового суверенитета государств, а это означает, что каждая страна может самостоятельно определять параметры регулирования собственного информационного пространства и соответствующей инфраструктуры»[1]. В этом контексте цифровой суверенитет обозначен как ведущая тема цифровой трансформации и цифровой политики, чтобы в равной мере охватить интересы личности, общества и государства.

В рамках процесса принятия политических решений и государственного контроля и надзора государство создает основу для действий, в которой люди могут принимать суверенные решения в цифровом пространстве. Государство ответственно за разработку и внедрение комплексных регуляторов для защиты конфиденциальности и личных данных граждан, должно обеспечивать защиту от нарушений конфиденциальности со стороны как государственных, так и частных учреждений, защищать право на неприкосновенность частной жизни

[1] https://www.interfax.ru/russia/758107

- *Обеспечение гражданских прав и свобод человека в цифровом пространстве.*

Основные права включают в себя такие права, как свобода выражения мнений, информации и общения, всеобщий и равный доступ, конфиденциальность и защита данных, право на анонимность, право «быть забытым», защита несовершеннолетних, интеллектуальная собственность и др. С одной стороны, государственные органы играют ключевую роль в формировании законодательства, которое защищает гражданские права в цифровом пространстве, и эффективное правовое регулирование должно обеспечивать баланс между защитой прав граждан и необходимостью обеспечения безопасности и порядка в интернет-пространстве. С другой – необходимо участие граждан в формировании и обсуждении цифровой политики. Это может быть достигнуто через платформы для общественных консультаций и диалогов, что позволит учитывать мнения и интересы различных групп населения.

- *Стандартизация и имплементация международных стандартов в сфере информационной безопасности*.

Регуляторы и международные стандарты в сфере информационной безопасности играют важнейшую роль в обеспечении цифрового суверенитета личности. Они устанавливают правила и нормы, которые защищают данные пользователей от несанкционированного доступа и злоупотреблений. В условиях глобализации и цифровизации соблюдение международных стандартов позволяет странам защищать свои интересы и обеспечивать безопасность граждан в киберпространстве, что, в свою очередь, укрепляет доверие пользователей к цифровым сервисам и платформам.

Центральные руководящие принципы и стандарты могут быть определены и приняты на уровне государственных структур по согласованию с организациями и, в идеале, способствовать обеспечению прозрачности информационной базы или основы принятия решений для компаний. В качестве примеров можно привести стандарты и спецификации по защите и

безопасности данных (например, Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации, Приказ ФСТЭК «Модель угроз в сфере безопасности информации). Правила и стандарты формируют конкурентоспособность организаций на глобальном рынке. Это способствует формированию цифрового суверенитета организаций, поскольку им не потребуется дополнительная помощь в определении или внедрении стандартов, а скорее будут использоваться встроенные рекомендации, предоставленные государством.

- *Экономическая стратегия и финансирование исследований и инноваций*.

Финансирование исследований и технологических новаций становится ключевым элементом для создания технологий, обеспечивающих цифровой суверенитет личности. Важно, чтобы экономическая стратегия государства включала в себя поддержку стартапов и инициатив, направленных на разработку безопасных цифровых решений. Это позволит не только обеспечить конфиденциальность личных данных, но и стимулировать экономический рост организаций.

Исследовательские программы призваны повысить ценность цифрового суверенитета как на государственном, так и на уровне организационных структур. Финансирование играет ключевую роль в определении приоритетов исследований. Увеличение инвестиций в проекты, направленные на развитие национальных технологий и инфраструктуры, может укрепить цифровой суверенитет государства. Например, финансирование исследований в области кибербезопасности, искусственного интеллекта и блокчейн-технологий может привести к созданию независимых решений, что снизит риски, связанные с иностранными технологиями. Влияние на цифровой суверенитет также имеет социальные последствия. Увеличение инвестиций в местные технологии может создать новые рабочие места, повысить уровень образования и улучшить качество жизни граждан.

С одной стороны, это может способствовать доступности альтернативных продуктов или услуг и, таким образом, положительно влиять на самостоятельность действий на национальном уровне. С другой стороны, эти типы регулирования могут выступать в качестве барьеров для инноваций. Таким образом, организации ограничены в своем праве на совместное определение и не могут способствовать технологическому разнообразию. В качестве примера можно привести социальные сети. Из-за значительного увеличения числа пользователей государство осознало необходимость принятия мер в отношении регулирования и контроля таких структур. Также важно учитывать, что без должного контроля и прозрачности такие инициативы могут привести к неравенству и социальной напряженности.

- *Государственная политика в отношении монополистических ИТ-структур.*

Баланс сил определяет отношения между государством и организацией. Возникает обеспокоенность в части того, что современные платформы или цифровые организации могут занять монопольное положение. Примеры включают платформы социальных сетей и технологические компании. Посредством технологий, стандартов и патентов крупные корпорации могут посягать на суверенитет государства, ограничивать конкуренцию и подавлять инновации, так как новые игроки не могут легко войти на рынок. В результате пользователи могут столкнуться с ограниченным выбором услуг и продуктов.

Когда несколько компаний контролируют значительную часть цифровой инфраструктуры, государство, организации и человек становятся зависимыми от их решений, что может угрожать цифровому суверенитету государства, которое может потерять возможность самостоятельно управлять своими данными и информационными потоками. Также стоит отметить, что монополисты часто оказывают значительное влияние на общественное мнение и политические процессы.

Монополистические структуры могут усугублять социальное неравенство, так как доступ к передовым технологиям часто оказывается

ограниченным для определенных групп населения. Это может привести к цифровому разрыву, где одни слои общества имеют доступ к современным технологиям, а другие остаются вне цифровой экономики.

В этой связи именно государству для защиты цифрового суверенитета необходимо разработать эффективные механизмы регулирования и политики, которые бы ограничивали монополистические практики и способствовали созданию более конкурентной среды.

- *Защита персональных данных.*

В условиях глобализации и цифровизации данные пользователей становятся объектом коммерческой эксплуатации и политического контроля. Эффективная защита персональных данных является основой для обеспечения индивидуальной безопасности и доверия общества к цифровым технологиям.

В открытом и демократическом обществе предполагается наличие пространств, в которых люди могут перемещаться и общаться без наблюдения. В этом контексте, вероятно, наиболее важным аспектом обеспечения или развития цифрового суверенитета является принятие специального законодательства, например, для ЕС – Общий регламент по защите данных (GDPR). Кроме того, такие термины, как безопасность данных, защита данных, патентное право и авторское право, облачные вычисления, регулирование электронной коммерции и рассмотрение общих договорных и коммерческих условий в цифровой экономике, могут быть представлены как часть правовой базы.

Государственное регулирование защиты персональных данных - это обеспечение конфиденциальности личной информации в сфере электронных коммуникаций. Сфера его действия применима к организации, которая предоставляет любую форму онлайн-коммуникационных услуг, применяет технологии онлайн-отслеживания или использует методы прямого электронного маркетинга. Такое регулирование, как правило, направлено на обеспечение более высокого уровня конфиденциальности для всех электронных коммуникаций и включает новых участников, более строгие

правила, информационное содержание и метаданные, новые возможности для бизнеса, упрощенные правила для файлов cookie, защиту от спама и более эффективное применение.

Вместе с тем утечки персональных данных могут привести к утрате доверия граждан к государственным учреждениям и компаниям, что, в свою очередь, может определить требования о более строгом регулировании в этой сфере. Защита персональных данных как социальный процесс также затрагивает вопросы этики и прав человека. Граждане требуют уважения к своей частной жизни и осознания того, как их данные используются. Это порождает необходимость разработки государственными структурами более прозрачных и ответственных политик.

- *Развитие образования и обеспечение доступа к образовательным технологиям.*

Образование является одним из ключевых параметров достижения цифрового суверенитета на каждом уровне модели (государственном, организационном и личностном). В частности, институционализированное обязательное общее образование с упором на приобретение цифровых навыков является основным требованием для суверенного участия в жизни общества. Также важны дополнительное обучение и образование взрослых. Определенный уровень цифровой грамотности является предпосылкой цифрового суверенитета. Государство обязано создать рамочные условия в образовательных учреждениях (например, школах, колледжах, университетах) и за их пределами, в которых граждане могут приобретать цифровые навыки. Это относится не только к связи образования и цифровизации в целом. Скорее, требуется глубокая и устойчивая реализация данной темы в учебных программах общего, среднего и высшего образования при обеспечении доступа к цифровым технологиям. Например, достижение суверенитета данных требует знания различных носителей, соответствующих аспектов безопасности и потенциальных рисков их использования. Кроме того,

требуются сертифицированные ИТ-продукты, системы и сетевые инфраструктуры, гарантирующие безопасную передачу данных.

- *Государственные услуги и электронное правительство.*

Государственные услуги можно рассматривать как своеобразный «интерфейс» между обязательствами государства и интересами граждан. Он показывает, что граждане все чаще требуют прозрачности, эффективности и оперативности от органов государственного и муниципального управления и общественных организаций в условиях цифровизации. Таким образом, все более широкое внедрение цифровых технологий представляет собой ключевой элемент реакции правительств на такие требования. Использование цифровых технологий для редактирования и обработки конфиденциальных данных граждан также требует совершенно новых концепций с точки зрения безопасности, доступности и передачи данных. Это относится не только к технической перспективе ИТ-систем, но и к ИКТ-компетенциям (например, знание современных ИТ-технологий и процессов поддержки, понимание технологии, знание архитектуры программного обеспечения) вовлеченных людей. Во взаимодействии политических решений, нормативно-правовой базы, проектирования образовательных процессов в цифровом мире и предоставления доступа к цифровым технологиям государственные услуги являются важным инструментом суверенно действующих граждан.

2. *Уровень организации.*

Способы влияния организации на цифровой суверенитет личности.

- *Технологические стандарты и свобода выбора.*

В современных организациях технологические стандарты определяют, какие инструменты, платформы и системы могут использоваться. Это может ограничивать свободу выбора сотрудников и влиять на их способность принимать решения. Например, внедрение единой системы управления может снизить гибкость и скорость реакции на изменения.

Свобода выбора технологий в организации может быть важным аспектом цифрового суверенитета личности. Индивиды, имея возможность

выбирать, какие инструменты использовать, могут лучше контролировать свои данные и избегать зависимости от определенных платформ. Ограничение этой свободы может привести к снижению уровня доверия к организациям и платформам.

Цифровой суверенитет личности касается контроля над своей цифровой идентичностью и данными. Технологические стандарты, установленные в организациях, могут как поддерживать, так и подрывать этот суверенитет. Если стандарты разрабатываются с учетом интересов пользователей и предоставляют им выбор, это может укрепить цифровой суверенитет. В противном случае, навязывание стандартов может привести к потере контроля над личной информацией.

- *Нормативная и правовая база, определяющая организационно-правовые аспекты деятельности организации.*

Нормативные акты организаций, устанавливающие правовые рамки, определяя права и обязанности как для самих организаций, так и для пользователей их услуг, не всегда успевают за новыми технологическими возможностями цифрового пространства. Правовая база организации может способствовать или препятствовать реализации цифрового суверенитета личности. Например, отсутствие четких норм, касающихся ответственности за утечку данных, может привести к снижению уровня защиты прав личности. В то же время наличие эффективных инструментов правовой защиты, таких как возможность судебного обжалования действий организаций, может усилить позиции индивидов в вопросах, касающихся их цифровых прав.

- *Обучение сотрудников организации новым технологиям.*

Обучение сотрудников организации новым технологиям может влиять на цифровой суверенитет несколькими способами:

Во-первых, повышение уровня знаний о технологиях может помочь сотрудникам лучше понимать, как работают цифровые инструменты и приложения, что, в свою очередь, может способствовать более осознанному поведению в сети. Во-вторых, обучение может укрепить навыки работы с

данными и защитой личной информации, что поможет сотрудникам более эффективно управлять своими цифровыми профилями и способствовать формированию корпоративной культуры, ориентированной на защиту данных и соблюдение цифровой этики.

Низкий уровень цифровых компетенций сотрудников может привести к снижению возможностей для организаций стать более суверенными в информационном пространстве. Также возможно и обратное, если организация становится более суверенной в цифровом отношении в результате внешнего или внутреннего давления, то это влияет на сотрудников, которые впоследствии повышают свой цифровой суверенитет. Вместе с тем обучение может привести к зависимости от технологий, что может снизить способность сотрудников принимать самостоятельные решения о контроле своих данных.

- *Взаимодействие между цифровым и аналоговым форматом в бизнес- процессах организации.*

В бизнес-процессах организациям часто необходимо сочетать цифровые и аналоговые форматы. Цифровые технологии могут улучшать эффективность процессов, автоматизировать задачи и упрощать доступ к информации. Однако аналоговые форматы (например, личные встречи, бумажная документация) могут сохранять важные элементы человеческого взаимодействия и доверия.

Представляется, что взаимодействие между цифровым и аналоговым форматами может как укреплять, так и ослаблять цифровой суверенитет. С одной стороны, использование информационных технологий может облегчить доступ к информации и повысить уровень контроля над данными. С другой - если организация не обеспечивает прозрачность в обработке данных или не предоставляет пользователю выбор в отношении использования его данных, это может привести к утрате контроля и, соответственно, к снижению цифрового суверенитета личности.

- *Право на участие в управлении организацией.*

Представляется, что одним из элементов цифрового суверенитета личности на уровне организации является наличие взаимосвязи между сотрудниками, имеющими право голоса в принятия решений в организации, и цифровым суверенитетом указанной организации. Степень понимания и использования людьми цифрового суверенитета имеет большое значение для безопасности компании. Вполне возможно, что отдельные сотрудники скорее передадут ответственность технической системе, чем возьмут на себя ответственность по защите данных, и таким образом могут стать источником угроз кибербезопасности.

- *Прозрачность деятельности организации.*

Прозрачность деятельности организации играет значимую роль в обеспечении цифрового суверенитета личности. Когда организации открыто делятся информацией о своих процессах и политике, это способствует формированию доверия со стороны пользователей. Доверие, в свою очередь, позволяет людям более осознанно управлять своими данными и выбирать, каким образом они будут использоваться. В условиях цифровой экономики, где личные данные становятся ценным ресурсом, прозрачность помогает предотвратить злоупотребления и утечки информации. Кроме того, организации, придерживающиеся принципов прозрачности и открытости, чаще всего соблюдают этические стандарты, что также укрепляет цифровой суверенитет. Таким образом, пользователи могут быть уверены, что их права защищены, а данные обрабатываются в соответствии с их интересами.

На уровне архитектуры технической и технологической системы организации представляется, что прозрачная среда приложений играет важную роль, когда необходимо решить, какое программное обеспечение использовать для конкретной задачи. На более высоком уровне значимую роль играет прозрачность рынка. Существуют, например, компании, а также правительственные агентства, которые помогают потребителям получить более полное представление о нескольких различных предложениях на рынках

с высокой информационной асимметрией. Это говорит о том, что организации могут положительно влиять на цифровой суверенитет личности.

- *Технологическая универсальность.*

Она представляет собой опыт и ноу-хау в широком спектре технологий и предложений, например, когда организация использует программное обеспечение с открытым исходным кодом или рассматривает несколько потенциальных поставщиков облачных вычислений, это может позволить организациям стать более суверенными в информационном пространстве. Обратное также может быть верным, если организация не стремится к привязке к конкретным поставщикам и решает использовать программное обеспечение с открытым исходным кодом, то сотрудники также применяют эту стратегию в своем личном выборе программного обеспечения.

- *Тип организации.*

Это может быть важным фактором реализации цифрового суверенитета личности. Следует различать коммерческие и некоммерческие компании, общественные организации, клубы и государственные учреждения. Кроме того, их внутренняя структура - централизованная или децентрализованная - может повлиять на то, как они воспринимают и действуют в отношении цифрового суверенитета.

- *Политика в отношении суверенитета данных в организации.*

Политика отражает способность организации контролировать свои данные. Организация с высокой степенью контроля может означать большую защиту данных для отдельных лиц. Однако низкие возможности организаций могут привести к выбору поставщиков с низким качеством или неэффективными методами защиты. Передовые методы обеспечения ИТ-безопасности можно рассматривать как часть суверенитета данных.

3. Уровень личности.

Выделим ключевые тематические кластеры на этом уровне.

Цифровая социализация личности и грамотность.

Цифровая социализация человека играет ключевую роль в формировании модели цифрового суверенитета личности, поскольку она определяет, как индивид взаимодействует с цифровыми технологиями и как осознает свои права и ответственность в цифровом пространстве. Например, поддержка со стороны родителей в освоении технологий может способствовать более активной позиции в использовании цифровых ресурсов и защите своей конфиденциальности.

Цифровая социализация формирует представления о том, что является приемлемым или неприемлемым в цифровом взаимодействии. Индивиды, выросшие в среде, где ценится защита личной информации и цифровая безопасность, скорее всего, будут более осторожными в своей онлайн-деятельности. Участие в различных онлайн-сообществах и социальных сетях формирует не только навыки взаимодействия, но и понимание вопросов конфиденциальности, безопасности и прав в цифровом пространстве. Это может либо укреплять, либо подрывать цифровой суверенитет в зависимости от характера этих сообществ.

Социализация также влияет на способность индивидов критически оценивать информацию, которую они получают из цифровых источников, что, несомненно, важно для защиты своих прав и свобод в условиях информационной перегрузки и манипуляций.

- *Возможности суверенного действия в цифровом пространстве.*

В цифровых обществах это становится особенно актуальным, когда люди всех возрастов сталкиваются со специфическими требованиями, касающимися приобретения и использования механизмов, методов доступа и самих информационных технологий. Основное внимание уделяется средствам, с помощью которых люди должны реализовывать себя во все более цифровом мире, преследовать личные цели и выполнять задачи. В связи с этим важно определить, какие возможности есть у индивида, чтобы самоутвердиться в цифровом мире и включиться (или не включиться) в процессы социального воспроизводства. Понятие цифрового суверенитета

пытается описать амбивалентную структуру механизмов государственного контроля, экономических и политических интересов и личного развития людей.

- *Знание и самоопределение в информационном пространстве.*

В многочисленных исследованиях подробно обсуждается положительное и отрицательное влияние цифровизации на суверенитет личности. Отмечается не столько важность сохранения суверенитета личности над своими цифровыми следами, сколько возможность познания индивидов и их суверенного самоопределение [1].

Возникают две фундаментальные перспективы: с одной стороны, индивидуальная. Потому что, во-первых, каждый человек принимает самостоятельное решение об использовании или неиспользовании цифровых технологий. На практике люди могут свободно использовать аналоговые или умные часы. Однако во все более оцифровываемом мире избегать цифровых технологий становится все труднее. Это подводит нас ко второй перспективе - проектирование рамочных условий в цифровом мире, в котором действуют люди. Эти рамочные условия относятся к миру цифрового текста. В этом цифровом текстовом мире требуются навыки, позволяющие человеку работать с текстами, созданными в условиях цифровизации. Эти тексты существенно отличаются от тех текстов, которые генерируются типографским способом.

- *Ответственность личности в цифровом пространстве.*

Представляется, что ответственность личности в цифровом пространстве является одним из важнейших элементов формирования цифрового суверенитета. Свобода самоопределения подразумевает ответственность за свои действия и выборы. Личность должна осознавать последствия своих решений, например, делясь личной информацией или взаимодействуя с различными онлайн-сообществами и социальными сетями. Кроме того, ответственность личности включает в себя активное участие в защите своей конфиденциальности и безопасности, что может проявляться в использовании

[1] Friedrichsen, M., Bisa, P.J.: Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft (2016)

некоторых технологий информационной безопасности, таких как сложные пароли, двухфакторная аутентификация и осознанный подход к выбору программного обеспечения и передаваемой информации по сети. Личность должна быть готова не только защищать свои права, но и понимать, как ее действия могут повлиять на других пользователей и на общество в целом. Это создает баланс между свободой и ответственностью, что является основой для формирования здорового цифрового пространства.

- *Навыки работы с цифровыми текстами.*

Цифровая компетентность становится важнейшей чертой цифрового суверенитета. Современный человек должен выработать понимание особенностей этих новых, постоянно меняющихся коммуникативных практик производства и восприятия текста, а также их (имплицитных) норм. Только таким образом он сможет не только воспользоваться возможностями, предлагаемыми социальными сетями, такими как спонтанное цифрово-текстовое самовыражение или создание новых виртуальных сообществ на основе текста, но также осознавать риски и решать проблемы. Это включает в себя рефлексивный подход к конфиденциальности и уважение личности и целостности других партнеров по взаимодействию, которые представляют себя в цифровом и текстовом виде. Этические и моральные аспекты, возникающие при работе с цифровыми текстами, не всегда могут быть решены с точки зрения культурно установленных норм.

Таким образом, концептуальная модель цифрового суверенитета личности включает в себя три базовых уровня: цифровой суверенитет государства, цифровой суверенитет организации и цифровой суверенитет личности. Цифровой суверенитет государства тесно связан с такими элементами информационной безопасности, как устойчивость критических информационных инфраструктур, конфиденциальность и защита персональных данных, контроль над экономическими экосистемами, доверие к нормам права и свободам человека, автаркия, функциональная совместимость с международными стандартами, мобильностью и открытыми

стандартами. Цифровой суверенитет организации основан на технологических стандартах, которые определяют, какие инструменты, платформы и системы могут использоваться. Свобода выбора технологий в организации может быть важным аспектом цифрового суверенитета личности: технологические стандарты, установленные в организациях, могут как поддерживать, так и подрывать этот суверенитет. Цифровой суверенитет личности, с одной стороны, складывается под влиянием и при участии двух предыдущих уровней суверенитета, с другой стороны, формируется самостоятельно индивидом и связан с возможностями и особенностями его цифровой социализации.

На основе предложенной концептуальной многоуровневой модели цифрового суверенитета личности можно сделать ряд теоретических выводов и практических рекомендаций, расширяющих социологические теоретические концепции, связанные с теорией сетевого общества Мануэля Кастельса и теорией социального капитала П. Бурдье, в частности:

- модель позволяет рассматривать цифровой суверенитет личности не как абстрактное индивидуальное качество, а как результат взаимодействия трех социальных уровней: государства, организации и самой личности. Это подчеркивает, что цифровой суверенитет — не только индивидуальная компетенция, но и социально обусловленный феномен, формирующийся в рамках институциональных и нормативных структур. Цифровой суверенитет формируется не только на основе индивидуальных компетенций, но и через социальные связи, которые становятся особенно важными в цифровом пространстве, что расширяет понимание социального капитала П. Бурдье, включая в него не только традиционные формы взаимодействия, но и новые, возникающие в онлайн-среде.

- погружение личности в цифровое пространство приводит к существенным изменениям в социальной идентификации и идентификационном поведении. Такие элементы модели, как цифровая социализация и самоопределение в цифровой среде, подтверждают выводы о

том, что Интернет становится для многих не только инструментом, но и средой формирования новой социальной идентичности, где возрастает значимость технологических аспектов с одновременным снижением коммуникативной составляющей. Это расширяет теорию М. Кастельса, подчеркивая, что сетевые структуры не только влияют на доступ к информации, но и на процесс самоопределения и идентификации индивидов.

- предложенная модель подчеркивает риски возникновения цифрового неравенства - различий в доступе к технологиям, цифровой грамотности и возможностях самостоятельного и независимого действия, что проявляется как на уровне личности (различия в цифровых компетенциях), так и на уровне общества (ограничение доступа к технологиям для отдельных групп населения). Такое различие может привести к формированию новых форм социальной стратификации, отражающих системное расслоение общества на основе различий в доступе к технологиям, уровне цифровых компетенций и возможностях суверенного действия, что согласуется с концепцией П. Бурдье о том, что социальный капитал может создавать и усиливать неравенство в обществе.

- модель демонстрирует, что цифровой суверенитет личности становится новым измерением социальной интеграции и легитимации институтов, в котором государство и организации вынуждены пересматривать свои функции, а личность - адаптироваться к новым формам взаимодействия и контроля.

- образование и развитие цифровых компетенций становятся ключевыми факторами социальной мобильности и интеграции в цифровое общество. Модель подтверждает, что без институциональной поддержки образования невозможно достичь реального цифрового суверенитета для широких слоев населения.

Разработанную в диссертации модель цифрового суверенитета личности целесообразно использовать в дальнейших социологических исследованиях, например, для:

- системного анализа взаимосвязи между институтами, организациями и личностью в цифровой среде;

- выявления новых форм и типов социальной идентификации, неравенства и гражданской активности;

- формулирования направлений для эмпирических исследований (например, изучение факторов цифрового разрыва, динамики доверия к цифровым институтам, изменений в социальной идентичности) и т.д.

Разработанная модель становится не только теоретическим, но и прикладным инструментом для анализа и прогнозирования социальных процессов в условиях цифровизации общества.

Ввиду того, что концептуальная модель цифрового суверенитета личности предлагает многоуровневый и междисциплинарный подход к обеспечению прав, возможностей и ответственности человека в цифровом пространстве через взаимодействие трех ключевых уровней: государства, организации и личности, целесообразно предложить набор практических рекомендаций по применению данной модели на каждом из этих уровней и межуровневом взаимодействии.

Рекомендации на государственном уровне.

- Разработка и совершенствование нормативно-правовой базы, в том числе при разработке и внесении поправок в национальные и федеральные проекты, федеральные программы и проекты («Цифровая экономика», «Цифровая трансформация», «Развитие науки, промышленности и технологий» и др.), создание правовых механизмов, обеспечивающих право граждан «быть забытыми» в цифровом пространстве, а также установление прозрачных правил для мониторинга и контроля деятельности монополистических ИТ-структур;

- совершенствование национальной цифровой инфраструктуры, в том числе создание государственных цифровых платформ для безопасного обмена информацией и предоставления государственных услуг;

- внедрение обязательных образовательных программ по цифровой грамотности на всех уровнях образования, а также разработка образовательных ресурсов, направленных на повышение уровня осведомленности граждан об их цифровых правах, ответственности и их цифровом суверенитете;

Рекомендации на уровне организаций.

- Обучение сотрудников, в том числе внедрение программ по развитию цифровых навыков и адаптации к новым технологиям, а также формирование культуры ответственного отношения к данным и информационной безопасности внутри организации;

- разработка методов и механизмов для обеспечения прозрачности в вопросах обработки и хранения персональных данных сотрудников и клиентов, а также оценка соответствия практик обработки данных внутренней политике и внешним требованиям;

Рекомендации на уровне личности.

- Повышение уровня цифровой грамотности посредством развития критического мышления для оценки достоверности информации в цифровом пространстве;

- регулярное ознакомление с политиками конфиденциальности цифровых сервисов и онлайн-платформ перед их использованием;

- осознанное поведение в цифровой среде через регулярный аудит личных цифровых следов и удаление ненужной информации из сети, формирование привычки проверять источники информации перед ее распространением;

- самостоятельное действие в цифровом пространстве посредством активного использования возможностей настройки приватности в цифровых сервисах и выбора альтернативных технологических решений, обеспечивающих большую защиту личных данных.

Механизмы взаимодействия между уровнями модели.

- Создание многосторонних платформ для диалога, в том числе организация регулярных форумов с участием представителей государства,

бизнеса и гражданского общества по вопросам цифрового суверенитета, а также поддержка инициатив, направленных на повышение осведомленности о цифровом суверенитете на всех уровнях;

- разработка системы индикаторов для мониторинга уровня цифрового суверенитета на каждом из трех уровней.

Практическое применение многоуровневой модели цифрового суверенитета личности требует скоординированных действий на уровне государства, организаций и граждан. Государство обеспечивает правовую основу и создает условия для защиты цифровых прав, организации внедряют необходимые технологические и организационные меры, а личность активно развивает навыки безопасного и осознанного поведения в цифровой среде.

Только при системном подходе, учитывающем взаимосвязи между всеми тремя уровнями, возможно эффективное обеспечение цифрового суверенитета личности в современном цифровом обществе. Развитие концепции цифрового суверенитета способствует не только защите прав и свобод граждан, но и укреплению доверия пользователей к современным технологиям, что является фундаментом устойчивого цифрового развития.

ЗАКЛЮЧЕНИЕ

Развитие современных цифровых технологий в мире и России и их интеграция в различные сферы жизнедеятельности общества расширяют возможности граждан свободно выражать мнение, активно участвовать в социальной жизнедеятельности и обсуждении значимых социальных вопросов в сети Интернет.

В условиях быстрого развития технологий и повсеместного распространения цифровых платформ современные общества сталкиваются с новыми вызовами, связанными с защитой личных данных, приватностью и контролем над цифровой идентичностью. Социальные сети, онлайн-сервисы и мобильные приложения собирают огромные объемы информации о пользователях, что приводит к необходимости глубже понять, как индивиды воспринимают свою безопасность и автономию в цифровом пространстве. Процесс глобализации и интеграции технологий создает новые возможности, но одновременно и усиливает риски, связанные с манипуляцией данными, утечками информации и несанкционированным доступом к личным данным. В этом контексте социологический анализ цифрового суверенитета личности позволяет выявить не только индивидуальные, но и социальные, культурные и политические аспекты, влияющие на формирование отношения людей к своему цифровому «я».

Цифровой суверенитет личности является многогранной концепцией, объединяющей в себе не только вопросы идентичности, но и механизмы защиты персональных данных, права на конфиденциальность, приватность, контроль над цифровой информацией и доступ к ней, а также вопросы ответственности и этического поведения в информационном пространстве.

Возникшая на ранних этапах развития Интернета идея о независимом цифровом пространстве, созданном вне территориальных границ, свободном от государственного регулирования и вмешательства, существующем со

своими правилами, правами и ответственностью пользователей, привела к пониманию необходимости сохранения цифрового суверенитета личности.

Исследователи подчеркивают, что именно люди и их индивидуальные коммуникации являются основными носителями суверенитета в киберпространстве. Благодаря силе и возможностям технологических корпораций государство зачастую не может в полном объеме обеспечивать безопасность коммуникаций своих граждан в Интернете, а это означает, что теперь на последних лежит необходимость защиты собственного личного цифрового суверенитета.

Развитие цифрового суверенитета личности во многом связано с ускорением цифровой трансформации и появлением более совершенных информационно-коммуникационных технологий. Учитывая доминирующее положение крупных технологических гигантов в области облачных вычислений и социальных сетей (Yandex, Google и тд.), данные практически каждого человека и организации в каком-то виде хранятся и обрабатываются неизвестным образом в облаке этих компаний, что может потенциально привести к нарушению фундаментальных прав человека и угрозе суверенитету человека в цифровом пространстве, приватности его персональных данных и конфиденциальности индивидуальных коммуникаций.

Одним из ключевых элементов цифрового суверенитета личности является концепция суверенной идентичности, обеспечивающая для индивидов возможность активного участия в цифровом пространстве и защиты своих интересов. По результатам анализа мнений участников фокус-группы были выделены ключевые принципы, позволяющие сформировать суверенную идентичность в информационном пространстве, в числе которых существование, контроль, доступ, совместимость, портативность и др.

Как показало исследование, цифровой суверенитет связан со способностью общества, государства, организации и личности к инновациям или внедрению технологических решений. Важным аспектом цифрового суверенитета является безопасность и неприкосновенность частной жизни как

отдельных граждан, так и коллективов. Это также касается владения и контроля над информационными данными, относящимися к обществу или государству. За концепцией цифрового суверенитета нередко стоит стремление создать противовес крупным транснациональным ИТ-компаниям. Дискурс о суверенитете, как правило, становится более актуальным в ситуациях, когда наблюдается слабость власти над объектом.

Отдельное внимание следует уделить выявлению и анализу рисков, связанных с утратой цифрового суверенитета личности. Анализ данных экспертного опроса и материалов фокус-групп позволил выделить такие риски, как снижение правовой защиты в Интернете и ответственности государственных и частных структур, интернет-зависимость и проблемное использование интернета, культура отмены и социальная инженерия, риски для конфиденциальности и безопасности в Интернете, риски автоматизированного принятия решений, в том числе связанные с профилированием, цифровая мобильность и т.д. Данные риски и угрозы оказывают большое влияние на динамику развития социальных процессов и возникновения новых социальных институтов. На основе экспертного опроса были сделаны выводы о том, что приоритетом для человека является конфиденциальность и защита личной информации, а также растущее недовольство по поводу практик сбора данных со стороны компаний и платформ, чрезмерным контролем и цензурой.

Цифровой суверенитет личности выступает в качестве важного элемента современного социокультурного контекста, в котором индивиды должны обладать не только правами, но и ответственностью за свои действия в цифровом пространстве. В условиях стремительного развития технологий и увеличения количества угроз, связанных с ними, возникает необходимость в более глубоком изучении данного аспекта, что открывает новые горизонты для социологических исследований и практической деятельности в сфере защиты цифровых прав личности.

Результаты исследования не только подтверждают гипотезу, но и демонстрируют, как взаимодействие между государственным, организационным и индивидуальным уровнями формирует цифровой суверенитет личности. Это взаимодействие, основанное на принципе синергетического подхода, влияет на динамику и регулирование социальных отношений в условиях цифровой среды, что подчеркивает необходимость комплексного анализа и разработки мер по защите прав и свобод граждан в цифровом обществе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Агеева А.В., Красноцветов Г.В. «Мягкая сила» в онлайн-пространстве: практический опыт применения технологий интернет-коммуникации //Власть. - 2020. - Том 28. - №2. - С.96-100.

2. Азизов Р.Ф. Электронное правительство как элемент электронного государства //Ученые труды Российской академии адвокатуры и нотариата. - 2014. - №4 (35). - С.22-27.

3. Амелин Р.В., Чаннов С.Е. Прямая электронная демократия в Российской Федерации: возможности и перспективы //Конституционное и муниципальное право. - 2017. - №1. - С.27-31.

4. Аничкин Е.С. Модернизация конституционно-правового статуса личности в условиях формирования цифрового пространства //Конституционное и муниципальное право. - 2019. - №12. - С.19-22.

5. Антонов Я.В. Конституционно-правовые перспективы развития электронной демократии в современной России //Конституционное и муниципальное право. - 2016. - №9. - С.17-20.

6. Архипов В.В., Наумов В.Б. Сквозные правовые проблемы Интернета вещей и пределы права: российская перспектива // Труды Института государства и права РАН. 2018. Т. 13. № 6. С. 94-123. С.97.

7. Аршинов В.И. Цифровая реальность в оптике постнеклассической парадигмы сложностности //Проектирование будущего. Проблемы цифровой реальности: труды 1-й Международной конференции (8-9 февраля 2018 г.,

Москва). - М., 2018. - С.147-151 [Электронный ресурс]. Режим доступа: http: //keldysh.ru/future/2018/22.pdf - (Дата обращения: 01.09.2022).

8. Ашманов И. Битва за рунет. Как добиться цифрового суверенитета? // E-news. 01.11.2019. Режим доступа:https://e-news.su/in-russia/303970-bitva-za-runet-kak-dobitsya-cifrovogo-suvereniteta-igor-ashmanov.html (дата обращения: 20.09.2022).

9. Бек. У. Общество риска. На пути к другому модерну. / Пер. с нем. В.Седельника и Н. Федеровой. М.: Прогресс- Традиция, 2000. 384 С.

10. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования /Перевод с английского, под редакцией В.Л.Иноземцева. -М.: «Academia», 2004 (ОАО Можайский полиграфический комбинат). - 786 с.

11. Бестужев-Лада И. Альтернативная цивилизация: актуальность социологического осмысления // Социология на пороге XX века: Основные направления исследований. / Под ред. С.И. Григорьева (Россия), Ж. Коэтен-Хуттера (Швейцария). М.: РУСАКИ, 1999. С.34-49.

12. Бродовская Е.В. Цифровые граждане, цифровое гражданство и цифровая гражданственность //Власть. - 2019. - Том 27. - №4. - С.65-69.

13. Богучарский А.А. Сетевое общество 21 века: влияние информационных технологий и виртуальной социализации на участие граждан в политических процессах политической жизни государства //Экономические и гуманитарные исследования регионов. - 2018. - №2. - С.53-58.

14. Бочков А.А. Современное государство и право в условиях цифровой реальности //Право. Экономика. Психология. - 2019. - №1 (13). - С.3-9.

15. Бредихин А.Л. Суверенитет как политико-правовой феномен: Монография. - М.: Издательский дом «Инфра-М», 2020. - 128 с.

16. Бурдье П. Практический смысл / Пер. с фр.: А. Т. Бикбов, К. Д. Вознесенская, С. Н. Зенкин, Н. А., Шматко; Отв. ред. пер. и Послесл. Н. А. Шматко. — СПб.: Алетейя, 2001 г. — 562 с.

17. Варламова Н.В. Цифровые – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Т. 14. № 4. С. 9-46. с. 12-13.

18. Василенко Л.А. Социология цифрового общества : монография / Л.А. Василенко, Н.Н. Мещерякова ; Томский политехнический университет. – Томск : Изд-во Томского политехнического университета, 2021.

19. Василенко Л.А., Мещерякова Н.Н.. Гибридность цифрового общества. Философия науки и техники 2023. Т. 28. № 1. С. 48–65

20. Васильев А.А., Шпопер Д. Государство и право перед вызовами новой научно-технологической реальности //Алтайский юридический вестник. -2019. - №3 (27). - С.7-10.

21. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. 2020. № 4. С. 3–11

22. Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой // Вестник КемГУ. Гуманитарные и общественные науки. 2020. - 4(2). - С.146-152.

23. Гидденс Э., Саттон Ф. Основные понятия в социологии. / пер. с англ. Е. Рождественской, С. Гавриленко; под науч.ред. С. Гавриленко. М.: Изд-дом Высшей школы экономики, 2021. – 336 с.

24. Гидденс Э. Устроение общества: Очерк структурации. – М.: Академический проект, 2023. – 528 с.

25. Государство и право в новой цифровой реальности: Монография /Редакторы-составители: Ловцов Д.А., Конюхова (Умнова) И.А. - М.: Институт научной информации по общественным наукам РАН, 2020 [Электронный ресурс]. Режим доступа: http: //inion.ru/ru/publishing/publications/gosudarstvo-i-pravo-v-novoi-tcifrovoi-realnosti/ - (Дата обращения: 30.08.2022).

26. Градоселъская Г.В. Сетевые измерения в социологии /Под редакцией Г.С.Батыгина. - М.: Издательский дом «Новый учебник», 2004. - 248 с.

27. Гуров О. Н., Петрунина М. А. (2020). Цифровая трансформация: человеческое измерение // Гуманитарный вестник. №2 (82). URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-chelovecheskoe-izmerenie (дата обращения: 09.11.2023).

28. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной Сети Интернет //Lex Russica. -2017. - №7 (128). - С.154-165.

29. Девятова С.В., Казарян В.П. Многомерность проблемы коммуникации в цифровом обществе //Российский гуманитарный журнал. - 2020. - Том 9. -№3. - С.165-173.

30. Деева Н.В. Тенденции развития российского гражданского общества в эпоху цифровизации //Гражданин. Выборы. Власть. - 2020. - №1 (15). - С.82-91.

31. Друкер П.Ф. Управление в обществе будущего /Перевод с английского и редакция Е.В.Трибушной. - М.: Издательство «Вильямс», 2007. - 306 с.

32. Ефремов А.А. Конституционные основы и законодательное обеспечение государственного суверенитета РФ в информационном пространстве //Государственная власть и местное самоуправление. - 2016. - №12. - С.39-43.

33. Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал высшей школы экономики. - 2017. - № 1. - С. 201-215.

34. Жижина М.В. Блогер в социальных представлениях молодежи //III Ломоносовские чтения. Актуальные вопросы фундаментальных и прикладных исследований. Сборник статей Международной научно-практической конференции (Петрозаводск, 14.11.2019). - Петрозаводск, 2019. - С.46-50.

35. Жужлов А. Гражданское общество и Интернет-технологии //Власть. - 2010. - №8. - С.82-84.

36. Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума //Российская газета (столичный выпуск). - №115 (7578). - 29.05.2018.

37. Каминская Т.Л. Блогер как актор развития онлайн-журналистики //Медиалингвистика. - 2014. - №53. - С.191-193.

38. Капустина А.Г. Правовой статус субъектов информационно-коммуникативной деятельности в Интернете //Актуальные проблемы гуманитарных и естественных наук. - 2015. - №11-7. - С.43-46.

39. Карпова А.Е. Государственный суверенитет в современных условиях //Молодой ученый. - 2016. - №23. - С.334-336.

40. Кастелъс М. Власть коммуникации /Перевод с английского Н.М.Тылевич; предисловие к изданию 2013 года А.А.Архиповой; под научной редакцией А.И.Черных. 2-е издание, дополненное. - М.: Издательский дом Высшей школы экономики, 2017. - 591 с.

41. Кастельс М. Информационная эпоха: экономика, общество и культура: Пер. с англ. под науч. ред. О.И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.

42. Киселев А.С. Современные теоретические подходы к понятию электронного государства //Актуальные проблемы российского права. - 2018. - №6 (91). - С.32-39.

43. Ковлер А.И. Права человека в цифровую эпоху //Бюллетень Европейского суда по правам человека. - 2019. - №6 (204). - С.146-150.

44. Кожемякин Е.А., Попов А.А. Блоги как средство журналистской коммуникации //Научные ведомости Белгородского государственного университета. Серия: гуманитарные науки. - 2012. - №6 (125). - Выпуск 13. - С.148-155.

45. Комарова А. В. Динамика информационно-коммуникационных процессов и их влияние на социокультурные институты // Верхневолжский филологический вестник. 2024. № 3 (38). С. 223–233. http://dx.doi.org/10.20323/2499-9679-2024-3-38-223. https://elibrary.ru/ZNLRQT

46. Конобеевская И. М. Цифровые права как новый объект гражданских прав // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. - 2019. - Т. 19. - № 3. - С. 330-334.

47. Кочетков Александр Павлович, Маслов Константин Вадимович Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. №2.

48. Коэн Д., Шмидт Э. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств /Перевод с английского С.Филина. - М.: Издательство «Манн, Иванов и Фербер», 2013. - 368 с.

49. Кравцов Д.В., Леонов Е.А. Разработка автоматизированной системы мониторинга информации в сети Интернет в целях борьбы с распространением идей терроризма и экстремизма. Наука и образование против террора - 2010: сборник работ участников Первого Открытого Конкурса «Наука и образование против террора - 2010». - М: МГТУ им. Баумана, 2011. - С.52-61.

50. Кравченко, С. А. Социология риска и безопасности: учебник и практикум для вузов / С. А. Кравченко. — Москва : Издательство Юрайт, 2023. — 272 с.

51. Кравченко, С. А. Социология цифровизации : учебник для вузов / С. А. Кравченко. - Москва : Издательство Юрайт, 2021. - 236 с. - (Высшее образование). - ISBN 978-5-534-14307-2.

52. Курячая М.М. Электронное голосование как этап развития непосредственной демократии //Конституционное и муниципальное право. - 2017. - №11. - С.31-35.

53. Лазинина Е.В.Коммуникативные процессы в виртуальной реальности цифрового общества. Монография. Ставрополь, 2023 г.

54. Лакатос И. Избранные произведения по философии и методологии науки / Пер. с англ. И.Н. Веселовского, А.Л. Никифорова, В.П. Поруса. М.: Академический проект, Трикста, 2008. – С. 475.

55. Мамут Л.С. «Сетевое государство»? //Государство и право. -2005. - №11. - С.5-12.

56. Масловская Т.С. Цифровая сфера и конституционное право: грани взаимодействия //Конституционное и муниципальное право. - 2019. - №9. - С.18-22.

57. Махаматов Т.М. Перспективы демократии и роль гражданского общества в цифровом пространстве //Философское образование. - 2018. - №1 (37). - С.28-33.

58. Международное право. Учебник под. Ред. А.А. Ковалева, С.В. Черниченко. М. -2008 – С.49-50

59. Нарушева П.Ю. Основные черты блога и его роль в жизни современного человека //Вестник молодых ученых и специалистов Самарского университета. - 2017. - №1. - С.38-43.

60. Невинский В.В. «Цифровые права» человека: сущность, система, значение //Конституционное и муниципальное право. - 2019. - №10. - С.26-32.

61. Нестеров А.В. О цифровых правах и объектах цифровых прав //Право и цифровая экономика. - 2020. - №1 (07). - С.11-16.

62. Нейсбит Дж. Мегатренды /Перевод с английского М.Б.Левина. -М.: АСТ: Ермак, 2003. - 380 с.

63. Пастухова Н.Б. Суверенитет и федеративная организация российского государства в условиях глобализации: конституционно-правовые аспекты. Автореферат дисс. Доктора. Юр. наук.,М.: 2010. 46 с.

64. Перова М. В., Волковская И. В., Максимова А. М. Цифровой суверенитет как приоритет государственной политики на современном этапе // Вызовы современности и стратегии развития общества в условиях новой реальности: сборник материалов VI Международной научно-практической конференции, Москва, 21 февраля 2022 года / редколлегия: Л. К. Гуриева, З. Ш. Бабаева [и др.]. Москва: ИП Овчинников Михаил Артурович (Типография Алеф), 2022. С. 118—122.

65. Полякова Н.Л. (2016). «Идентичность» в современной социологической теории. Вестн. Моск. Ун-та. Сер. 18. Социология и политология. № 4

66. Проект Концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации // https://rocit.ru/uploads/4f68dc0a2487678a7675ad7589280277050b4004.docx?t=1639585614

67. Рабочая книга социолога / Под общ. ред. и с предисл. Г. В. Осипова. Изд. 5-е. — М.: Книжный дом «ЛИБРОКОМ», 2009. — 480 с. Источник: https://www.isras.ru/publ.html?id=6535

68. Ровинская Т.Л. Киберлибертарианство - новая альтернативная идеология информационного общества в условиях глобализации /В сб. Партийно-политические системы и политические идеологии в странах Запада в

начале XXI века: факторы эволюции и направления трансформации. - М.: Национальный исследовательский институт мировой экономики и международных отношений имени Е.М.Примакова Российской академии наук, 2016. - С.39-43.

69. Рождение коллективного разума. О новых законах сетевого социума и сетевой экономики и об их влиянии на поведение человека. Великая трансформация третьего тысячелетия /Ф.Хейлинг и др.; под редакцией Б.Б.Славина. - М.: URSS, 2013. - 285 с.

70. Славин Б. Когда цифровая демократия не работает //Ведомости. - 12.11.2019. - №212. - С.7 [Электронный ресурс]. Режим доступа: http: //elib.fa.ru/art2019/bv2106.pdf. - (Дата обращения: 01.09.2022).

71. Талапина Э.В. Государственное управление в информационном обществе. Правовой аспект = Public administration in the information society. Legal aspect = L'administration publique dans la société de l'information. L'aspect juridique: монография /Российская академия наук, Институт государства и права. - М.: Издательство «Юриспруденция», 2015. - 188 с.

72. Тарасов А.М. Электронное правительство: понятие и система //Право и кибербезопасность. - 2013. - №2. - С.10-21.

73. Терентъева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве //Lex Russica. - 2019. - №7 (152). - С.119-128.

74. Тимофеева Л.Н. Новая социальность в информационной повестке дня: роль старых и новых медиа //Вестник Воронежского государственного университета. Серия: История. Политология. Социология. - 2020. - №2. - С. 64-69.

75. Тоффлер Э. Третья волна /Переводчики: Барабанов С., Бурмистров К., Бурмистрова Л., Заритовская З., Комарова Е., Кротовская Н., Кулагина-Ярцева В., Микиша А., Москвина-Тарханова И., Руднева Е., Татаринова К., Хмелик Н. Научный редактор П.С.Гуревич. - М.: ООО «Фирма "Издательство АСТ"», 2004. - 261 с.

76. Турчин А.В., Батин М.А. Футурология. XXI век: бессмертие или глобальная катастрофа? - М.: Бином. Лаборатория знаний, 2012. - 263 с.

77. Федотова Ю.Г. Электронная демократия как средство обеспечения информационной безопасности государства //Информационное право. -2016. - №3. - С.17-24.

78. Хабермас Ю. От картин мира к жизненному миру /Habermas J. Von den Weltbildern zur Lebenswelt. - М.: Идея-Пресс, 2011. - 128 с.

79. Харари Ю.Н. Homo Deus. Краткая история будущего. - М.: Синдбад, 2019. - 496 с.

80. Хмелевский С.В. Государственный суверенитет: понятие, содержание, актуальные теоретические и практические проблемы реализации //Пробелы в российском законодательстве. - 2015. - №4. - С.280-286.

81. Хоркхаймер М., Адорно Т. Культурная индустрия. Просвещение как способ обмана масс /Перевод с немецкого: Т.Зборовская. - М.: Ад Мар-гинем Пресс, 2016. - 103 с.

82. Цифровая трансформация и защита прав человека в цифровом пространстве. Доклад Совета при Президенте РФ по развитию гражданского общества и правам человека, М. 2021 https://ifap.ru/pr/2021/n211213a.pdf

83. Черников А. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома // Vc.ru. 28.01.2020. Режим доступа: https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma (дата обращения: 20.09.2022).

84. Черняк Л. Ю. К вопросу о понятии информационного суверенитета: теоретический и сравнительно-правовой аспекты // Сибирский юридический вестник. - 2012. - № 3. - С. 117-122.

85. Шваб К. Четвертая промышленная революция. - М.: Издательство «Эксмо», 2016. - 138 с. [Электронный ресурс]. Режим доступа: http: //ncrao.rsvpu.ru/sites/default/files/library/k._shvab_chetvertaya_promyshlennaya_revolyuciya_2016.pdf. - (Дата обращения: : 01.09.2022).

86. Шестопал С. С., Мамычев А. Ю. Суверенитет в глобальном цифровом измерении: современные тренды // БГЖ. 2020. №1 (30). URL: https://cyberleninka.ru/article/n/suverenitet-v-globalnom-tsifrovom-izmerenii-sovremennye-trendy (дата обращения: 21.08.2023).

87. Эрделевский А.М. О цифровых правах //ЮрФак: изучение права онлайн. - 26.06.2019 [Электронный ресурс]. Режим доступа: https: //urfac.ru/?p=2342. - (Дата обращения: 30.08.2022).

88. AI HLEG: High-level expert group on artificial intelligence: the assessment list for trustworthy artificial intelligence (ALTAI). https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (2020).

89. Alboaie S and Cosovan D. Private data system enabling self-sovereign storage managed by executable choreographies. Lecture Notes in Computer Science LNCS 10320, 2017, 83–98. P. 86

90. Allen, C. «The Four Kinds of Privacy». Life With Alacrity blog. 2015. /2015/04/the-four-kinds-of-privacy.html

91. Allen, C. «The Path to Self-Sovereign Identity», Life With Alacrity, 2016.

92. Baischew, D., Kroon, P., Lucidi, S., Märkel, C., Sörries, B.: Digital sovereignty in Europe: a first benchmark. Wik-consult report, Bad Honnef , 2020. http://hdl.handle.net/10419/251539

93. Bannister F., Gronlund A. Information Technology and Government Research: A Brief History //Proceedings of the 50th Hawaii International Conference on System Sciences, 2017. - P.2943-2952 [Electronic resource]. Режим доступа: https: //scholarspace.manoa.hawaii.edu/bitstream/10125/41512/1/paper0363.pdf. - (Дата обращения: 30.08.2022).

94. Baumgartner S.E. , W.A. van der Schuur, J.A. Lemmens, F. te Poel The relationship between media multitasking and attention problems in adolescents: Results of two longitudinal studies Human Communication Research, 44 (1). 2018, pp. 3-30

95. Beauchamp TL and Childress JF. Principles of Biomedical Ethics. Oxford and New York: Oxford University Press. 2013, P. 104-105

96. Bellanger P. De la souveraineté numérique. Le Débat 170(3), 2012, 149–159. P. 154

97. Benedek, W.: International organizations and digital human rights. In: Wagner, B., Kettemann, M.C., Vieth, K. (eds.) Research Handbook in Human Rights

and Digital Technology. Global Politics, Law and International Relations, 2019, pp. 364–375. Edward Elgar Publishing.

98. Bhandar B. The conceit of sovereignty: toward post-colonial technique. In: Lessard B (ed.) *Stories Communities: Narratives of Contact and Arrival in Constituting Political Community*. Vancouver, BC, Canada: University of British Columbia Press, 2011, pp. 66–88.

99. BITKOM: Digitale Souveränität. Datenschutz und Datensicherheit - DuD 42(5), 2018, 294–300. https://doi.org/10.1007/s11623-018-0944-y

100. Bogenstahl, C., Zinke, G. Digitale Souveränität - ein mehrdimensionales Handlungskonzept für die deutsche Wirtschaft. Digitale Souveränität, 2017, p. 65

101. Cheesman, M., «Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity», Geopolitics, 2020, pp. 1–26

102. Coulthard SG. Red Skin, White Masks: Rejecting the Colonial Politics of Recognition. Minneapolis, MN: University of Minnesota Press. 2014.

103. Courtney M. Regulating the cloud crowd. Engineering & Technology 8(4): 2013, 60–63. P. 60

104. Couture, S., & Toupin, S. What does the notion of "sovereignty" mean when referring to the digital? New media and society, 21(10), 2019, 2305–2322.

105. D. D'Orazio. Deplatforming in Theory and Practice: The Ann Coulter Debacle. In E. Macfarlane, eds., Dilemmas of free expression (Toronto: University of Toronto Press, 2022), p. 269.

106. Dworkin G. Autonomy and behavior control. The Hastings Center Report 6(1): 1976, pp. 23–28.

107. Digital E. , « EIT Digital Report on European Digital Infrastructure and Data Sovereignty » . 2020. Режим доступа: https://www.earto.eu/eitdigital- report-on-european-digital-infrastructure-and-data-sovereignty/

108. Esposito C, Castiglione A and Choo KKR. Encryption-Based Solution for Data Sovereignty in Federated Clouds. IEEE Cloud Computing 3(1): 12–17. 2016, P. 14

109. Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., Wendeborn, T. Towards a Layer Model for Digital Sovereignty: A Holistic Approach.

In: Hämmerli, B., Helmbrecht, U., Hommel, W., Kunczik, L., Pickl, S. (eds) Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723. Springer, Cham. 2023. Режим доступа: https://doi.org/10.1007/978-3-031-35190-7_9

110. Friedrichsen, M., Bisa, P.J.: Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft, 2016

111. Frederking, V., Krommer, A.: Digitale Textkompetenz: Ein theoretisches wie empirisches Forschungsdesiderat im deutschdidaktischen Fokus, 2019. https://bit.ly/38fJoRU

112. Haché A. La souveraineté technologique. *Dossier Ritimo*. 2014. Режим доступа: https://www.ritimo.org/IMG/pdf/dossier-st1.pdf P. 11

113. Hartmann, E.A. Digitale souveränität: soziotechnische bewertung und gestaltung von anwendungen algorithmischer systeme. In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten II, 2022, pp. 1–13. Springer, Heidelberg https://doi.org/10.1007/978-3-662-64408-9_1

114. Garrison NA, Hudson M, Ballantyne LL, et al. Genomic research through an indigenous lens: Understanding the expectations. Annual Review of Genomics and Human Genetics 20, 2019. P. 495.

115. Hartmann, E.A.: Digitale souveränität in der wirtschaft – gegenstandsbereiche, konzepte und merkmale. In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten, pp. 1–16. Springer, Heidelberg, 2021. https://doi.org/10.1007/978-3-662-62377-0_1

116. Hinsley FH/ *Sovereignty*. 2nd ed. Cambridge, MA: Cambridge University Press. 1986.

117. Hippelainen L, Oliver I and Lal S. Towards dependably detecting geolocation of cloud servers. In: Yan Z, et al. (eds) Network and System Security. Cham: Springer, 2017. pp.643–656. P. 645

118. Hollis DB. *Stewardship Versus Sovereignty? International Law and the Apportionment of Cyberspace* (ID 2038523, SSRN scholarly paper, 19 March). Rochester, NY: Social Science, 2012.

119. Horgan D., Dimitrijevic B. Frameworks for citizens participation in planning: from conversational to smart tools //Sustainable Cities and Society. - 12 Apr. 2019.

120. Hu TH. A Prehistory of the Cloud. Cambridge, MA: The MIT Press.-№48, 2015 Режим доступа: https: //doi.org/10.1016/j.scs.2019.101550.

121. Internet Rights & Principles Coalition. (2014). The Charter of Human Rights and Principles for the Internet., 2014 Режим доступа:https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

122. Irion K. Government cloud computing and national data sovereignty. Policy & Internet 4(3–4): 2012, 40–71. P . 41

123. Ishmaev, G., «Sovereignty, privacy, and ethics in blockchain-based identity management systems», Ethics and Information Technology, 2020, pp. 1–14.

124. Jenderny, S., Foullois, M., Kato-Beiderwieden, A.-L., Bansmann, M., Wöste, L., Lamß, J., Maier, G. W., Röcker, C.: Development of an instrument for the assessment of scenarios of work 4.0 based on socio-technical criteria. In: PETRA '18: Proceedings of the 11th PErvasive Technologies Related to Assistive Environments. Conference June 2018.

125. Keonig PD. The place of conditionality and individual responsibility in a “data-driven economy”. 2017, Big Data & Society 4(2): 205395171774241

126. Kheng Leong, Tan, Chi-Hung, Chi, and Kwok-Yan, Lam. Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization // 2022, Режим доступа: https://arxiv.org/abs/2202.10069

127. Kukutai T and Cormack D. Census 2018 and implications for M_aori. New Zealand Population Review 44: 2018, 131–151. P. 145

128. Lehmann, C., Dörr, L. Digital souveräne gestaltung von services – ein marktfähiger mehrwert? In: Hartmann, E.A. (ed.) Digitalisierung souverän gestalten II, 2022, pp. 14–24. Springer, Heidelberg P. 14. https://doi.org/10.1007/978-3-662-64408-9_2

129. Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, 33 PHILOSOPHY AND TECHNOLOGY 369, 371 , 2020.

130. Maréchal, N. Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication, 2017,* 5(1), pp.29-41.

131. McKinlay, R. Technology: Use or lose our navigation skills. Nature, 573–575. 2016. https://doi.org/10.1038/531573a

132. Mueller M. Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Malden, MA: Polity, 2017.

133. Niël Henk Conradie, Saskia K. Nagel. Digital sovereignty and smart wearables: Three moral calculi for the distribution of legitimate control over the digital. Journal of Responsible Technology. Volume 12, December 2022

134. Niker F. , G. Felsen, S.K. Nagel, P.B. Reiner Autonomy, evidence-responsiveness, and the ethics of influence The law and ethics of freedom of thought, Palgrave-Macmillan, Cham, 2021.

135. Nitot T. Numérique : reprendre le contrôle. Paris: Framasoft. Available at: https://framabook.org/docs/NRC/Numerique_ReprendreLeControle_CC-By_impress.pdf P.3, 2016.

136. Nugraha Y, Kautsarina K and Sastrosubroto AS (2015) Towards data sovereignty in cyberspace. In: 2015 3rd international conference on information and communication technology (ICoICT), Nusa Dua, Indonesia, 27–29 May 2015, pp.465–471.

137. Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock. Data sovereignty: A review Big Data & Society 2021 8:1

138. Pentenrieder, A., Bertini, A., Künzel, M. Digitale Souveränität als Trend? Digitalisierung souverän gestalten. 2021, Режим доступа. https://doi.org/10.1007/978-3-662-62377-0_2

139. Peters A. Humanity as the A and Ω of sovereignty European Journal of International Law, 20 (3), 2009, pp. 513-544

140. Philpott D. Sovereignty. *Stanford Encyclopedia of Philosophy Archive*, 31 May. Page 3, Available at: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/.

141. Pohle, J.: Digitale Souveränität. Handbuch Digitalisierung in Staat und Verwaltung, 2020. https://doi.org/10.1007/978-3-658-23669-4_21-1

142. Rainie SC, Schultz JL, Briggs E, et al. Data as a strategic resource: Self-determination, governance, and the data challenge for indigenous nations in the United States. International Indigenous Policy Journal 8(2). 2017, P 5-6

143. Stets, Jan E. and Peter J. Burke. "The Development of ldentity Theory." Advances in Group Processes 31, 2014, pp. 57-97

144. Stets, Jan E. and Peter J. Burke. "Emotions and Identity Non-Verification." Social Psychology Quarterly 77, 2014. 387-410. P.390

145. Tiina Pajuste (ed.), Specific Threats to Human Rights Protection from the Digital Reality. Tallinn: Tallinn University, 2022

146. Thorsten Busch, Fair Information Technologies: The Corporate Responsibility of Online Social Networks as Public Regulators 71, 2013 https://www.alexandria.unisg.ch/228863/

147. Tomalty, J. Is There a Human Right to Internet Access?. *Philosophy Now*, 2017, pp.6-8. Режим доступа: https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access

148. Ulich, E. Arbeitssysteme als soziotechnische Systeme – Eine Erinnerung. J. Psychol. Alltagshandelns 6(1), 2013, 4–12

149. Watt, E. The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7), 2017, pp.773-799. P.788

150. Werner WG and De Wilde JH. The Endurance of sovereignty. European Journal of International Relations 7(3), 2001, P 307

151. Woods AK. Litigating data sovereignty. Yale Law Journal 128(2), 2018, 328–406. P. 335

ПРИЛОЖЕНИЕ 1. РЕЗУЛЬТАТЫ ЭКСПЕРТНОГО ОПРОСА «Цифровой суверенитет личности»

В экспертном опросе приняли участие 217 человек из различных сфер общественной жизни (таблица 1), из которых представителей ИТ блока, в том числе занимающихся вопросами информационной безопасности и защитой персональных данных - 78 человек.

Сфера	Количество человек	Процент
ИТ структура	78	36%
ВУЗ	41	19%
финансовая организация, страховая организация, бизнес-организация	45	21%
государственный и муниципальный орган	31	14%
общественная организация	13	6%
частная организация, индивидуальный предприниматель	9	4%

А Н К Е Т А

Уважаемый коллега!

Просим Вас принять участие в экспертном опросе по вопросам исследования цифрового суверенитета личности. Ваше мнение окажет существенную помощь в решении научных и практических задач по выявлению механизмов формирования цифрового суверенитета личности.

Внимательно ознакомьтесь с вопросами и отметьте порядковые номера ответов, отражающих Ваше мнение.

Заранее благодарим за участие в исследовании!

* * * * * * *

1. ПО ВАШЕМУ МНЕНИЮ, ЧТО ВХОДИТ В ОСНОВУ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ? *(ответьте, пожалуйста, по каждой строке)*

№		Да	Нет	Не знаю
1.	возможность независимо и самостоятельно высказывать свое мнение в цифровом пространстве	69,1%	16,6%	14,3%
2.	возможность выбора информационного контента в Интернете	77,9%	14,3%	7,8%
3.	возможность получения государственных услуг как в личном присутствии (офлайн), так и на цифровых платформах (онлайн)	78,3%	14,3%	7,4%
4.	защищенность от указания своих персональных данных в процессе доступа к информационным ресурсам и сервисам	78,3%	11,5%	10,1%

5.	возможность отказа от предоставления своих персональных данных	77%	11,5%	11,5%
6.	обязательное согласие человека при использовании его цифрового профиля и персональных данных	77,4%	14,3%	8,3%
7.	установление ответственности за разглашение и утечку персональных данных	86,2%	8,3%	5,5%
8.	защищенность от мошенников, использующих персональные данные, применяющих цифровой буллинг, распространяющих фейки (ложную информацию)	83,4%	8,3%	8,3%
9.	защищенность от отслеживания персональной геолокации	88,5%	6,5%	5,1%
10.	другое (напишите) _____			

2. ПРОДОЛЖИТЕ ПРЕДЛОЖЕНИЕ:
Я буду обладать цифровым суверенитетом, если

_____
_____
_____
_____

3. КАК ВЫ, В ЦЕЛОМ, ОЦЕНИВАЕТЕ ЗАЩИЩЕННОСТЬ ВАШЕГО ЛИЧНОГО ЦИФРОВОГО СУВЕРЕНИТЕТА?

	Ответы респондентов
отлично	8,3%
хорошо	18%
удовлетворительно	53,5%
плохо	14,7%
очень плохо	1,4%
затрудняюсь ответить	4,1%

4. ЧТО МОЖЕТ СДЕЛАТЬ ЧЕЛОВЕК ДЛЯ СОХРАНЕНИЯ СВОЕГО ЦИФРОВОГО СУВЕРЕНИТЕТА? *(можно выбрать любое количество ответов)*

1.	осознавать личную ответственность за свои личные действия в цифровом пространстве	81,1%
2.	соблюдать этические нормы работы в Интернете	56,7%
3.	знать нормативные акты, не нарушать государственные требования информационного законодательства	51,2%
4.	выполнять требования цифровых платформ и социальных сетей	37,8%
5.	самому контролировать использование своих персональных данных	53,5%
6.	повышать собственную цифровую грамотность	69,6%
7.	осознавать риски использования «умных» устройств (часы, смартфоны, гаджеты)	56,7%
8.	другое (напишите) _____	
9.	затрудняюсь ответить	

5. НА ВАШ ВЗГЛЯД, КАКИЕ ИЗ НИЖЕПЕРЕЧИСЛЕННЫХ ПРАВ И СВОБОД ДОЛЖНЫ СОБЛЮДАТЬСЯ В СЕТИ ИНТЕРНЕТ? *(можно отметить любое количество ответов)*

1.	неприкосновенность частной жизни	74,7%
2.	равенство перед законом	77%
3.	свобода совести и религии	58,1%
4.	свобода мысли, мнений и их выражения	50,7%
5.	право на доступ в Интернет	65,9%
6.	право на мирные собрания и свободу объединений	40,6%
7.	право на получение образования	33,2%
8.	право на безопасность и защиту персональных данных	83,9%
9.	право на труд	42,9%
10.	права на защиту потребителей в Интернете	68,7%
11.	право на правовую защиту и справедливое судебное разбирательство	35%
12.	что еще (напишите)	
13.	не знаю	
14.	затрудняюсь ответить	

6. КАКИЕ ОБЯЗАННОСТИ МОГУТ БЫТЬ У ЧЕЛОВЕКА В СЕТИ ИНТЕРНЕТ? *(можно отметить любое количество ответов)*

1.	не нарушать права и свободы других людей	82,9%
2.	соблюдать государственную политику информационной безопасности	70%
3.	не распространять недостоверную и ложную информацию	88,5%
	выполнять требования цифровых платформ и социальных сетей	35,9%
4.	не оскорблять других людей и не клеветать	73,3%
5.	не распространять противозаконные идеи	74,2%
6.	не использовать персональные данные другого пользователя без его согласия	83,9%
7.	не нарушать авторские или смежные права в Интернете	57,6%
8.	проходить обязательную авторизацию в сети Интернет	18,4%
9.	что еще (напишите)	
10.	не знаю	
11.	затрудняюсь ответить	

7. КАКИЕ ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ СВОЕГО ЦИФРОВОГО СУВЕРЕНИТЕТА ВЫ ИСПОЛЬЗУЕТЕ *(ответьте, пожалуйста, по каждой строке)*

	технологические аспекты	Знаю и использую	Знаю, но не использую	Знаю частично и использую	Знаю частично и не использую	Не знаю и не использую	Затрудняюсь ответить
1.	использую только проверенные сайты и платформы, «защищенный» Интернет	65%	13%	5%	3%	4%	8%
2.	использую надежное антивирусное программное обеспечение,	76%	13%	3%	4%	1%	3%

3.	регулярно обновляю программные системы безопасности	56%	34%	6%	0%	0%	3%
4.	использую надежные пароли						
5.	копирую и сохраняю личную информацию	42%	42%	2%	1%	4%	1%
6.	обращаюсь в специализированные компании по информационной безопасности	20%	53%	0%	4%	12%	9%
7.	постоянно изучаю новые возможности защиты своего цифрового суверенитета	33%	40%	6%	5%	7%	9%
8.	другое (напишите)_____						

8. КАК ВЫ ДУМАЕТЕ, НАСКОЛЬКО ЗАЩИЩЕНЫ ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ? (ответьте, пожалуйста, по каждой строке)

	место хранения персональных данных	**высокая степень защиты**	**средняя степень защиты**	**низкая степень защиты**	**затрудняюсь ответить**	**не знаю**
1.	в организации, где Вы работаете	62%	28%	6%	1%	4%
2.	в личной переписке	19%	34%	42%	1%	5%
3.	в социальных сетях	16%	28%	51%	1%	4%
4.	в аккаунтах интернет-сервисов и в интернет-магазинах	13%	19%	60%	3%	4%
5.	в государственных и муниципальных информационных системах	27%	50%	17%	0%	6%
6.	в банках, кредитных и страховых и иных организациях	53%	35%	7%	0%	4%
7.	в электронных сервисах государственных и муниципальных услуг	35%	45%	13%	0%	7%

9. СУЩЕСТВУЕТ ЛИ В ОРГАНИЗАЦИИ, В КОТОРОЙ ВЫ РАБОТАЕТЕ, СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ?

1.	да	59%
2.	нет	11%
3.	не знаю	20%
4.	затрудняюсь ответить	10%

10. ЕСЛИ СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ, В КОТОРОЙ ВЫ РАБОТАЕТЕ, СУЩЕСТВУЕТ, ТО КАКИЕ КОНКРЕТНЫЕ МЕРЫ ПРЕДПРИНИМАЮТСЯ? *(можно выбрать не более 5 вариантов ответов)*

№	меры защиты персональных данных	Да	Нет	Не знаю
1.	принятие политики информационной безопасности и норм электронного взаимодействия	73%	11%	15%
2.	наличие отдела по информационной безопасности	66%	18%	12%
3.	использование строгой парольной политики	67%	14%	18%
4	ответственность работников за утечку персональных данных, за разглашение служебной и личной информации	72%	6%	20%
5	ограниченность использования персональных данных, шифрование персональных данных	68%	9%	22%
7	использование «защищенного» Интернета	66%	10%	23%
8	управление доступом к информационным системам предприятия	79%	4%	16%
9	использование специализированных программных инструментов и антивирусного программного обеспечения	79%	7%	13%
10	регулярное обновление приложений, резервное копирование данных	65%	10%	24%
11	контроль за обработкой и использованием персональных данных	76%	3%	19%
12	регулярное обучение сотрудников новым информационным технологиям	52%	21%	26%
13	что еще (напишите)			

11. КАКИЕ ЭЛЕМЕНТЫ ВАШЕЙ РАБОЧЕЙ ДЕЯТЕЛЬНОСТИ КОНТРОЛИРУЮТСЯ В ОРГАНИЗАЦИИ? *(можно выбрать не более 5 вариантов ответа)*

1.	использование рабочего времени	53%
2.	контент на компьютерах	68%
3.	активность в сети Интернет	38%
4.	рабочая почта и переписка	29%
5.	выполнение задач	49%
6.	использование программного обеспечения	54%
7.	личная переписка	8%
8.	использование социальных сетей	12%
9.	типы и виды «умных» носимых устройств	35%
10.	другое (напишите)	0
11.	не знаю	5%
12.	затрудняюсь ответить	6%

12. СКАЖИТЕ, ПОЖАЛУЙСТА, ЧТО КОНКРЕТНО МОЖЕТ СДЕЛАТЬ ЧЕЛОВЕК ДЛЯ ЗАЩИТЫ СВОЕГО ЦИФРОВОГО СУВЕРЕНИТЕТА? *(можно выбрать не более 5 вариантов ответа)*

1.	использовать только проверенные сайты и платформы	77%
2.	знать нормативные акты, не нарушать государственные требования	36%
3.	использовать надежное антивирусное программное обеспечение, регулярно обновлять системы безопасности	65%
4.	использовать надежные пароли, копировать и сохранять информацию	70%
5.	обращаться в специализированные компании по защите цифрового профиля	16%

6.	осознавать личную ответственность при использовании информационных технологий	40%
7.	контролировать использование своего цифрового профиля	35%
8.	повышать собственную цифровую культуру и грамотность	27%
9.	осознавать риски использования «умных» устройств (часы, смартфоны, гаджеты)	17%
10.	соблюдать этические нормы работы в Интернете	13%
11.	отказаться от использования зарубежных программных средств, сервисов и систем	19%
12.	другое (напишите) _____	
13.	не знаю	
14.	затрудняюсь ответить	

13. ЧТО КОНКРЕТНО ДОЛЖНЫ СДЕЛАТЬ ИНФОРМАЦИОННЫЕ ПЛАТФОРМЫ И ОРГАНИЗАЦИИ ДЛЯ СОХРАНЕНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ? *(можно выбрать не более 5 вариантов ответа)*

1.	развивать политику информационной безопасности	68%
2.	внедрять системы по контролю утечек персональных данных работников	56%
3.	внедрять передовые стандарты и лучшие практики в сфере информационной безопасности	50%
4.	создать системы фильтрации, ограничивающие доступ к запрещенному контенту	36%
5.	установить ответственность за разглашение служебной и личной информации	53%
6.	обучать сотрудников новым информационным технологиям и основам информационной безопасности	38%
7.	использовать как цифровой, так и аналоговый форматы коммуникаций и документооборота	20%
8.	развивать корпоративную культуру и этические нормы электронного взаимодействия	16%
9.	осуществлять цифровую трансформацию организации	13%
10.	ответственно подходить к использованию систем искусственного интеллекта	27%
11.	соблюдать принципы прозрачности деятельности	2%
12.	внедрять широкодоступные технологии (open source)	4%
13.	что еще (напишите)	
14.	не знаю	
15.	затрудняюсь ответить	

14. ЧТО ДОЛЖНО, НА ВАШ ВЗГЛЯД, СДЕЛАТЬ ГОСУДАРСТВО ДЛЯ ЗАЩИТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ? *(можно выбрать не более 5 вариантов ответа)*

1.	развивать государственную политику в информационной сфере	66%
2.	обеспечивать гражданские права и свободы в цифровом пространстве	50%
3.	контролировать российский сегмент Интернета	36%
4.	разрабатывать и внедрять технические средства по противодействию информационным угрозам	54%
5.	блокировать ненадежные зарубежные социальные сети и сайты	55%

6.	установить ответственность за распространение фейков, ложной информации, утечку персональных данных	53%
7.	снижать зависимость от глобальных информационных систем, разрабатывать отечественные информационные программы и платформы	40%
8.	повышать цифровую грамотность граждан и разрабатывать образовательные программы	24%
9.	развивать и распространять моральные и этические нормы работы в Интернете	9%
10.	расширять возможности для получения электронных услуг	13%
11.	совершенствовать государственные информационные системы (Госуслуги и др.)	29%
12.	что еще (напишите)	
13.	не знаю	
14.	затрудняюсь ответить	

15. КАК ВЫ СЧИТАЕТЕ, КАКОВА СТЕПЕНЬ РИСКОВ, ВОЗНИКАЮЩИХ В ИНТЕРНЕТЕ, ДЛЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ЛИЧНОСТИ? *(ответьте, пожалуйста, по каждой строке)*

	риски, возникающие в Интернете	**высокая степень**	**средняя степень**	**низкая степень**	**не знаю**	**затрудняюсь ответить**
1.	принудительное вовлечение в цифровую среду	47%	28%	15%	2%	9%
2.	низкая ответственность за распространение фейков и ложной информации	51%	23%	15%	3%	9%
3.	возникновение интернет-зависимости	43%	26%	17%	12%	1%
4.	осуждение за убеждения или высказывания в Интернете, цифровой буллинг	46%	36%	12%	3%	4%
5.	нарушение конфиденциальности человека, потеря персональных данных	61%	23%	9%	1%	6%
6.	размытость этических норм	43%	31%	16%	1%	9%
7.	риски, связанные с искусственным интеллектом	45%	23%	21%	2%	9%
8.	отслеживание персональной геолокации граждан	48%	32%	8%	4%	8%
9.	принудительное отключение от цифровых платформ	38%	33%	13%	6%	10%
10.	возникновение цифрового неравенства	47%	27%	11%	6%	9%
11.	риски, связанные с «умными» устройствами (часы, смартфоны, гаджеты)	32%	41%	13%	5%	9%
12.	риски для здоровья	33%	27%	24%	6%	11%
13.	что еще (напишите)					
14.	затрудняюсь ответить					