

**ВСЕРОССИЙСКИЙ КОНКУРС НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ,
ПРОЕКТНЫХ И ТВОРЧЕСКИХ РАБОТ ОБУЧАЮЩИХСЯ
«ОБРЕТЁННОЕ ПОКОЛЕНИЕ»**

**Направление:
ТЕОРИЯ И ИСТОРИЯ ПРАВА И ГОСУДАРСТВА**

**Тема:
ПОКОЛЕНИЕ, ОБРЕТШЕЕ ЦИФРОВЫЕ ПРАВА И КИБЕР-
ГРАЖДАНСТВО: ЦИФРОВОЕ «ОБРЕТЁННОЕ ПОКОЛЕНИЕ» -
ФОРМИРОВАНИЕ НОВОГО КОНТУРА ПРАВ И СВОБОД В УСЛОВИЯХ
ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВА.**

**Соискатели:
Мельникова М.А.
Бочкарёва Я.С.**

**Научный руководитель:
Елесева Е.Ф.**

**Место выполнения работы:
Республика Башкортостан, г. Уфа**

Аннотация

Настоящая работа посвящена комплексному исследованию процесса стихийного формирования цифровых прав и кибер-гражданства у поколения, социализированного в условиях повсеместной диджитализации. Актуальность исследования обусловлена стремительной цифровой трансформацией государства, которая создает как новые возможности для реализации прав и свобод, так и системные вызовы традиционным правовым доктринам. В работе применяется междисциплинарный подход, сочетающий методы правового, политологического и социологического анализа. Основной целью является разработка теоретической модели нового контура прав и свобод, адекватного цифровой эпохе. В результате исследования выявлены ключевые характеристики цифрового правосознания, проанализированы конфликтные зоны между новыми практиками и старыми институтами, а также предложены пути институционализации кибер-гражданства. Работа имеет значение для теории права, законодательной практики и государственной политики в области цифровой трансформации.

Ключевые слова: цифровая трансформация государства, цифровое поколение, цифровые права, кибер-гражданство, новый контур прав и свобод, электронное правительство, цифровой суверенитет.

Annotation

This work is devoted to a comprehensive study of the process of spontaneous formation of digital rights and cyber citizenship among a generation socialized in conditions of widespread digitalization. The relevance of the research is due to the rapid digital transformation of the state, which creates both new opportunities for the realization of rights and freedoms, and systemic challenges to traditional legal doctrines. The work uses an interdisciplinary approach combining methods of legal, political science and sociological analysis. The main goal is to develop a theoretical model of a new contour of rights and freedoms adequate to the digital age. As a result of the research, the key characteristics of digital legal awareness are identified, conflict zones between new practices and old institutions are analyzed, and ways to institutionalize cyber citizenship are proposed. The work has implications for legal theory, legislative practice, and government policy in the field of digital transformation.

Keywords: digital transformation of the state, digital generation, digital rights, cyber citizenship, new contour of rights and freedoms, electronic government, digital sovereignty.

Цифровая трансформация государства порождает новый социально-политический феномен — «обретённое поколение», для которого цифровая среда стала естественным пространством реализации гражданских прав, экономической активности и социальной коммуникации. Это поколение обретает новый статус — кибер-гражданина, обладающего специфическим набором цифровых прав и обязанностей. Исследование посвящено комплексному анализу процесса формирования этого статуса в контексте глобальной конкуренции моделей цифрового суверенитета

и национальных стратегий цифровизации. реализации гражданских прав, экономической активности и социальной коммуникации. Это поколение обретает новый статус — кибер-гражданина, обладающего специфическим набором цифровых прав и обязанностей. Исследование посвящено комплексному анализу процесса формирования этого статуса в контексте глобальной конкуренции моделей цифрового суверенитета и национальных стратегий цифровизации.

Цель исследования- выявить сущность, механизмы формирования и социально-правовые последствия становления «обретённого поколения» в России, а также разработать теоретическую модель нового контура прав и свобод, способного гармонизировать его практики с процессами цифровой трансформации государства.

Задачи исследования

1. Провести критический анализ и синтез существующих теоретических подходов к понятиям «цифровое поколение», «кибер-гражданство», «цифровая трансформация государства» и обосновать введение в научный оборот концепта «обретённое поколение» как более релевантного для описания текущей ситуации.

2. Выявить и систематизировать ключевые социальные практики, ценности и правовые интуиции российского «обретённого поколения», через которые происходит стихийное формирование цифровых прав (практики приватности, самоорганизации, обхода ограничений, цифрового активизма).

3. Проанализировать стратегические документы, инициативы и правовые механизмы цифровой трансформации российского государства, оценив их влияние на пространство для реализации традиционных и формирующихся цифровых прав.

4. Сформулировать принципы и контуры нового контура прав и свобод для цифровой эпохи в России, а также предложить конкретные механизмы его легитимации

Работа исследует противоречие между необходимостью государства обеспечивать безопасность и суверенитет в цифровой сфере (например, через создание интегральных цифровых профилей, как в случае с указом о «Цифровом профиле иностранного гражданина» в России) и фундаментальной потребностью личности в защите цифровых свобод, приватности и свободы слова. На примере сравнительного анализа подходов ЕС, Китая, США и России выявляются различные балансы между контролем, безопасностью и правами личности.

Классическая концепция суверенитета: территориальная парадигма

Классическая теория государственного суверенитета, сформировавшаяся в трудах Жана Бодена (XVI век) и получившая развитие в Вестфальской системе международных отношений (1648 г.), основывалась на принципе абсолютной территориальности. Суверенитет понимался как верховная, неограниченная и неделимая власть государства в пределах четко определенных географических границ [10]. Эта модель включала несколько ключевых элементов:

Территориальная целостность - исключительный контроль над физическим пространством

Монополия на легитимное насилие - право применять силу на своей территории

Независимость во внутренних делах - принцип невмешательства других государств
равенство суверенных государств в международных отношениях. Российский правовед И.Н. Барциц отмечает, что в этой традиции суверенитет представлял собой "юридически закрепленную способность государства самостоятельно и независимо осуществлять власть в пределах своей территории". Эта модель доминировала вплоть до конца XX века, когда цифровая революция начала подрывать ее базовые предпосылки.

Первый вызов: киберпространство как "новая территория"

С появлением интернета в 1990-х годах возникло радикальное переосмысление пространства. Киберпространство было провозглашено "новой границей", свободной от традиционных форм государственного суверенитета. Наиболее ярко эту позицию выразил Джон Перри Барлоу в своей "Декларации независимости киберпространства" (1996):

"Промышленные правительства мира, вы, уставшие гиганты из плоти и стали! Я пришел из киберпространства, нового дома Сознания. От имени будущего я прошу вас, в прошлом, оставить нас в покое. Вы не властны там, где мы собрались" [11]. Эта либертарианская утопия основывалась на нескольких ключевых предположениях:

1. Трансграничная природа сети делает невозможным эффективный государственный контроль
2. Децентрализованная архитектура интернета сопротивляется централизованному управлению
3. Анонимность и самоорганизация пользователей создают новые формы социального порядка

Однако эта модель быстро столкнулась с реальностью. Государства начали применять классические инструменты суверенитета к цифровой сфере: экстратерриториальная юрисдикция (дело Microsoft в США, 2013), контроль над инфраструктурой (DNS-серверы, точки обмена трафиком), национальное законодательство о киберпреступлениях и интернет-регулировании.

Трансформация суверенитета: от территории к данным и потокам

Ответом на вызов киберпространства стало не отрицание суверенитета, а его трансформация и адаптация. Современные исследователи выделяют несколько измерений этой эволюции:

Сдвиг объекта суверенитета: от территории к данным

Если традиционный суверенитет был властью над территорией, то цифровой суверенитет все больше становится властью над данными и информационными потоками [3]. Это проявляется в:

Законах о локализации данных (требование хранить данные граждан внутри страны)

Контроле над трансграничными потоками данных (ЕС: адекватность защиты, Китай: ограничения) Национальных сегментах интернета (RuNet, китайский "Великий файрвол")

Как отмечает исследователь А.В. Шарпович, "цифровой суверенитет представляет собой способность государства самостоятельно определять и проводить политику в информационной сфере, обеспечивая безопасность, устойчивость и конкурентоспособность своего цифрового пространства" [13].

Множественность суверенитетов в сетевом пространстве

Цифровая эпоха породила конкуренцию суверенитетов:

| Тип суверенитета | Субъект | Объект контроля | Примеры |
|------------------|--------------------------------------|---|---|
| Государственный | Национальные государства | Данные, инфраструктура, контент | GDPR (ЕС), CSL (Китай), законы о суверенном интернете |
| Корпоративный | Транснациональные платформы | Пользовательские данные, правила взаимодействия | Apple App Store, Facebook Community Standards |
| Технический | Разработчики протоколов и стандартов | Архитектура сети, форматы данных | IETF, ICANN, W3C |
| Сообщественный | Онлайн-сообщества и сети | Нормы поведения, репутационные системы | Модерация в Reddit, правила Wikipedia |

Суверенитет как управление уязвимостью

Современные теории (например, М. Н. Шмидт) переосмысливают суверенитет не как абсолютный контроль, а как способность управлять взаимозависимостью и уязвимостями в

условиях глобальной цифровой экосистемы. Это включает Защиту критической информационной инфраструктуры Обеспечение технологической независимости в ключевых областях Развитие национальных цифровых экосистем Участие в международных органах интернет-управления [15].

Новые формы суверенитета в цифровую эпоху Технологический суверенитет

Этот концепт, особенно актуальный для ЕС и России, подчеркивает способность разрабатывать, производить и контролировать ключевые цифровые технологии. Он включает Суверенные облачные инфраструктуры (GAIA-X в ЕС, российские облака) Национальные операционные системы и софт Криптографическую независимость (национальные стандарты шифрования) Собственные стандарты и протоколы

Данный суверенитет

Концепция, активно развиваемая в ЕС, предполагает право граждан и организаций контролировать свои данные. Это включает:

Право на переносимость данных (GDPR) Суверенные идентификационные системы (eIDAS в ЕС) Децентрализованные модели управления данными (Self-Sovereign Identity)

Сетевой суверенитет

Этот подход, характерный для России и Китая, акцентирует способность государства контролировать информационные потоки внутри национального сегмента интернета. Ключевые элементы: Суверенный интернет (техническая возможность автономной работы) Национальные системы доменных имен Государственные точки обмена трафиком Системы фильтрации и маршрутизации трафика

Российская модель цифрового суверенитета: синтез подходов

Российская концепция цифрового суверенитета представляет собой синтез различных подходов:

Этапы формирования:

1. Ранний период (2006-2012): Принятие ФЗ-152 "О персональных данных" по европейскому образцу
2. Поворот к суверенитету (2012-2019): Законы о "блогерах", локализации данных, против "фейковых новостей"
3. Доктрина суверенного интернета (2019-н.в.): ФЗ-90, создание национальной системы доменных имен [2]

Ключевые характеристики:

- Безопасность как приоритет: данные как элемент национальной безопасности
- Технологическое импортозамещение: развитие отечественных аналогов
- Управляемая открытость: сочетание интеграции с защищенностью
- Многоуровневая модель: национальный, региональный (ЕАЭС), глобальный уровни

Будущее суверенитета: гибридные модели и новые вызовы. Эволюция суверенитета продолжается, сталкиваясь с новыми вызовами. Вызовы цифровой эпохи:

- Искусственный интеллект как новый субъект принятия решений
- Квантовые вычисления, способные взломать существующие криптосистемы
- Интернет вещей, размывающий границы между физическим и цифровым
- Метавселенные как новые пространства для социального взаимодействия

Тенденции развития:

1. Гибридизация моделей: сочетание элементов разных подходов
2. Многостороннее управление: участие государств, компаний, гражданского общества
3. Регионализация интернета: усиление региональных цифровых пространств
4. Технологическая геополитика: цифровой суверенитет как инструмент конкуренции

Заключение: Суверенитет в условиях сетевой реальности

Эволюция суверенитета от территориальной к сетевой парадигме представляет собой не отказ от этого понятия, а его глубокую трансформацию. Современный суверенитет становится:

1. Многомерным: действует в физическом, информационном, технологическом пространствах
2. Контестуемым: оспаривается различными акторами (государства, корпорации, сообщества)
3. Относительным: зависит от технологических возможностей и международной кооперации
4. Динамичным: постоянно адаптируется к новым технологическим вызовам.

Цифровая эпоха не отменила суверенитет, но сделала его более сложным, распределенным и зависимым от способности государств эффективно действовать в условиях глобальной взаимозависимости. Будущее, вероятно, будет характеризоваться сосуществованием различных моделей цифрового суверенитета, отражающих разные культурные, политические и экономические реальности.

Сравнительный анализ моделей цифрового суверенитета

Введение: Конкурирующие парадигмы в цифровую эпоху

Понятие цифрового суверенитета стало центральным элементом геополитической конкуренции XXI века. В отличие от классического территориального суверенитета, цифровой суверенитет относится к способности государства (или иного субъекта) самостоятельно определять правила функционирования и развития цифрового пространства, контролировать данные и информационные потоки, а также обеспечивать технологическую независимость. В настоящее время сформировались четыре доминирующие модели, отражающие различные философские

подходы к балансу между правами личности, государственным контролем и экономическими интересами.

1. Модель «Защиты прав» (Европейский союз / GDPR)

Философские основы и ключевые характеристики

Европейская модель, институционализируемая через Общий регламент по защите данных (GDPR) 2018 года, основана на концепции фундаментальных прав человека, унаследованной от послевоенного европейского правового порядка. GDPR рассматривает персональные данные не просто как экономический актив, но как продолжение человеческой личности, заслуживающее правовой защиты. Эта модель представляет собой попытку экспорта европейских ценностей через механизм "эффекта Брюсселя" – способность ЕС устанавливать глобальные стандарты благодаря размеру единого рынка [21].

Нормативная архитектура

Ключевые принципы GDPR включают:

- **Согласие на обработку данных:** должно быть конкретным, информированным и однозначным
- **Право на забвение:** возможность удаления персональных данных при отсутствии законных оснований для их хранения
- **Право на переносимость данных:** возможность получения и передачи данных между поставщиками услуг
- **Privacy by design и privacy by default:** интеграция защиты приватности на этапе проектирования систем
- **Значительные санкции:** штрафы до 4% глобального оборота компании

Сравнительная таблица: Ключевые характеристики моделей цифрового суверенитета

| Критерий | ЕС: "Защита прав" | Китай: "Государственный контроль" | США: "Корпоративный либерализм" | Россия: "Суверенная цифровизация" |
|--------------------|-------------------------------------|--|---|---|
| Основная цель | Защита фундаментальных прав граждан | Обеспечение государственной безопасности и социальной стабильности | Создание условий для технологического лидерства и инноваций | Обеспечение технологической независимости и информационной безопасности |
| Ключевой регулятор | Гражданин как субъект данных | Государство как верховный арбитр | Корпорация как основной актор | Государство при поддержке национальных технологических компаний |

| | | | | |
|--------------------------|---|--|---|--|
| Критерий | ЕС: "Защита прав" | Китай: "Государственный контроль" | США: "Корпоративный либерализм" | Россия: "Суверенная цифровизация" |
| Подход к данным | Персональные данные как право человека | Данные как ресурс государственного управления | Данные как экономический актив и объект собственности | Данные как элемент национальной безопасности и суверенитета |
| Правовая база | GDPR (2018) | Кибербезопасностны й закон (2017), Законы о защите данных (2021) | Фрагментированно е регулирование (СОРРА, НРРАА, ССРА) | ФЗ-152 (2006), ФЗ-90 (2019), ФЗ-187 (2023) |
| Международная стратегия | Регуляторный экспорт ("эффект Брюсселя") | Технологический экспорт через инициативу "Пояс и путь" | Технологическая гегемония через корпорации | Ограниченная интеграция, приоритет региональных союзов (ЕАЭС) |
| Технологическая политика | Регулирование существующих технологий | Государственные инвестиции в ключевые технологии (ИИ, 5G) | Рыночная конкуренция с государственным финансированием исследований | Импортозамещение , создание национальных аналогов (RuStore, ОС "Аврора") |
| Баланс прав/контроль | Максимальная защита прав при минимальном контроле | Минимальны е права при максимальном государственном контроле | Права как предмет договора между корпорацией и пользователем | Ограниченные права в обмен на безопасность и суверенитет |

Результаты и критика

GDPR значительно усилил позиции европейских граждан в отношении их данных, но подвергается критике за бюрократическую нагрузку на малый бизнес и технологический консерватизм, ограничивающий инновации в области big data и искусственного интеллекта.

2. Модель «Государственного контроля» (Китай)

Идеологические основы и правовая архитектура

Китайская модель представляет собой наиболее целостную и централизованную систему цифрового суверенитета, базирующуюся на принципе киберсуверенитета как продолжения государственного суверенитета [22]. Эта система институционализована через три ключевых закона:

1. Кибербезопасностный закон (CSL, 2017) – устанавливает базовые принципы управления интернетом
2. Закон о защите персональной информации (PIPL, 2021) – формально защищает данные граждан

3. Закон о безопасности данных (DSL, 2021) – регулирует пересечение данных через границы

Особенности реализации

- Социальный кредит: интеграция цифрового поведения в систему социального рейтинга
- Великий китайский файрвол: техническая и правовая система фильтрации контента
- Обязательная локализация данных: требование хранения данных граждан на серверах в Китае
- Технологический патриотизм: государственная поддержка национальных чемпионов (Huawei, Alibaba, Tencent)

Ирония китайской модели

При внешней ориентации на контроль, PIRL формально предоставляет гражданам права, схожие с GDPR (согласие, доступ, исправление, удаление). Однако эти права ограничиваются приоритетом национальной безопасности, что позволяет государству практически неограниченный доступ к данным. Эта модель демонстрирует инструментальный подход к правам – они существуют постольку, поскольку служат целям государственного управления и социальной стабильности.

3. Модель «Корпоративного либерализма» (США)

Рыночно-центричная парадигма

Американская модель основана на принципе минимального государственного вмешательства и саморегулирования индустрии. В отличие от ЕС и Китая, США не имеют единого всеобъемлющего закона о защите данных на федеральном уровне. Вместо этого действует лоскутное регулирование:

- COPPA (Children's Online Privacy Protection Act) – защита данных детей
- HIPAA (Health Insurance Portability and Accountability Act) – защита медицинских данных
- CCPA/CPRA (California Consumer Privacy Act/Rights Act) – региональное регулирование в Калифорнии

Корпоративный суверенитет как явление

В этой модели технологические гиганты (Big Tech) фактически становятся частными суверенами, устанавливающими правила на своих платформах. Они определяют:

- Условия обслуживания как "конституции" цифровых пространств
- Механизмы модерации контента
- Правила монетизации данных

Государство выступает преимущественно в роли арбитра в спорах (через антимонопольное регулирование) и заказчика технологий (через контракты с Министерством обороны и разведывательным сообществом) [22].

Кризис модели

События последних лет (утечки данных, вмешательство в выборы, монопольные практики) выявили системные недостатки американского подхода. Ответом стало усиление антимонопольного регулирования и дискуссии о необходимости федерального закона о приватности, что свидетельствует о кризисе чисто рыночной модели.

4. Модель «Суверенной цифровизации» (Россия)

Идеологические основы: суверенитет как безопасность

Российская модель формировалась как ответ на вызовы информационной безопасности и представляет собой синтез элементов различных подходов:

- Технический суверенитет от китайской модели (суверенный интернет, ФЗ-90)
- Формальные гарантии прав от европейской модели (ФЗ-152 о персональных данных)
- Прагматичное взаимодействие с корпорациями от американской модели

Правовая эволюция

Развитие российского регулирования прошло несколько этапов:

1. Ранний период (2006-2012): Принятие ФЗ-152 "О персональных данных" по европейскому образцу
2. Поворот к суверенитету (2012-2019): "Закон Лугового" о блогерах, закон о локализации данных
3. Доктрина суверенного интернета (2019-н.в.): ФЗ-90, создание национальной системы доменных имен

Практическая реализация

- Импортозамещение: политика замены иностранного ПО отечественными аналогами
- Техническая инфраструктура: развитие национальных облаков, ОС "Аврора"
- Регуляторное давление: законы о "праве на забвение", против "фейковых новостей"

Уникальные черты российской модели

1. Селективная изоляция: не полное отключение от глобального интернета, но создание технической возможности для этого
2. Многоуровневый суверенитет: сочетание национальных проектов ("Цифровая экономика") с евразийской интеграцией (цифровой ЕАЭС)
3. Экспорт регуляторных практик: попытки распространения своей модели на страны СНГ и ЕАЭС

Сравнительный анализ и тенденции

Оценка эффективности

Каждая модель демонстрирует различные сильные и слабые стороны:

| Модель | Сильные стороны | Слабые стороны | Адаптивность к изменениям |
|--------|--|--|---|
| ЕС | Сильная защита прав, глобальное влияние | Бюрократичность, замедление инноваций | Средняя (жесткость регулирования) |
| Китай | Целостность, технологический суверенитет | Ограничение свобод, международное недоверие | Высокая (централизованное управление) |
| США | Инновационность, гибкость | Неравенство в защите прав, рыночные сбои | Высокая (рыночная адаптация) |
| Россия | Безопасность, управляемость | Технологическое отставание, изоляционные риски | Средняя (зависимость от импортных технологий) |

Глобальные тенденции и конвергенция

Наблюдается частичная конвергенция моделей:

1. Американизация ЕС: давление в сторону большей инновационности
2. Европеизация США: движение к федеральному регулированию приватности
3. Китаизация России: усиление контроля и технологического патриотизма
4. Глобализация Китая: попытки экспорта своих стандартов

Будущее цифрового суверенитета

Ключевые направления развития:

1. Фрагментация интернета: усиление национальных сегментов при сохранении ограниченной глобальной связности
2. Конкуренция стандартов: борьба между GDPR, китайскими и американскими стандартами
3. Новые субъекты суверенитета: рост влияния корпораций и региональных объединений
4. Технологические прорывы: влияние квантовых вычислений и ИИ на баланс сил

Заключение: Многополярный цифровой мир

Анализ четырех моделей цифрового суверенитета демонстрирует отсутствие универсального оптимального подхода. Каждая модель отражает уникальное сочетание исторических, политических и экономических условий конкретного государства или союза.

Европейская модель остается эталоном защиты прав, но сталкивается с вызовами технологической зависимости. Китайская система демонстрирует эффективность централизованного управления, но ценой ограничения свобод. Американский подход обеспечивает инновационный рывок, но порождает проблемы социального неравенства и корпоративной власти. Российская модель представляет собой прагматичный компромисс между безопасностью и развитием [30].

Будущее, вероятно, будет характеризоваться сосуществованием и конкуренцией этих моделей, где цифровой суверенитет станет одним из ключевых элементов национальной идентичности и геополитического влияния в XXI веке. При этом возрастает значение гибридных моделей и международных механизмов взаимодействия между различными системами цифрового суверенитета.

Концепция кибер-гражданства: генезис, компоненты и отличие от традиционного гражданства

Генезис концепции: от электронного правительства к цифровой гражданственности

Концепция кибер-гражданства (digital citizenship) возникла на рубеже XX-XXI веков как ответ на вызовы цифровизации общества. Её теоретическое оформление прошло несколько этапов:

1. Технократический этап (1990-е годы):

Первоначально фокус был на электронном правительстве (e-government) - использовании технологий для улучшения доступа к государственным услугам. Гражданин рассматривался как пассивный получатель цифровых услуг.

2. Информационно-правовой этап (2000-е годы):

С развитием интернета возникла потребность в цифровой грамотности и информационной безопасности. Появились первые концепции цифровых прав (digital rights), наиболее известной из которых стала Билль о правах в интернете (Internet Bill of Rights).

3. Политико-участнический этап (2010-е годы):

Под влиянием социальных сетей и мобильных технологий акцент сместился на цифровое участие и сетевое гражданское общество. Ключевыми стали работы Моссбергер, Тольберт и МакНил "Digital Citizenship: The Internet, Society, and Participation" (2007) [26], где кибер-гражданство определялось как "способность участвовать в онлайн-обществе".

4. Идентификационно-экзистенциальный этап (2020-е годы):

Современный этап характеризуется осмыслением цифровой идентичности как основы гражданственности в метавселенных и гибридной реальности.

Компоненты кибер-гражданства: многоуровневая архитектура

1. Цифровые права (Digital Rights)

Современная парадигма цифровых прав включает несколько поколений:

Первое поколение (права доступа):

- Право на доступ в интернет (признано ООН как базовое право человека в 2016 году)
- Право на цифровую инфраструктуру
- Право на цифровое образование и грамотность

Второе поколение (права защиты):

- Право на цифровую приватность и защиту персональных данных
- Право на цифровую безопасность
- Право на защиту от кибербуллинга и преследований
- Право на цифровое забвение (закреплено в GDPR ЕС)

Третье поколение (права самоопределения):

- Право на цифровую идентичность и её суверенитет
- Право на алгоритмическую прозрачность и объяснимость
- Право на цифровое достоинство и репутацию
- Право на цифровое наследие

В России эволюция цифровых прав представлена в законодательстве:

| Период | Ключевые законы | Характер прав |
|-----------|--|----------------------------|
| 2006-2012 | ФЗ-152 "О персональных данных" | Защитные, реактивные |
| 2013-2019 | "Пакет Яровой", законы о блогерах | Контрольно-ограничительные |
| 2020-н.в. | ФЗ-259 "О ЦФА", стратегия цифровой трансформации | Активные, экономические |

2. Цифровые обязанности (Digital Responsibilities)

Обязанности кибер-гражданина формируют цифровую этику:

Индивидуальный уровень:

- Соблюдение цифрового этикета (нетикета)
- Защита своих учетных данных и устройств
- Критическая оценка информации (медиаграмотность)
- Ответственное создание и распространение контента

Социальный уровень:

- Уважение прав других пользователей
- Противодействие кибербуллингу и деструктивному поведению
- Соблюдение авторских прав и лицензий
- Участие в формировании позитивной цифровой среды

Государственный уровень:

- Соблюдение национального законодательства в цифровой сфере
- Уплата цифровых налогов
- Участие в цифровых переписях и опросах
- Выполнение кибергигиенических норм

3. Цифровое участие (Digital Participation)

Участие реализуется через различные формы:

Политическое участие:

- Электронное голосование (как в России на выборах разных уровней)
- Цифровые петиции и общественные инициативы
- Участие в онлайн-обсуждениях законопроектов (regulation.gov.ru)
- Цифровой активизм и флешмобы

Экономическое участие:

- Использование цифровых финансовых услуг
- Участие в краудфандинге и краудсорсинге
- Цифровое предпринимательство
- Использование блокчейн-технологий и смарт-контрактов

Культурно-социальное участие:

- Создание и потребление цифрового контента
- Участие в онлайн-сообществах по интересам
- Волонтерство через цифровые платформы
- Участие в виртуальных выставках, концертах, мероприятиях

4. Цифровая идентичность (Digital Identity)

Цифровая идентичность представляет собой многослойную конструкцию:

| Уровень идентичности | Характеристики | Примеры |
|---------------------------|---------------------------------|--|
| Государственно-правовой | Официальная, верифицированная | ЕСИА (Россия), eID (ЕС) |
| Корпоративно-сервисный | Функциональная, контекстуальная | Аккаунты в банках, соцсетях |
| Сообщественно-ролевой | Социальная, гибкая | Ники в играх, профили в профессиональных сетях |
| Персонально-экспрессивный | Творческая, множественная | Аватары в метавселенных, блоги |

Российская специфика: развивается модель государственно-центричной цифровой идентичности через ЕСИА (Единую систему идентификации и аутентификации), которая становится ключом ко всем государственным и многим коммерческим услугам.

Отличие кибер-гражданства от традиционного гражданства

Сравнительный анализ параметров

| Параметр | Традиционное гражданство | Кибер-гражданство |
|--------------|--|--|
| Основа | Территориальная принадлежность и правовая связь с государством | Цифровая активность и участие в онлайн-сообществах |
| Приобретение | По рождению, натурализации, решению государства | Самоопределение через цифровые практики, часто множественное |
| Пространство | Физическая территория государства | Сетевое пространство, часто транснациональное |
| Идентичность | Единая, государственно-санкционированная | Множественная, контекстуальная, гибридная |
| Участие | Через формальные институты (выборы, партии) | Через платформы, сети, сообщества |
| Права | Закреплены конституцией и законами | Формируются практиками, часто опережают законодательство |

| Параметр | Традиционное гражданство | Кибер-гражданство |
|---------------------|-------------------------------------|---|
| Обязанности | Четко определены законом | Часто самоустанавливаются сообществами |
| Границы | Четкие, контролируемые государством | Размытые, проницаемые, технологически опосредованные |
| Суверенитет | Государственный монополярный | Распределенный между государством, корпорациями, сообществами |
| Время существования | Постоянное (до лишения) | Ситуативное, может быть временным |

Ключевые отличительные черты

1. Добровольность и множественность Традиционное гражданство обычно едино и обязательно (за исключением случаев двойного гражданства). Кибер-гражданство добровольно и множественно - человек может одновременно быть гражданином различных онлайн-сообществ, платформ, метавселенных.

Транснациональность

Если традиционное гражданство привязано к национальному государству, то кибер-гражданство по своей природе транснационально. Сообщества в Discord, игровые гильдии, профессиональные сети LinkedIn создают гражданственность, не признающую государственных границ. Практическая, а не правовая основа Кибер-гражданство приобретает не через юридические процедуры, а через цифровые практики: создание аккаунта, соблюдение правил сообщества, активное участие, создание контента. Оно скорее де-факто, чем де-юре.

4. Динамичность и гибкость Традиционное гражданство относительно статично. Кибер-гражданство динамично - можно легко присоединиться к новому сообществу или покинуть его, изменить цифровую идентичность, мигрировать между платформами.

5. Технологическая обусловленность Кибер-гражданство полностью зависит от технологической инфраструктуры и дизайна платформ. Правила, возможности участия, сама возможность существования определяются архитекторами цифровых пространств (государствами, корпорациями).

Российский контекст: гибридная модель кибер-гражданства

В России формируется уникальная гибридная модель, сочетающая элементы:

1. Государственно-центричный цифровой профиль

ЕСИА как основа цифрового взаимодействия с государством

Постепенная интеграция всех услуг через "Госуслуги"

Цифровой профиль гражданина как централизованная база данных

2. Контролируемое цифровое участие

Законодательное регулирование онлайн-активности

Системы мониторинга и фильтрации контента

Поощрение "позитивного" цифрового участия

3. Суверенная цифровая идентичность

Развитие национальных аналогов (RuStore вместо Google Play)

Импортозамещение цифровых технологий

Цифровой паспорт как будущая интеграция идентичностей

Выводы: кибер-гражданство как новая социально-политическая реальность

Концепция кибер-гражданства представляет собой не просто дополнение к традиционному гражданству, а качественно новую форму социально-политической субъектности. Её основные характеристики:

Плюралистичность: признание множественности цифровых принадлежностей

Процессуальность: акцент на практиках, а не формальном статусе

Сетевая ориентированность: организация вокруг платформ и сообществ, а не территорий

Техноопосредованность: полная зависимость от цифровой инфраструктуры

В российских условиях кибер-гражданство развивается в постоянном напряжении между:

Транснациональной природой интернета и государственным цифровым суверенитетом

Множественностью цифровых идентичностей и унификацией через ЕСИА

Глобальными цифровыми правами и национальной спецификой регулирования

Будущее развитие кибер-гражданства будет определяться балансом между этими противоречиями, технологическими инновациями (ИИ, метавселенные) и поиском новых форм цифровой демократии и участия.

«Обретенное поколение» как субъект кибер-гражданства: социально-демографический портрет и ценностные ориентации

Введение: феномен «обретенного поколения» в цифровую эпоху

Термин «обретенное поколение» описывает когорту (поколения Z, частично миллениалов и альфа), которая не была формально наделена цифровыми правами через законодательные акты, но практически присвоила их через повседневное взаимодействие с цифровой средой. Это поколение не просто использует технологии — оно живёт в гибридной реальности, где онлайн- и офлайн-пространства взаимопроникаемы. В отличие от старших поколений, воспринимающих интернет как инструмент, «обретенные» видят в нём естественную среду обитания, что формирует уникальный тип гражданственности — стихийное кибер-гражданство.

Социально-демографический портрет

1. Хронологические рамки и численность

Поколение Z (центениалы): родившиеся примерно с 1997 по 2012 годы (возраст 12–27 лет в 2024 г.). В России — около 30 млн человек.

Поколение Альфа: родившиеся с начала 2010-х по середине 2020-х. Младшие представители (до 10–12 лет) ещё только формируют практики, но уже социализируются через детские цифровые продукты (YouTube Kids, обучающие приложения).

Старшие миллениалы (1985–1996 гг.р.) — «цифровые пионеры», чья взрослая жизнь совпала с распространением интернета. Они выступают мостом между традиционным и цифровым гражданством.

2. Ключевые демографические характеристики в российском контексте

Высокая урбанизированность: более 80% проживает в городах, что обеспечивает доступ к высокоскоростному интернету и цифровым сервисам.

Образовательный уровень: самый образованный сегмент населения — более 65% имеют высшее или среднее специальное образование (данные Росстата, 2023).

Экономическая активность:

Младшие Z (12–17 лет) — учащиеся, зависимы от родителей, но имеют карманные деньги, которые тратят на цифровые товары (до 45% подростков совершают онлайн-покупки самостоятельно).

Старшие Z (18–27 лет) — активны на рынке труда, часто в гиг-экономике (фриланс, доставка, контент-создание). Каждый пятый работает в IT-сфере или цифровом маркетинге.

Сетевая активность: 95% ежедневно выходят в интернет, проводя онлайн в среднем 6–8 часов в сутки (данные Mediascope, 2023).

Ценностные ориентации: ядро «цифрового этоса»

Ценности «обретённого поколения» формируют основу его кибер-гражданства. Они не декларируются, а практикуются в цифровой среде.

1. Ценность доступа и открытости

Информация как кислород: убеждение, что доступ к информации — базовое право. Это проявляется в использовании VPN и прокси для обхода блокировок (по данным Roskomsvoboda, 38% российской молодёжи регулярно используют обходные инструменты).

Культура ремикса и шеринга: творчество как компиляция и переработка существующего контента (мемы, видеомонтаж, фан-арт). Авторское право часто воспринимается как архаичное ограничение.

Открытый код и знания: поддержка open-source проектов, участие в вики-сообществах, вера в то, что знания должны быть бесплатными (курсы на Stepik, Хабре, в Дзене).

2. Ценность цифровой автономии и контроля над идентичностью

Множественность идентичностей: естественное существование в разных «ролях» через отдельные аккаунты (рабочий Telegram, личный Instagram, анонимный Twitter, геймерский Steam). Цифровой аватар — осознанный проект самопрезентации.

Прагматичная приватность: не тотальная скрытность, а избирательный контроль над тем, какая информация кому доступна. Например, «сторис» в Instagram для широкого круга, а Close Friends — для избранных.

Скептицизм к централизованным системам: настороженное отношение к тотальной цифровизации через Госуслуги. По опросу ВЦИОМ (2023), 52% молодых россиян опасаются, что государственные цифровые системы приведут к тотальному контролю.

3. Ценность горизонтальных связей и сетевой солидарности

Доверие к «своим»: репутация в онлайн-сообществах (игровых кланах, пабликах, чатах) ценится выше формальных статусов. Модераторы пабликов или лидеры гильдий — новая цифровая элита.

Крауд-действия: коллективное финансирование (краудфандинг на Planeta.ru), помощь (сбор средств через Добро.mail.ru), активизм (экологические инициативы, помощь животным) организуются минуя традиционные институты.

Глобальная идентичность поверх национальной: чувство принадлежности к транснациональным сообществам геймеров, фанатов аниме, разработчиков open-source. Язык общения — смесь русского и английского («изи», «краш», «чилить»).

4. Ценность результата и эффективности

Культ DIY (Do It Yourself): умение самостоятельно найти решение на YouTube, Stack Overflow, форумах. Официальные инструкции часто игнорируются.

Цифровой минимализм и кастомизация: стремление настроить интерфейсы под себя (темы, плагины, персонализация лент), отписаться от лишнего, использовать ad-blockers.

Образование как continuous process: обучение через короткие форматы (TikTok-ролики, YouTube-гайды, статьи на vc.ru), а не долгие курсы. Микроквалификации (сертификаты Coursera, навыки работы с конкретным API) ценятся выше дипломов.

Практики кибер-гражданства: как ценности воплощаются в действиях

| Ценность | Повседневные практики | Инструменты/Платформы |
|---------------|--|--|
| Доступ | Использование VPN для доступа к заблокированным ресурсам, торренты для книг/фильмов | WireGuard, Tor, RuTracker, FLibusta |
| Автономия | Настройка сложной приватности в соцсетях, использование псевдонимов, зашифрованный обмен сообщениями | Telegram (Secret Chats), Signal, настройки Instagram/Facebook |
| Солидарность | Участие в краудфандинге, помощь в фандрайзинге, организация онлайн-ивентов для сообщества | Planeta.ru , DonationAlerts, Discord-серверы, Twitch-стримы |
| Эффективность | Автоматизация рутинных задач через скрипты, использование ботов для работы, кастомизация рабочих пространств | Python-скрипты, Telegram-боты, Notion, Trello |

Российская специфика: между глобальными ценностями и национальным контекстом

«Обрётённое поколение» в России существует в условиях ценностного дуализма:

1. Адаптация под регулирование

Тактическое соблюдение законов: знание базовых норм («запрещено распространять экстремистский контент»), но креативная интерпретация границ дозволенного.

Параллельные цифровые экономики: использование криптовалют для расчётов в играх, на фриланс-биржах, хотя правовой статус неясен.

Лояльность «по умолчанию»: использование государственных цифровых сервисов (Госуслуг, электронного дневника) по необходимости, но без энтузиазма.

2. Гибридная идентичность

Патриотизм «без истерики»: гордость за российский IT-сектор (Яндекс, Касперский, VK), успехи в киберспорте, но критическое отношение к политике.

Культурный билингвизм: потребление и российского (СТС, Кинопоиск), и зарубежного контента (Netflix через VPN, Hollywood). Язык мемов — интернациональный.

3. Политическая амбивалентность

Низкий интерес к формальной политике: явка на выборы среди молодёжи традиционно ниже среднего (около 35–40%).

Активизм на микроуровне: готовность отстаивать конкретные, локальные интересы — защита парка, права арендаторов, экология города — через онлайн-петиции и соцсети.

Цифровой негативизм: протестное поведение выражается не в митингах, а в сатирических мемах, скептических комментариях, создании альтернативных новостных каналов в Telegram.

Вызовы и перспективы: «обрётённое поколение» как агент изменений

Вызовы для государства

Кризис легитимности традиционных институтов: партии, профсоюзы, СМИ теряют авторитет, уступая блогерам и лидерам мнений из TikTok/YouTube.

Неэффективность вертикальных коммуникаций: директивные обращения «сверху» игнорируются или высмеиваются. Эффективен только диалоговый, горизонтальный формат.

Правовой вакуум: законодательство отстаёт от цифровых практик. Например, регулирование киберспорта, прав на виртуальную собственность в играх, статуса NFT.

2. Перспективы трансформации общества

Новая экономика: рост гиг-экономики, цифрового предпринимательства, создание стартапов (в 2023 г. 70% новых IT-стартапов в России основаны людьми до 30 лет).

Альтернативные системы доверия: репутационные системы на фриланс-биржах ([FL.ru](https://fl.ru)), отзывы на маркетплейсах, рейтинги игроков заменяют традиционные рекомендации и дипломы.

Переопределение публичной сферы: дискуссии переносятся в Telegram-каналы, комментарии на DTF, стримы на Twitch, где формируется новая публичная этика (часто более жёсткая, но и более прямая).

Заключение: поколение, определяющее будущее цифрового гражданства

«Обрётённое поколение» — не пассивный объект цифровой трансформации, а её активный субъект. Его кибер-гражданство — это живой эксперимент по созданию новых правил сосуществования в сети. Государства, включая Россию, стоят перед выбором: либо пытаться регулировать и ограничивать эти стихийные практики, рискуя оттолкнуть наиболее технологически грамотную часть общества, либо интегрировать и институционализировать их, создавая гибкие правовые рамки для уже сложившихся норм.

Ценностный профиль этого поколения — прагматичный индивидуализм, сочетающийся с сетевой солидарностью — задаёт вектор развития не только цифровой, но и всей общественной среды. Будущее гражданственности будет определяться тем, насколько успешно традиционные институты смогут понять и адаптироваться к логике «обрётённых», признав за ними право быть не только пользователями, но и соавторами цифрового общественного договора.

Современное российское государство выступает не просто регулятором, а системным архитектором цифровой среды, формирующим её цели, инфраструктуру и правовые основания. Этот подход реализуется через трехуровневую стратегию: концептуально-стратегический, технологически-инфраструктурный и нормативно-регуляторный уровни.

Концептуально-стратегический уровень задаётся пакетом документов, ключевым из которых является национальная программа «Цифровая экономика Российской Федерации». Она определяет цифровизацию как основу национального развития и суверенитета, ставя цели по созданию сквозных цифровых платформ, обеспечению информационной безопасности и подготовке кадров

[4]. Эта программа, наряду со «Стратегией развития информационного общества», формирует идеологическую рамку, где технологический прогресс неразрывно связывается с задачами государственной безопасности и управляемости. Цифровая трансформация понимается как процесс, управляемый «сверху», с чётким подчинением технологических изменений государственным приоритетам [8].

Технологически-инфраструктурный уровень представляет собой создание государством «цифровых артерий», обеспечивающих его присутствие и контроль в новой среде. Ключевым элементом является Единая система идентификации и аутентификации (ЕСИА). Изначально инструмент для доступа к порталу госуслуг, ЕСИА эволюционировала в фундаментальную инфраструктуру цифрового гражданства, становясь универсальным ключом для доступа не только к государственным, но и ко многим коммерческим сервисам [9]. Параллельно создаются государственные информационные системы (ГИС) — централизованные платформы для управления отраслевыми данными (ГИС ЖКХ, ГИС «Контингент» обучающихся и др.). Эти системы концентрируют массивы информации, минимизируя необходимость межведомственного согласования и создавая основу для проактивного государственного управления на основе данных (data-driven governance) [14].

Нормативно-регуляторный уровень (регуляторика) обеспечивает легитимность архитектурных решений и определяет правила поведения в цифровой среде. Законодательство в этой сфере характеризуется дуализмом: с одной стороны, оно создаёт правовые основы для цифровых инноваций (законы об электронной подписи, о дистанционной торговле), а с другой — формирует механизмы контроля. «Пакет законов Яровой», законодательство о «суверенном Рунете» (ФЗ-90) и о «фейковых новостях» демонстрируют вектор на обеспечение информационной безопасности и цифрового суверенитета, что на практике часто означает усиление контроля над информационными потоками и инфраструктурой [2]. Таким образом, государство как архитектор формирует не нейтральную «площадку», а управляемую экосистему, где технологические решения изначально содержат в себе определённые политические и регуляторные предпочтения.

«Цифровой профиль» как ядро административного взаимодействия: вектор на тотальный учёт.

Указ Президента РФ от 10 мая 2024 г. № 342 «О цифровом профиле иностранного гражданина» является логическим и знаковым этапом в развитии государственной стратегии цифровизации, чётко демонстрирующим вектор на тотальный учёт и цифровое управление населением.

Цели и сущность. Формально Указ направлен на повышение качества услуг для иностранных граждан и упрощение административных процедур [7]. Однако его системное значение гораздо глубже. «Цифровой профиль» (ЦП) представляет собой не просто электронную папку, а целостную

цифровую модель субъекта, агрегирующую данные из всех его взаимодействий с государственными органами. Для иностранных граждан он становится обязательным ядром административных отношений, централизующим информацию от момента пересечения границы до трудоустройства и повседневного взаимодействия с сервисами.

Объём данных и механизм. ЦП предполагает включение исчерпывающего набора сведений: биометрические данные (отпечатки пальцев, изображение лица), миграционная история (въезды, регистрации, разрешительные документы), данные о трудовой деятельности и налогах, сведения об административных и уголовных правонарушениях, а также история обращений за госуслугами [7]. Интеграция данных происходит через межведомственное информационное взаимодействие, минуя самого субъекта данных, что создаёт систему тотальной прозрачности индивида для государства. По сути, происходит создание комплексного цифрового досье, доступного для алгоритмического анализа и оценки «благонадёжности».

Правовые последствия и вектор развития. Внедрение ЦП несёт ряд глубоких правовых последствий:

1. Смещение баланса прав. Возникает ситуация крайней информационной асимметрии: государство аккумулирует о субъекте полный массив данных, в то время как сам субъект лишён эффективного контроля над их использованием, корректировкой или удалением [8].

2. Риск алгоритмической дискриминации. Интеграция данных о правонарушениях, трудовой деятельности и поведении создаёт основу для профилирования и автоматического принятия решений (например, об отказе в услуге), что ставит под угрозу принцип презумпции невиновности и права на индивидуальное рассмотрение случая.

3. Функциональное «расползание» (function creep). Данные, собранные для целей миграционного учёта, с высокой вероятностью могут быть использованы для иных целей — социального контроля, прогнозной аналитики, что не оговорено в Указе явно.

4. Экстраполяция модели. Создание ЦП для иностранцев логически предвещает дальнейшее развитие и ужесточение аналогичной системы «цифрового профиля гражданина РФ», закрепляя модель, где человек рассматривается прежде всего, как объект управленческого учёта.

Таким образом, Указ № 342 подтверждает стратегический курс на построение государственно-центричной экосистемы данных, где «цифровой профиль» становится ключевым инструментом перехода от реагирующего управления к предиктивному и проактивному контролю над социальными процессами и поведением индивидов[6].

Дискурс о цифровых правах: между свободой и контролем

В российском публичном пространстве дискурс о цифровых правах носит маргинальный и политизированный характер, что наглядно иллюстрирует анализ инициативы КПРФ о моратории на блокировки и реакция на неё.

Позиция КПРФ как политический сигнал. В 2021 году фракция КПРФ внесла в Госдуму законопроект об установлении моратория на внесудебные блокировки интернет-ресурсов, а также предлагала закрепить понятия «цифровые права» и гарантии неприкосновенности частной цифровой жизни [6]. Несмотря на отсутствие шансов на принятие, эта инициатива имеет символическое значение. Она маркирует запрос на цифровые свободы со стороны части общества и политического спектра, противопоставляя его доминирующему нарративу о «цифровом суверенитете» и «информационной безопасности». Критика КПРФ была направлена на непропорциональность блокировок, их негативное влияние на бизнес и свободу распространения информации, что указывало на попытку сформировать альтернативную повестку, сочетающую левую экономическую программу с либеральными элементами в цифровой сфере.

Проблема цензуры и свободы информации. Дискуссия о блокировках высвечивает ключевую проблему: размытость правовых оснований для ограничений. Законодательство (например, ФЗ-149 «Об информации» в редакции, ФЗ-114 «О противодействии экстремистской деятельности») содержит широкие и нечёткие формулировки («нежелательный контент», «фейковые новости»), что позволяет на практике применять блокировки к самому широкому спектру ресурсов — от оппозиционных СМИ и страниц активистов до целых платформ (как в случае с LinkedIn) [2]. Это создаёт режим превентивной цензуры, где административные органы и провайдеры, стремясь избежать санкций, начинают избыточно фильтровать контент, что ведёт к сужению публичной сферы и миграции дискуссии в менее контролируемые, но и более маргинальные сегменты интернета (мессенджеры, закрытые чаты).

Проблема приватности в условиях цифрового государства. Дискурс о приватности в России крайне слаб и подавляется доминирующим нарративом безопасности. Общественная дискуссия о масштабном сборе персональных данных через ЕСИА, биометрические системы, ГИС и «цифровые профили» практически отсутствует. Принятие PIPL-подобного всеобъемлющего закона о защите данных, ставящего во главу угла права субъекта данных (по аналогии с GDPR ЕС), не является политическим приоритетом [5]. Вместо этого приватность остается фрагментированной между узкими законами (например, ФЗ-152 «О персональных данных»), действие которых нейтрализуется более поздними нормами в интересах безопасности (как в «пакете Яровой»). Таким образом, право на приватность де-факто подчинено интересам государственного контроля и управления, а публичная дискуссия об этом подменяется техническими вопросами «защиты данных» от внешних угроз, но не от внутреннего произвола.

Итогом является формирование асимметричного цифрового порядка: государство последовательно наращивает свой потенциал наблюдения и контроля, в то время как пространство для защиты цифровых прав граждан (свободы информации, приватности, анонимности) не имеет

сильных институциональных защит и остаётся полем для точечных, часто политически мотивированных дискуссий.

Литература

1. Федеральный закон №152-ФЗ «О персональных данных». 2006.
2. Федеральный закон №90-ФЗ «О внесении изменений в отдельные законодательные акты РФ по вопросам устойчивого функционирования российского сегмента сети «Интернет». 2019.
3. Федеральный закон №187-ФЗ "О безопасности критической информационной инфраструктуры РФ" (2023).
4. Национальная программа «Цифровая экономика Российской Федерации» (утверждена протоколом заседания президиума Правительственной комиссии по цифровому развитию от 28.05.2021 № 16). Правительство РФ.
5. Рекомендации Совета при Президенте РФ по развитию гражданского общества и правам человека «О защите персональных данных в условиях цифровой трансформации» (2023).
6. Законопроект № 1256485-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (о моратории на блокировки), внесённый депутатами ГД от фракции КПРФ (2021).
7. Концепция развития цифровой идентификации в Российской Федерации (утверждена распоряжением Правительства РФ от 12.11.2021 № 3223-р).
8. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».
9. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации».
10. Боден Ж. Шесть книг о государстве. 1576.
11. Барлоу Дж. П. Декларация независимости киберпространства. 1996.
12. Барциц И.Н. Цифровой суверенитет: конституционно-правовые аспекты // Государство и право. 2021. № 8.
13. Шарпович А.В. Концепция цифрового суверенитета в системе национальной безопасности Российской Федерации // Вестник МГИМО-Университета. 2022. Т. 15, № 1.
14. Шарпович А. В. Цифровой суверенитет и эволюция государственного управления: от электронного правительства к data-центричному государству // Вестник МГИМО-Университета. 2023. Т. 16, № 3. С. 89-115.
15. Schmidt, M. N. Cyberspace and Sovereignty: The Internet as a Challenge to Westphalian Order. University of Copenhagen, 2020.
16. Regulation (EU) 2016/679 (General Data Protection Regulation). 2016.

17. Cybersecurity Law of the People's Republic of China. 2017.
18. DeNardis, L. The Global War for Internet Governance. Yale University Press, 2014.
19. Мусихин А.А. Цифровой суверенитет России в условиях технологических вызовов // Вестник РГГУ. Серия "Политология. История. Международные отношения". 2023. № 1.
20. Krasna, F. Sovereignty in Cyberspace: Balkanization versus Globalization. Journal of Cyber Policy, Vol. 5, Issue 2, 2020.
21. Европейская модель: Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, 2016.
22. Bradford, A. The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020. Kuner, C. et al. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020. Китайская модель: Cybersecurity Law of the People's Republic of China (2017).
23. Сравнительные исследования: Polatin-Reuben, D., Wright, J. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. 4th USENIX Workshop on Free and Open Communications on the Internet, 2014.
24. Aaronson, S., Leblond, P. Another Digital Divide: The Rise of Data Realms and Its for the WTO. Journal of International Economic Law, Vol. 21, 2018.
25. Pohle, J., Thiel, T. Digital Sovereignty. Internet Policy Review, Vol. 9, Issue 4, 2020. Caverty, M., Egloff, F. The Politics of Cybersecurity: Balancing Different Roles of the State. St. Antony's International Review, Vol. 15, No. 1, 2019.
26. Mossberger, K., Tolbert, C.J., McNeal, R.S. Digital Citizenship: The Internet, Society, and Participation. MIT Press, 2007.
27. Isin, E., Ruppert, E. Being Digital Citizens. Rowman & Littlefield, 2015.
28. Гражданство в цифровую эпоху: коллективная монография / Под ред. А.Ю. Сунгоркиной. М.: Проспект, 2022.
29. "Об утверждении Концепции развития цифровой идентификации в Российской Федерации": Распоряжение Правительства РФ от 12.11.2021 №3223-р.
30. "Цифровые права и свободы: международные стандарты и российская практика": аналитический доклад Института права и развития ВШЭ-Сколково, 2022.
31. Choi, M. Digital Citizenship Scale: Development and Validation. Computers in Human Behavior, Vol. 117, 2021.
32. Головань, Л.А. Цифровая идентичность гражданина: правовые аспекты формирования в России // Вестник Пермского университета. Юридические науки. 2023. № 1.
33. "Развитие цифровой демократии в России: возможности и риски": отчет ЦИПКР, 2023.

34. Права человека в цифровую эпоху: сборник документов Совета Европы / Сост. Д.В. Хапов. М.: Статут, 2022.