УДК 334.02

Е. В. Стовба ORCID ID 0000-0002-9041-6194
Бирский филиал ФГБОУ ВО «Уфимский университет науки и технологий», Бирск, Россия, e-mail: stovba2005@rambler.ru

Е. И. Шевалдина ORCID ID 0000-0002-3979-3744
ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Уфа, Россия

А. В. Стовба
Бирский филиал ФГБОУ ВО «Уфимский университет науки и технологий», Бирск, Россия

К. С. Шевалдина ORCID ID 0009-0003-1060-2830
ФГАОУ ВО «Казанский (Приволжский) федеральный университет», Казань, Россия

ЦИФРОВОЙ ДЕТОКС И ДЕЦИФРОВИЗАЦИЯ КАК ИНСТРУМЕНТ ЗАЩИТЫ ПРАВ ГРАЖДАН В ЭКОНОМИЧЕСКОМ И ОБЩЕСТВЕННОМ ПРОСТРАНСТВЕ

Ключевые слова: децифровизация, цифровой детокс, экономическое пространство, цифровые права, цифровые технологии, цифровое принуждение, цифровая зависимость, банковская сфера.

В статье актуализируется проблематика защиты прав граждан в современных условиях тотальной цифровизации экономического и общественного пространства. Авторами рассмотрены теоретические основания и предпосылки, практические проявления ограничений цифрового воздействия на экономику и общественную жизнедеятельность. Исследуются феномены децифровизации и цифрового детокса, используемые в качестве защитных механизмов негативных последствий чрезмерной цифровизации, финансового мошенничества в экономическом и общественном пространстве. Представлена авторская оценка процессов государственного регулирования цифровизации на национальном и международном уровне. Приведены примеры частных инициатив граждан по цифровому дауншифтингу и защите от принудительной цифровизации. Особое внимание в статье уделяется российской проблематике цифрового принуждения и отсутствия гарантий аналоговых альтернатив. Резюмируется, что переход от модели тотальной цифровизации к селективному цифровому развитию позволит обеспечить экономический баланс между технологическим развитием и защитой конституционных прав граждан в цифровой среде.

E. V. Stovba ORCID ID 0000-0002-9041-6194
Birsk Branch of Ufa University of Science and Technology, Birsk, Russia, e-mail: stovba2005@rambler.ru

E. I. Shevaldina ORCID ID 0000-0002-3979-3744
Ufa State Petroleum Technical University, Ufa, Russia

A. V. Stovba
Birsk Branch of Ufa University of Science and Technology, Birsk, Russia

K. S. Shevaldina ORCID ID 0009-0003-1060-2830
Kazan (Volga Region) Federal University, Kazan, Russia

DIGITAL DETOX AND DEDIGITIZATION AS A TOOL FOR PROTECTING THE RIGHTS OF CITIZENS IN THE ECONOMIC AND SOCIAL SPACE

Keywords: dedigitization, digital detox, economic space, digital rights, digital technologies, digital coercion, digital dependence, banking sector.

This article addresses the issue of protecting citizens' rights in the current context of the total digitalization of the economic and social space. The authors examine the theoretical foundations and prerequisites, as well as the practical manifestations of limitations in the digital impact on the economy and social life. They explore the phenomena of dedigitization and digital detox, used as protective mechanisms against the negative consequences of excessive digitalization and financial fraud in the economic and social space. The

author presents an assessment of state regulation of digitalization at the national and international levels. Examples of private citizen initiatives for digital downshifting and protection from forced digitalization are provided. The article pays particular attention to the Russian problem of digital coercion and the lack of guarantees for analog alternatives. It is concluded that the transition from a model of total digitalization to selective digital development will ensure an economic balance between technological development and the protection of citizens' constitutional rights in the digital environment.

Введение

Современная эпоха характеризуется беспрецедентным и активным внедрением цифровых технологий во все сферы экономики и общества, от отдельных аспектов личной коммуникации до критически важных систем государственного управления и жизнеобеспечения [1]. В то же время следует подчеркнуть, что чем более интегрированными становятся цифровые системы в экономическое пространство и повседневную жизнь людей, тем более уязвимым становятся само общество и отдельные отрасли к цифровым сбоям, манипуляциям и злоупотреблениям. В отличие от локальных технических и компьютерных проблем, наблюдаемых в прошлые десятилетия, современные цифровые риски отражают системный характер и они способны охватить целые области общественной жизни и экономической деятельности одновременно.

В данном контексте на внедрение цифровых технологий формируется двойственная реакция экономики и общества. Так, с одной стороны, продолжается широкомасштабная цифровизация с учетом определенных экономических и политических интересов, с другой стороны появляются и формируются движения за децифровизацию, цифровой детокс и защиту прав граждан от принудительного цифрового воздействия. В то же время активное внедрение цифровых технологий во многих секторах реальной экономики способствует повышению уровня производительности, эффективности и работоспособности сотрудников компаний и организаций [2].

Современная цифровая среда характеризуется экспоненциальным ростом применяемых устройств Интернета вещей, которые регулярно собирают персональные данные пользователей. В свою очередь, видеокамеры с технологией распознавания лиц, носимые устройства, собирающие данные о медицинских состояниях и физической активности в реальном времени, создают беспрецедентно детальную картину частной жизни граждан.

Необходимо отметить, что особую озабоченность вызывает способность современных цифровых систем к созданию комплексной персональной картины на основе агрегации данных и алгоритмическое профилирование, которое способно раскрывать персональные и интимные атрибуты личности без сознательного предоставления данной информации пользователем. Также облачные сервисы, ставшие базисом современной цифровой инфраструктуры, формируют новые векторы атак на персональную информацию. При этом удаленная обработка цифровых данных создает объективные угрозы безопасности информационных и экономических систем, особенно в переходные моменты времени «миграции» внутренних приложений и массивов данных в облако. Данный процесс определяет риски раскрытия информации третьим сторонам, которые могут воспользоваться личными персонализированными данными потребителей.

В экономическом аспекте применение алгоритмов искусственного интеллекта создает риски алгоритмического смещения, при которых из-за системных ошибок машинного обучения формируются некорректные результаты, что, в свою очередь, предоставляет преимущества определенным группам людей и влияет на их доступность к кредитным финансовым средствам, образовательным услугам, государственным ресурсам, медицинским услугам и к инвестициям.

Материалы и методы исследования

Дизайн настоящего исследования отражает достижение цели, направленной на проведение контент-анализа определения роли феноменов цифрового детокса и децифровизации, рассматриваемых как инструменты защиты прав граждан в экономическом и общественном пространстве. Проведение экономического и контент-анализа базировалось на основных положениях теории технологического детерминизма и концепции цифрового гуманизма, утвержденных нормах и международных стандартов защиты цифровых прав граждан.

Корпус материалов включает отечественные нормативно-правовые акты (Доктрину информационной безопасности

(утв. Указом Президента РФ от 05.12.2016 № 646) [6]; Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [7]; Концепцию государственной системы противодействия противоправным деяниям с использованием ИКТ (расп. Правительства РФ от 30.12.2024 № 4154-р) [5]; документацию, массивы статистических и аналитических данных; научные публикации и материалы открытых источников.

Критерии отбора для материалов составили: для нормативных актов – действующая редакция законодательных документов на временной период проведения контент-анализа (февраль 2026 г.); для научных статей – релевантные проблематике исследования материалы и рецензируемые публикации, изданные не ранее 2020 г. Период анализа основного массива источников охватывал временной период доступных наблюдений с 2020 по 2026 гг. При осуществлении исследования использовался тематический анализ с индуктивным кодированием при выделении следующих категорий, а именно: «государственное регулирование», «международный опыт», «цифровой детекос», «децифровизация», «цифровое принуждение», «инструменты защиты», «цифровые риски». Проверяемость основывалась на двойном кодировании отдельных текстовых фрагментов исследователями (соавторами настоящей статьи) и дальнейшем согласовании авторских позиций и формулировке итоговых суждений, выводов.

Результаты исследования и их обсуждение

Безусловно, наблюдаемая цифровизация банковских услуг создала новый ландшафт финансовых угроз, и многие клиенты банков в настоящее время предпочитают управлять своими банковскими счетами с помощью мобильных приложений, компьютеров, что, в свою очередь, радикально изменило характер наблюдаемых финансовых рисков. Сегодня фишинговые атаки составляют существенную часть мошеннических операций в цифровом банкинге, что непосредственно отражает повышенную сложность и эффективность использования социальной инженерии в цифровой среде.

Выделим еще одно негативное последствие цифровизации в банковской сфере, а именно дропперство, использование банковских карт и счетов граждан для приема, обналичивания и перевода денег, полученных с помощью мошенничества. Данное явление наиболее активно распространяется среди подростков, студентов, пенсионеров, безработных и других наиболее уязвимых социальных групп населения [3]. Основные схемы вовлечения в данную схему включают предложения «легкого заработка» с минимумом усилий, маскировку под официальные банковские программы, а также использование сетевого маркетинга и имитацию возможного трудоустройства [11].

Исследования отечественных ученых показывают необходимость перехода от тотальной цифровизации к селективному подходу [4; 10]. На современном этапе тотальная цифровизация привела к тому, что активное применение передовых цифровых технологий создало принципиально новые возможности для привлечения граждан в террористическую и криминальную деятельность. Так, например, анонимность цифрового пространства, доступность социальных сетей и развитие технологий психологического воздействия определили отрицательные возможности использования интернета для эффективный радикализации и криминального рекрутинга.

Следует отметить, что вербовщики используют различные профессиональные психологические методики, включающие поэтапное воздействие на личность человека. Первоначально они изолируют человека от близкого окружения и социума в целом, заменяя наиболее близких людей на «духовных сестер и братьев». При работе с верующими молодыми людьми вербовщики эффективно применяют свои знания в теологической сфере и сознательно искажают сущность религиозных понятий.

В экономическом аспекте применение алгоритмов искусственного интеллекта создает риски алгоритмического смещения, при которых из-за системных ошибок машинного обучения формируются некорректные результаты, что, в свою очередь, предоставляет преимущества определенным группам людей и влияет на их доступность к кредитным финансовым средствам, образовательным услугам, государственным ресурсам, медицинским услугам и к инвестициям.

Цифровизация должна применяться только там, где она демонстрируемо улучшает человеческое благосостояние и экономическое благополучие без создания неприемлемых рисков [12]. Ключевые принципы селективной цифровизации включают принципы цифрового минимализма, безопасности и этики,

сотрудничества, общественного блага, глобальной ответственности и обратимости. Право на цифровое самоопределение должно определять права на отказ от использования цифровых технологий без ущерба для доступа к основным услугам, аналоговые альтернативы для всех критически важных сервисов, объяснение алгоритмических решений, влияющих на жизнь граждан, цифровое «забвение» и полное удаление персональных данных, защиту от алгоритмической дискриминации, цифровую реабилитацию для зависимых от технологий.

Фундаментальные исследования демонстрируют, что использование социальных сетей активирует те же самые нейронные сети, что и наркотические вещества, и этот процесс можно назвать «цифроманией» [8]. При взаимодействии с социальными медиа происходит высвобождение дофамина в специфические «ядра-мишени», что мотивирует к продолжительному использованию. Пользователи оказываются в замкнутом «дофаминовом цикле», создаваемом бесконечными лентами социальных сетей. Цифровые платформы создают устойчивые паттерны внимания, от которых пользователям становится сложно освободиться.

Следует выделить такое явление, распространяемое в последние годы как цифровой дауншифтинг, который представляет собой сознательное снижение интенсивности использования цифровых технологий в пользу более простого и осмысленного образа жизни. Данный феномен является частью более широкого движения добровольной простоты, а именно образа жизни, отвергающего потребительский стиль жизни.

Российская специфика цифровизации может быть обозначена так – цифровой суверенитет без защиты граждан. Конституционной основой защиты граждан в цифровой среде является конституционное право граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом. Государственная политика исходит из принципа правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса.

Федеральный закон «О персональных данных» от 27 июля 2006 г. является основным законом о персональных данных в РФ [7]. При этом в новой редакции ФЗ от 24.06.2025 г. отмечено: «Согласие на обработку персональных данных должно быть оформлено отдельно от иных информации и (или) документов, которые подтверждает и (или) подписывает субъект персональных данных». Закон о «суверенном интернете», вступивший в действие 1 ноября 2019 года, представляет независимую инфраструктуру для бесперебойного функционирования интернета в России [9]. Официальная позиция властей заключается в защите российского сегмента Сети от внешних угроз и кибератак, включая отключение от Всемирной паутины. Закон требует от операторов связи установки технических средств противодействия угрозам на свои сети.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является ключевым государственным органом, ответственным за регулирование и контроль в сфере информационных технологий. Основные функции Роскомнадзора в сфере защиты граждан включают контроль за соблюдением законодательства о персональных данных, блокировку запрещенных сайтов и ресурсов, противодействие киберпреступности, повышение цифровой грамотности населения.

Цифровое принуждение в российском контексте представляет собой отсутствие экономических и правовых гарантий сохранения аналоговых альтернатив для получения критически важных услуг и реализации основных прав граждан. Сущность проблемы заключается в том, что в российском законодательстве отсутствуют нормы, которые гарантируют добровольность использования цифровых технологий.

Основным инструментом цифрового принуждения стало принудительное вовлечение граждан в Единую систему идентификации и аутентификации, которая функционирует через портал «Госуслуги». При этом система не только требует обязательной регистрации, но и осуществляет «отслеживание событий частной жизни граждан» и «государственное управление данными граждан». С 1 апреля 2025 года вступили в силу требования, согласно которым банки обязаны использовать Единую биометрическую систему для идентификации клиентов. Критически важно, что банк не вправе требовать от клиентов представления иных сведений и документов для идентификации при использовании ЕБС. Это означает, что традиционные способы идентификации фактически отменяются в пользу принудительной биометрии.

Авторская оценка моделей цифровизации в экономическом пространстве
Источник: составлен авторами по результатам собственных исследований

В образовательной сфере реализуется федеральный проект «Цифровая образовательная среда», который предполагает обязательное использование государственных информационных систем: ГИС «Моя школа», цифрового сервиса «Мой колледж», платформы «Сферум», электронных дневников и журналов. Внедрение автоматизированных технологий по обработке и передаче персональных данных увеличивает риск уязвимости частной жизни ребенка и создает угрозы незаконного оборота персональных данных несовершеннолетних.

Показательным примером цифрового принуждения стал переход с аналогового на цифровое телевидение, и этот процесс затронул миллионы россиян в отдаленных и малообеспеченных регионах. При этом реальные причины неготовности цифрового перехода заключались в том, что люди просто не знали и не понимали, что им нужно делать, или они были бедны. Переход требовал значительных расходов на современные телевизоры, приставки, спутниковые тарелки. Для малообеспеченных семей, особенно в «медвежьих уголках» страны, это создало непреодолимый барьер для доступа к необходимой информации.

В отличие от стран Азии и Запада, российское государство не разработало специальных программ поддержки цифрового шаббата или цифрового детокса. Напротив, государственная политика сосредоточена на продвижении цифрового правительства с акцентом на внедрение технологий безбумажного документооборота, информатизацию процессов управления. Это создает парадоксальную ситуацию, где государство активно продвигает цифровизацию всех сфер экономики и жизнеобеспечения, но не предусматривает механизмы защиты граждан от негативных последствий чрезмерного внедрения цифровых технологий.

Необходимо констатировать, что в российском дискурсе утвердился термин «цифровой детокс» как «временный сознательный отказ от использования смартфонов, компьютеров, планшетов и других устройств с целью снятия стресса, погружения в реальное общение, творчество, сон или работу». С концепцией цифрового детокса тесно связано понятие «медиаскетика», которое включает сформировавшийся образ жизни, характеризующийся пониманием новейших средств коммуникации и разумным использованием их для человеческой жизни.

На основе обобщения результатов контент-анализа по таким критериям, как целевые ориентиры и последствия, а также ключевые риски нами сопоставлены модели селективной и тотальной цифровизации. Авторская оценка моделей цифровизации в экономическом пространстве представлена на рисунке.

Для решения проблемы перегибов тотальной цифровизации в экономическом и общественном пространстве можно предложить комплекс мер краткосрочной, среднесрочной и долгосрочной перспективы. Краткосрочные меры защиты цифровых прав включают создание межведомственной координационной структуры по кибербезопасности и защите цифровых прав, учреждение института уполномоченного по цифровым правам, внедрение механизмов общественного контроля, законодательное закрепление права на цифровую паузу в трудовых отношениях, принятие поправок к Конституции РФ о цифровых правах, разработку национальной программы цифровой грамотности с широким охватом населения и создание сети центров цифрового детокса.

Среднесрочные стратегические инициативы определяют принятие специального федерального закона «О защите граждан от алгоритмической дискриминации», законодательное закрепление права на аналоговые альтернативы цифровым услугам, создание национальной системы мониторинга цифрового неравенства, развитие инфраструктуры цифровой реабилитации и поддержку разработки «этичных технологий».

Долгосрочные институциональные реформы должны включать разработку комплексной доктрины цифровых прав человека, интеграцию принципов цифровой безопасности в образовательные стандарты всех уровней, формирование международных соглашений о защите цифровых прав человека, создание технологически свободных зон по португальской модели, развитие альтернативной аналоговой инфраструктуры и создание системы социальной поддержки «цифроисключенных» граждан.

Выводы

Таким образом, проведенное исследование позволяет сделать ряд принципиальных выводов о роли децифровизации и цифрового детокса как средств защиты прав граждан в экономическом и общественном пространстве. Во-первых, осуществленный контент-анализ показал, что движения за децифровизацию и цифровой детокс не являются иррациональной технофобией или попыткой остановить технический прогресс в отдельных секторах экономики. Напротив, они представляют собой рациональный ответ на объективно существующие системные риски чрезмерной цифровизации, включающие угрозы приватности, финансовой безопасности, демократическим процессам, психическому здоровью и социальной стабильности.

Во-вторых, исследование выявило научную обоснованность практик цифрового воздержания. Нейробиологические, психологические и социологические исследования убедительно демонстрируют негативное воздействие чрезмерного использования цифровых технологий на когнитивные способности, социальные навыки и общее экономическое благосостояние и благополучие человека.

В-третьих, сравнительный анализ международного опыта показывает конвергенцию различных национальных подходов к проблеме защиты граждан от негативных последствий цифровизации. Несмотря на различия в методах, от активной государственной поддержки программ цифрового детокса в Южной Корее до правовых гарантий аналоговых альтернатив в Германии, наблюдается общее признание необходимости защитных мер против чрезмерной цифровизации в экономическом и общественном пространстве.

В-четвертых, анализ российской ситуации выявляет существенные пробелы в защите граждан от цифрового принуждения. Парадоксальность российской модели заключается в сочетании развитой технической инфраструктуры кибербезопасности с систематическим принуждением граждан к участию в цифровых системах без предоставления аналоговых альтернатив. Это соз-

дает особые риски для наиболее уязвимых групп населения – пожилых граждан, людей с ограниченными возможностями, малообеспеченных слоев.

Исследование показало необходимость парадигмального сдвига в понимании роли «цифры» в экономике и обществе. Вместо модели тотальной цифровизации, основанной на императиве технологического детерминизма, объективно важным является переход к экономической модели селективной цифровизации, основанной на принципах цифрового гуманизма. Главный вызов современности заключается в необходимости найти оптимальный экономический баланс между использованием возможностей цифровых технологий и сохранением человеческой автономии.

Библиографический список

1. Будович Ю. И. Разочарование в цифровизации и децифровизация? // Теоретическая экономика. 2019. № 8 (56). С. 54-58. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_42896849_46104867.pdf (дата обращения: 12.01.2026).

2. Ганичев Н. А., Кошовец О. Б. «Новый цифровой разворот» – от дискурса экономического роста к технологическому расколу мира и принудительной рационализации // Вопросы теоретической экономики. 2022. № 4 (17). С. 7-24. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_49810846_36403939.pdf. (дата обращения: 12.01.2026). DOI: 10.52342/2587-7666VTE_2022_4_7_24.

3. Дропперство: что это и чем опасно // Газпромбанк. 2024. 6 ноября. [Электронный ресурс]. URL: https://www.gazprombank.ru/pro-finance/safety/kak-ne-stat-dropperom (дата обращения: 12.01.2026).

4. Низамов С. С., Макарова О. Б. Общество, экономика и право: проблемы взаимодействия в современных условиях // Общество, право, государственность: ретроспектива и перспектива. 2023. № 2 (14). С. 71-74. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_54109717_38989846.pdf (дата обращения: 12.01.2026).

5. Распоряжение Правительства РФ от 30 декабря 2024 г. № 4154-р «Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий». [Электронный ресурс]. URL: http://government.ru/docs/53922 (дата обращения: 12.01.2026).

6. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 12.01.2026).

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». [Электронный ресурс]. URL: https://base.garant.ru/12148567/?ysclid=mlju7mkilc77673888 (дата обращения: 12.01.2026).

8. Черданцев В. П., Подгородецких А. Р., Дейнеко С. И. Внедрение информационных технологий в управление человеческим капиталом: предпринимательский и государственный аспекты // Электронное сетевое издание «Международный правовой курьер». 2025. № 2. С. 124-127. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_82024144_98446481.pdf (дата обращения: 12.01.2026).

9. Чернышова Е. Суверенный интернет в России: суть закона и последствия // РБК Тренды. 2022. 28 февраля. [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/609a52329a79471fba0f0837 (дата обращения: 12.01.2026).

10. Шарапова Н. В., Зова В. А. Организационно-методические особенности экономического анализа в условиях информационных запросов цифровой экономики // Вестник Алтайской академии экономики и права. 2023. № 6-1. С. 122-130. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_54044740_37078225.pdf (дата обращения: 12.01.2026). DOI: 10.17513/vaael.2868.

11. Banerji A. How Gen Z toppled Nepal's government // Context. 2025. 14 September. [Электронный ресурс]. URL: https://www.context.news/digital-divides/why-are-nepals-gen-z-protesting-a-social-media-ban (дата обращения: 12.01.2026).

12. Zeynalova A. Digital detox and philosophy: a comparative analysis in the age of artificial intelligence // Universum: общественные науки. 2025. № 10-2 (125). С. 11-13. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_83112182_ 56522653.pdf (дата обращения: 12.01.2026). DOI: 10.32743/UniSoc.2025.125.10.20971.