Tolstoy, 1989d – *Tolstoy L.* Komu u kogo uchit'sya pisat', krest'yanskim rebyatam u nas, ili nam u krest'yanskikh rebyat? // Leo N. Tolstoy, Pedagogicheskiye sochineniya, (ed.) I. F. Protchenko, Moscow: Pedagogika, 1989. P. 301-324.

Tolstoy, 1989e – *Tolstoy L.* Progress i opredeleniye obrazovaniya // Leo N. Tolstoy, Pedagogicheskiye sochineniya, (ed.) I. F. Protchenko, Moscow: Pedagogika, 1989. P. 325-355.

Tolstoy, 2003 – *Tolstoy L.* Filosofskiy dnevnik. 1901-1910, (ed.) Nikolyukin A. N. Moscow: Izvestia, 2003. 543 p.

Veikshan, 1953 – *Veikshan V.* L.N. Tolstoy o vospitanii i obuchenii, Moscow: Academy of Pedagogical Sciences), 1953. 145 p.

Wenzel, 2013 – *Wenzel Ch. H.* Ethics and Relativism in Wittgenstein // Ethics – Society – Politics. Papers of the 35th International Wittgenstein Symposium, Berlin: De Gruyter Ontos. P. 348-350.

Wittgenstein, 1967 – *Wittgenstein L.* Remarks on the Foundations of Mathematics, (tr.) G. E. M. Anscombe, Cambridge, Massachusetts and London: The M.I.T. Press, 1967. 204. p.

Wittgenstein, 1999 – *Wittgenstein L.* Philosophical Investigations, G. E: M. Anscombe (tr.), Oxford and Malden, Massachusetts: Blackwell, 1999. 272 p.

УДК 001

Антюхова Е. А.,
доктор политических наук, доцент,
профессор кафедры мировых политических процессов,
МГИМО МИД России.

Крынжина М.Д.,
кандидат философских наук, доцент, доцент кафедры международной журналистики,
МГИМО МИД России.

Ценностные основания практик цифрового и технологического суверенитета ЕС

DOI: 10.33979/2587-7534-2025-4-134-147

Статья посвящена анализу ценностных оснований практик цифрового и технологического суверенитета ЕС. Концептуализированы понятия «научный суверенитет», «цифровой суверенитет», «технологический суверенитет». Определены различия в отечественных и европейских подходах к данным дефинициям. Систематизированы эффективные европейские практики, призванные обеспечить цифровой и технологический суверенитет ЕС. Сделан вывод, что практики технологического и цифрового суверенитета ЕС представляют собой не только инструменты обеспечения безопасности и

конкурентоспособности, но и механизмы глобальной трансляции и гегемонии европейских ценностей.

Ключевые слова: *научный суверенитет, цифровой суверенитет, технологический суверенитет, суверенитет ЕС, европейские ценности, практики ЕС.*

Antyukhova E. A.,
Doctor of Political Sciences, Associate professor,
Professor at the Department of Global Political Processes,
MGIMO University, Ministry of Foreign Affairs of the Russian Federation.

Krynzhina M. D.,
PhD in Philosophy, Associate professor,
Associate professor at the Department of International Journalism,
MGIMO University, Ministry of Foreign Affairs of the Russian Federation.

The value foundations of the EU's digital and technological sovereignty practices

This article analyzes the value foundations of the European Union's digital and technological sovereignty practices. It conceptualizes the terms «science sovereignty», «digital sovereignty», and «technological sovereignty». The study identifies differences between Russian and European approaches to these definitions. It systematizes effective European practices aimed at ensuring the EU's digital and technological sovereignty. The article concludes that the EU's technological and digital sovereignty practices serve not only as tools for ensuring security and competitiveness but also as mechanisms for the global dissemination and hegemony of European values.

Keywords: *science sovereignty, digital sovereignty, technological sovereignty, EU sovereignty, European values, EU practices.*

Введение

Современный мир переживает фундаментальные трансформации, связанные с изменением характера международных отношений, переходом к глобализации в формате многополярности, а также усилением роли государства в обеспечении стратегической независимости. В этих условиях концепты «научный суверенитет», «цифровой суверенитет» и «технологический суверенитет» приобретают особое значение. Концептуализация этих понятий позволяет по-новому осмыслить роль науки и технологий в контексте многочисленных вызовов национальной безопасности, сохранение культурной идентичности и устойчивое развитие.

В российской научной литературе акцент делается на анализе сущности технологического суверенитета с позиций экономического развития страны, что

отражает приоритеты государственной политики [Шкодинский, Кушнир, Продченко, 2022; Константинов, Константинова, 2022]. В мировой литературе вопросы технологического и цифрового суверенитета активно обсуждаются в рамках политической философии [Edler et al., 2023], экономики [Stephan, 2020] и международных отношений [Crespi et al., 2021]. Особое внимание в научных публикациях уделяется сравнительному анализу моделей цифрового и технологического суверенитета в разных регионах мира [Jiang, 2024]. Эти концепции рассматриваются как инструменты обеспечения национальной безопасности [Calderado, Blumfelde, 2022], экономической конкурентоспособности [Nouveau, 2020] и культурной идентичности [Ivic, Troitino, 2022] в условиях глобализации. При этом в научной литературе не выработаны единые подходы к определениям рассматриваемых понятий. И, как следствие отсутствия единого понимания данных дефиниций, наибольшие дискуссии в экспертных кругах вызывают вопросы о балансе между автономией [Broeders, Cristiano, 2023] и международным сотрудничеством [Fritzsche, Spoiala, 2022], а также о рисках нового технологического протекционизма и цифрового колониализма [Avila, 2018]. При этом практики обеспечения цифрового и технологического суверенитета рассматриваются в научном поле не только как средство защиты от внешнего влияния, но и продвижения ценностей [Roberts et al., 2021].

Анализ актуальных практик ЕС в контексте обеспечения научного суверенитета союза представляет особую ценность, так как ценностные основания в концепции европейского единства играют особую роль. Для того, чтобы выявить ценности, лежащие в основе стратегий технологического и цифрового суверенитета ЕС, необходимо решить следующие задачи: 1) концептуализировать понятия «научный суверенитет», «цифровой суверенитет», «технологический суверенитет»; 2) определить различия в отечественных и европейских подходах к данным дефинициям; 2) систематизировать эффективные европейские практики, призванные обеспечить технологический и цифровой суверенитет союзу.

Метод исследования

Если неолиберальная модель науки ориентирована на глобальный рынок, универсальность знаний и транснациональные стандарты научной деятельности, то концепт научного суверенитета подчеркивает необходимость организации научной деятельности в соответствии с национальными приоритетами государства, исходя из ценностных оснований национального научного сообщества [Балышев, Коннов, 2025]. Метод исследования основывается на теории культурной гегемонии А. Грамши, которая рассматривает, как доминирующие социальные группы, в данном случае институты ЕС, продвигают свои ценности, нормы и идеологические конструкты через культурные, образовательные и политические институты, формируя тем самым мировой консенсус вокруг внедряемых европейских практик и используя последние как средство легитимации ценностей ЕС в глобальном масштабе [Грамши, 1959]. В контексте технологического и цифрового суверенитета ЕС этот подход

позволяет проанализировать, как такие ценности, как стратегическая автономия, устойчивое развитие и ответственное использование данных, встраиваются в стратегии и практики технологического и цифрового суверенитетов союза, и как через экспорт нормативных стандартов формируется культурная и технологическая гегемония.

Научный, цифровой и технологический суверенитеты

В российских публикациях термин «научный суверенитет» или эквивалентный ему по смыслу концепт «суверенная наука» встречаются преимущественно в материалах научно-популярного характера, в то время как в научной периодике при анализе стратегических приоритетов развития науки в России используются термины «технологический суверенитет» и «цифровой суверенитет». Такое словоупотребление не случайно. В российской политике и официальных программных документах проблема обеспечения технологического суверенитета занимает центральное место. Стратегия научно-технологического развития Российской Федерации (2024) предлагает следующее определение «технологического суверенитета»: «способность государства создавать и применять наукоемкие технологии, критически важные для обеспечения независимости и конкурентоспособности, и иметь возможность на их основе организовать производство товаров (выполнение работ, оказание услуг) в стратегически значимых сферах деятельности общества и государства» [Указ, 2024]. Концепция технологического развития России на период до 2030 г. конкретизирует понятие «технологический суверенитет» в значении «наличия в стране (под национальным контролем) критических и сквозных технологий собственных линий разработки и условий производства продукции на их основе, обеспечивающих устойчивую возможность государства и общества достигать собственные национальные цели развития и реализовывать национальные интересы» [Концепция, 2023]. В Концепции также отмечается, что технологический суверенитет должен быть обеспечен в двух основных формах: «исследования, разработка и внедрение критических и сквозных технологий (по установленному перечню) и производство высокотехнологичной продукции, основанного на указанных технологиях».

Вопреки расхожему мнению, обеспечение технологического суверенитета не предполагает изоляционизма. Т. Гареев, исследуя западные подходы к осмыслению сущности технологического суверенитета, приходит к выводу, что практики реализации технологического суверенитета не противоречат призывам к углублению международной кооперации. Он заключает: «Судя по докладу ОЭСР, основной рекомендацией является введение уровня «общих ценностей» в основание научно-технологической политики. Другими словами, государственное вмешательство в экономические отношения может быть обосновано требованием технологического суверенитета, если для этого есть основание на уровне общих ценностей (например, демократии, прав человека, устойчивого развития и др.). Такой подход в целом соответствует современным западным философским представлениям о концепции суверенитета, в которых отводится роль ценностным и нравственным ориентирам» [Гареев, 2023]. Что

касается России, то в Концепции технологического лидерства отдельным пунктом указано, что обеспечить технологический суверенитет возможно «с опорой на устойчивое международное научно-техническое сотрудничество с дружественными странами» [Концепция, 2023], что, в свою очередь, косвенно подчеркивает роль общих ценностных установок в процессе международного научного сотрудничества.

Анализируя роль технологического суверенитета в системе национальной безопасности, А. Афанасьев трактует технологический суверенитет с позиций шести ракурсов: экономико-теоретического, системно-безопасностного, институционального, производственного, промышленно-политического, критериально-оценочного. Согласно данному подходу, с точки зрения целей обеспечения национальной безопасности «технологический суверенитет представляет собой достигнутый уровень реальной независимости страны в областях науки, техники и технологий, чем обеспечивается беспрепятственная реализация национальных интересов в техносфере с учетом существующих и перспективных угроз» [Афанасьев, 2025: 487].

Несмотря на то, что термин «цифровой суверенитет» в нормативных отечественных документах не закреплен, очевидно, что именно развитие цифровых технологий представляет критическую важность для обеспечения независимости страны и реализации задач в рамках приоритетных направлений научно-технологического развития. Более того, именно благодаря развитию цифровых технологий и распространению социальных медиа стало очевидно, что границы, которые существуют в онлайн-среде между странами, весьма условны. Сегментирование аудитории в цифровом пространстве было обусловлено преимущественно языковыми ограничениями, однако с развитием цифровых технологий и генеративных нейросетей эти и без того условные границы оказались стерты, что привело западных мыслителей к необходимости анализа сущности и условий существования суверенитета в цифровой среде. Так, исследуя взаимосвязь концептов «суверенитет» и «цифровой суверенитет», М. Роблес-Каррильо приходит к выводу, что научный дискурс пока не выработал единое определение и понимание функций цифрового суверенитета, «однако с точки зрения логики и согласно мнению большинства ученых, цифровой суверенитет должен пониматься как более широкое и общее понятие, а технологический суверенитет – как его компонент, нацеленный на сущностные аспекты» [Robles-Carrillo, 2023: 680]. Российские исследователи также указывают на то, что, несмотря на то что «в новых условиях интернет становится ключевым источником новых опасностей, у мировых правительств нет единых подходов к определению понятия «суверенитет в киберпространстве», ими не ведется работа по разработке международных соглашений, аналогичных договору о космосе, об Антарктике или о суверенитете в воздушном пространстве» [Безруков, 2021: 110].

Т. Гареев также приходит к выводу, что «неспособность эффективного регулирования технологических платформ (если не считать их полного запрета на территории) стала <…> тем вызовом, который привел к появлению концепции

технологического суверенитета в западных странах» [Гареев, 2023: 45]. Исследователь в данном случае синонимично использует слово «технологические» применительно к цифровым платформам.

Необходимость регулировать цифровые платформы обусловлена осознанием ценности больших данных и цифрового контента как стратегического ресурса внешнеполитического влияния на глобальном рынке цифровых технологий. И. Данилин подчеркивает, что «контроль за данными или особый режим доступа к ним, теоретически, может если не компенсировать «провалы», связанные с отсутствием крупных глобальных платформенных компаний, то, по крайней мере, создать некоторые альтернативные преимущества и каналы влияния» [Данилин, 2020: 110]. Поскольку ведущие цифровые платформы, пользующиеся глобальной популярностью, базируются в США и Китае, регионы остального мира, которые условно можно назвать «цифровой периферией» вынуждены принимать меры для защиты данных пользователей. Первопроходцами и примером в сфере цифрового регулирования и контроля данных являются страны ЕС благодаря имплементации Общего регламента защиты персональных данных (General Data Protection Regulation – далее GDRP) [Regulation, 2016]. Хотя GDRP не является международным договором, его нормы влияют на мировые стандарты защиты данных. Де-факто GDRP стал глобальным стандартом защиты данных благодаря заключению двусторонних соглашений с другими странами о передаче данных и необходимости транснациональных компаний соблюдать правила ЕС, чтобы работать на европейском рынке.

Практики цифрового и технологического суверенитета Европейского Союза

Политика ЕС в области научного суверенитета строится вокруг нескольких стратегических направлений, целью которых является укрепление автономии, конкурентоспособности и безопасности ЕС в сферах исследований, инноваций и критических технологий. Эта политика основывается на сочетании регламентов, промышленных стратегий, финансирования и международного сотрудничества в целях обеспечения ЕС статуса ключевого игрока в мировой науке. Концепции цифрового и технологического суверенитета сосуществуют в политике ЕС, но не являются взаимозаменяемыми, охватывая разные аспекты.

Цифровой суверенитет подразумевает способность стран-членов ЕС контролировать собственные цифровые инфраструктуры, данные и критически важные технологии, не завися от ключевых конкурентов – США и Китая. Д. Ламбах и Л. Монзеес, анализируя европейские подходы к концепту цифрового суверенитета отмечают, что «озабоченность Европейского Союза цифровым суверенитетом отражает как долгосрочные опасения, так и актуальные международные дискурсы. Понятие «суверенитет» особенно привлекательно в геополитической и экономической среде, которая воспринимается как неопределенная, быстро меняющаяся и угрожающая. Трудно не заметить, что современные дебаты – это очередное проявление классических страхов перед «технологическим разрывом» по сравнению с более развитыми глобальными

конкурентами. ЕС постоянно обеспокоен своей экономической конкурентоспособностью и инновационными возможностями. Цифровые технологии представляются как поле битвы в разворачивающемся геополитическом противостоянии между США и Китаем – или, в расширенной интерпретации, между демократией и автократией» [Lambach, Monsees, 2025: 83].

Таким образом, цели обеспечения цифрового суверенитета ЕС заключаются в уменьшении влияния глобальных цифровых платформ на европейское пространство, развитии европейских альтернатив в этом направлении, а также в обеспечении безопасности и конфиденциальности данных европейских пользователей. Таким образом, контроль над данными, включающий защиту, хранение и обработку информации, в совокупности с защитой от киберугроз и иностранного вмешательства определяют содержание практик ЕС по достижению цифрового суверенитета. К наиболее эффективным практикам в этой области следует отнести уже упомянутый выше регламент GDPR, а также проект европейского суверенного облака Gaia-X и Закон о данных, регулирующий доступ и использование данных в Европе.

Проект Gaia-X [Gaia-X] представляет собой инициативу ЕС, направленную на создание федеративной, суверенной и открытой инфраструктуры облачных вычислений, которая призвана обеспечить цифровой суверенитет Европы. В отличие от традиционных облачных платформ, где все данные и вычисления контролируются одним провайдером, Gaia-X распределён среди множества участников - компаний, государственных учреждений и исследовательских центров. Каждый участник управляет своей частью инфраструктуры, но все они следуют общим стандартам и правилам. Запущенный в 2020 году при поддержке Германии и Франции, Gaia-X ставит своей целью снижение зависимости от иностранных облачных платформ, таких как Amazon Web Services (США), Microsoft Azure (США) и Alibaba Cloud (Китай). Эти сервисы доминируют на мировом рынке облачных вычислений благодаря раннему выходу на рынок[5], эффекту масштаба[6], технологическому превосходству, широкому спектру услуг, глобальной инфраструктуре и развитой экосистеме партнеров. Проект Gaia-X, несмотря на нехватку инвестиций и машстаба, предлагает децентрализованную архитектуру, которая позволяет предприятиям и организациям хранить и обрабатывать данные в соответствии с GDRP.

Gaia-X можно считать эффективной практикой обеспечения цифрового суверенитета по нескольким причинам. Во-первых, проект позволяет европейским компаниям и государственным учреждениям хранить и обрабатывать данные на территории ЕС, что минимизирует риски несанкционированного доступа и утечек данных за пределы европейского

[5] AWS был запущен в 2006 году, Alibaba – в 2009, Azure – в 2010.

[6] AWS, Azure и Alibaba Cloud владеют самыми крупными дата-центрами в мире, что обеспечивает высокую производительность, надёжность и глобальное покрытие. Экономия на масштабе позволяет им предлагать услуги дешевле, чем конкуренты, что привлекает как малый бизнес, так и корпоративных клиентов.

пространства. За счет ожидаемого в перспективе снижения зависимости от доминирующих иностранных облачных сервисов, проект способствует экономической и политической автономии Европы, что, в свою очередь, создает условия для развития европейских технологий и компаний и, как следствие, роста конкурентоспособности ЕС в глобальной цифровой экономике.

Что же касается Закона о данных [Data Act], то это регламент Европейского Союза, принятый в январе 2024 года (первоначальный проект был представлен в феврале 2022 года), который устанавливает правила для доступа, использования и обмена данными на территории ЕС. Закон является частью стратегии ЕС по цифровому суверенитету и направлен на обеспечение контроля над данными, генерация которых происходит на территории Европы, а также на стимулирование инноваций и конкурентоспособности европейской экономики за счет обеспечения доступа к данным с цифровых устройств исследователям и промышленным компаниям, за исключением данных, содержащих коммерческую тайну или персональную информацию. Хотя закон запрещает компаниям накладывать несправедливые ограничения на доступ к данным, если это препятствует конкуренции и инновациям, и гарантирует, что права на интеллектуальную собственность не нарушаются при обмене данных, не все компании готовы предоставлять доступ к своим данным из-за отсутствия стандартизированных форматов или боязни утечки конфиденциальной информации. Кроме того, закон обязывает компании в случае кризисов и в целях обеспечения общественных интересов предоставлять данные государственным учреждениям для принятия решений.

Понимание технологического суверенитета в стратегиях ЕС по научному развитию выходит за рамки цифровых технологий и фокусируется на владении критически важными технологиями во всех сферах науки, как-то: промышленность, энергетика, оборона, здравоохранение и прочие отрасли. О. Еремченко и Н. Куракова приходят к выводу, что предпосылкой к переосмыслению странами ЕС концепции технологического суверенитета стало осознание в период пандемии углубляющейся технологической и производственной зависимости Европы от других государств. Исследователи отмечают, что «в странах Европейского союза обсуждение проблемы обеспечения технологического суверенитета сосредоточено на трех аспектах – экономическом, политическом и академическом» [Еремченко, Куракова, 2023: 49]. Стратегия технологического суверенитета ставит перед странами ЕС следующие задачи: развитие критических технологий – полупроводники, искусственный интеллект, квантовые технологии, биотехнологии – и, как следствие, снижение зависимости от иностранных технологий (например, тайваньских чипов); стимулирование европейских инноваций за счет финансирования и, как следствие, контроль над стратегическими технологиями.

К наиболее эффективным практикам в области обеспечения технологического суверенитета ЕС следует отнести Европейский закон о чипах [European Chips Act, 2022], Стратегию ЕС по критическим сырьевым материалам [Critical Raw Materials Act, 2023], проект по созданию европейской квантовой

коммуникационной инфраструктуры EuroQCI [Quantum Communication Infrastructure, 2019], а также программу «Глобальный портал» [Global Gateway].

Цель Европейского закона о чипах заключается в обеспечении стратегической автономии ЕС в производстве полупроводников и снижении зависимости от Тайваня (TSMC), США (Intel, NVIDIA) и Китая, так как зависимость от Азии, на территории которой производится до 70% мирового объема чипов, и США создаёт потенциальные угрозы для безопасности и экономики ЕС, особенно в условиях торговых войн и санкций. Выгодным отличием закона ЕС от аналогичных регламентов и нормативных документов, действующих в других странах, является акцент на сотрудничестве между странами ЕС и частным сектором и диверсификации источников сырья и компонентов для нивелирования рисков зависимости от одного региона. В отличие от США и Китая, ЕС стремится к сбалансированному развитию всей цепочки производства полупроводников, что делает данный подход к реализации технологического суверенитета более гибким и адаптивным к вызовам глобальной экономики.

В свою очередь, Стратегия по критически важным сырьевым материалам представляет собой комплексную инициативу, направленную на снижение зависимости ЕС от импорта редкоземельных металлов, лития, кобальта и других стратегических ресурсов, которые являются основой для развития зелёных технологий, таких как аккумуляторы для электромобилей, солнечные панели, ветряные турбины, и цифровых инноваций, к которым можно отнести в том числе и полупроводники. Так как на сегодняшний день до 90% редкоземельных металлов поставляется из Китая, что создаёт значительную угрозу для европейской промышленности в случае торгового конфликта, данная стратегия переориентирует страны ЕС на активное сотрудничество с альтернативными поставщиками в Африке и Латинской Америке. Документ также предусматривает создание стратегических запасов сырья, что в перспективе позволит ЕС гарантировать стабильность цен и непрерывность производства критически важных технологий даже в условиях глобальных кризисов.

Будучи частью более широкой программы Quantum Technologies Flagship, инновационный проект EuroQCI, цель которого заключается в разработке и внедрении квантовой коммуникационной инфраструктуры для защищенного обмена данными, уже демонстрирует конкретные достижения, хотя он все еще находится на этапе развертывания. По данным на 2025 год, в рамках реализации проекта уже запущены пилотные квантовые сети в Германии, Нидерландах и Франции, разработаны квантовые повторители для увеличения дальности передачи данных, что на данным момент является основополагающим ограничением для развития квантового интернета. Планируемое подключение к квантовой сети всех государственных учреждений ЕС позволит странам Европы защитить коммуникации от кибератак и обеспечить долгосрочную безопасность данных, что критически важно для государственных учреждений, обороны и критической инфраструктуры.

Еще одна практика по обеспечению технологического суверенитета ЕС – программа Global Gateway – инициатива, запущенная в 2021 году в целях укрепления сотрудничества со странами Африки, Латинской Америки, Азии и Восточной Европы в области инфраструктуры, цифровых технологий и устойчивого развития с анонсированным бюджетом в 306 млрд евро. По сути, данная программа является европейской альтернативой китайской инициативе «Один пояс, один путь». Е. Хельдт полагает, что именно «возвышение Китая как глобального финансиста инфраструктурных проектов <…> побудило ЕС проявить готовность и необходимость играть более активную геополитическую лидерскую роль, чтобы противодействовать китайскому влиянию на африканском континенте и за его пределами, одновременно формируя собственную сферу влияния Евросоюза» [Heldt, 2023: 225].

Хотя Global Gateway позиционируется Евросоюзом как инициатива, направленная на устойчивое развитие, страны-партнеры, среди которых лидирующее место по количеству реализуемых проектов занимают государства африканского континента, усматривают в таком взаимодействии риски формирования модели цифрового колониализма под видом взаимовыгодного сотрудничества. Например, инвестиции ЕС в развитие цифровой инфраструктуры в виде подводных кабелей, облачных платформ и центров обработки данных в Африке и Латинской Америке часто сопровождаются навязыванием европейских стандартов, платформ и регуляторных норм, что ограничивает местные компании в развитии собственных технологических решений. Кроме того, контроль над критически важной инфраструктурой со стороны европейских компаний может привести к зависимости стран-партнеров от ЕС, аналогично тому, как это происходит в рамках китайской инициативы «Один пояс, один путь». В долгосрочной перспективе это создаст риски утраты цифрового суверенитета местными правительствами, поскольку ключевые решения в области технологий, данных и безопасности будут приниматься за пределами этих стран.

Анализируя текущее отношение африканских стран-партнеров к формату сотрудничества в рамках программы Global Gateway, Е. Хельдт резюмирует: «В целом представители африканских стран критикуют патерналистский подход ЕС <…> страны-реципиенты недовольны ценностно-ориентированным подходом ЕС <…> При реализации "Global Gateway" важно, чтобы ЕС избегал ловушки действий как колониальной державы, диктуя правила и воссоздавая зависимости. Предоставление африканским странам определённой самостоятельности имеет решающее значение для успешной реализации всего процесса» [Heldt, 2023: 230].

Заключение

Цифровой суверенитет в политике ЕС фокусируется на контроле над данными, цифровыми инфраструктурами и защите от киберугроз, в то время как технологический суверенитет охватывает более широкий спектр критических технологий – от полупроводников и квантовых коммуникаций до энергетической и промышленной независимости. Эти концепции не являются

взаимозаменяемыми, но дополняют друг друга, формируя комплексную стратегию, направленную на укрепление автономии, конкурентоспособности и безопасности ЕС в глобальном мире. При этом ценностные основания практик технологического и цифрового суверенитета ЕС включают демократию, права человека, устойчивое развитие и этичное использование технологий, что отражает стремление союза не только к технологической автономии, но и к глобальному доминированию в результате формирования новой культурной и политической идентичности Европы.

Систематизация практик ЕС выявила, что наиболее эффективными инструментами обеспечения технологического и цифрового суверенитета являются такие нормативные стандарты и проекты, как Общий регламент защиты персональных данных, проект суверенного европейского облака, Европейский закон о чипах, Закон о данных, проект по созданию европейской квантовой коммуникационной инфраструктуры и проект «Глобальный портал». Эти нормативные стандарты и инициативы не только укрепляют автономию ЕС в критических технологических сферах, но и транслируют европейские ценности на глобальном уровне, формируя новую модель цифрового и технологического лидерства. Вместе с тем реализация таких проектов, как «Глобальный портал», сталкивается с критикой со стороны стран-партнеров, которые усматривают в них риски цифрового колониализма и навязывания европейских стандартов.

Таким образом, практики технологического и цифрового суверенитета ЕС представляют собой не только инструменты обеспечения безопасности и конкурентоспособности, но и механизмы трансляции ценностей, формирующих новую культурную и политическую идентичность Европы в условиях многополярного мира и глобальной цифровой фрагментации.

Список литературы

Афанасьев, 2022 – *Афанасьев А. А.* Технологический суверенитет: к вопросу о сущности //Креативная экономика. 2022. Т. 16. №. 10. С. 3691-3708.

Афанасьев, 2025 – *Афанасьев А. А.* Технологический суверенитет: сущность, цели и механизм достижения //Вопросы инновационной экономики. 2025. Т. 15. №. 2. С. 469-488.

Балыше, Коннов, 2025 – *Балышев А., Коннов В.* Глобальная наука и национальные научные культуры: трудности сопряжения //Международные процессы. 2025. Т. 14. №. 3. С. 96-111.

Безруков, 2021 – *Безруков А. О.* и др. Суверенитет и "цифра" //Россия в глобальной политике. 2021. Т. 19. №. 2 (108). С. 106-119.

Гареев, 2023 – *Гареев Т. Р.* Технологический суверенитет: от концептуальных противоречий к практической реализации //Terra Economicus. 2023. Т. 21. №. 4. С. 38-54. С. 42.

Грамши, 1959 – *Грамши А.* Избранные произведения : в 3 т. / пер. с итал. М., 1959. Т. 3 571 с.

Данилин, 2020 – *Данилин И. В.* Влияние цифровых технологий на лидерство в глобальных процессах: от платформ к рынкам? //Вестник МГИМО Университета. 2020. №. 1 (70). С. 100-116.

Еремченко, Куракова, 2023 – *Ерёмченко О. А., Куракова Н. Г.* Измерение уровня технологического суверенитета в зарубежных странах: опыт Европейского союза //Экономика науки. 2023. Т. 9. №. 3. С. 47-60.

Константинов, Константинова, 2022 – *Константинов И. Б., Константинова Е. П.* Технологический суверенитет как стратегия будущего развития российской экономики //Вестник Поволжского института управления. 2022. Т. 22. №. 5. С. 12-22.

Концепция, 2023 – Концепция технологического развития на период до 2030 года. Утверждена распоряжением Правительства Российской Федерации от 20 мая 2023 г. № 1315-р. URL: http://static.government.ru/media/files/KlJ6A00A1K5t8Aw93NfRG6P8OIbBp18F.pdf (дата обращения: 21.10.2025)

Указ, 2024 – Указ Президента Российской Федерации от 28 февраля 2024 г. № 145 "О Стратегии научно-технологического развития Российской Федерации". URL: https://www.garant.ru/products/ipo/prime/doc/408518353/ (дата обращения: 09.11.2025)

Шкодинский, Кушнир, Продченко, 2022 – Шкодинский С. В., Кушнир А. М., Продченко И. А. Влияние санкций на технологический суверенитет России //Проблемы рыночной экономики. 2022. Т. 2. №. 1. С. 75-96.

Avila, 2018 – *Avila Pinto R.* Digital sovereignty or digital colonialsim //SUR-Int'l J. on Hum Rts. 2018. Vol. 15. P. 15.

Broeders, Cristiano, 2023 – *Broeders D., Cristiano F., Kaminska M.* In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions //JCMS: Journal of Common Market Studies. 2023. Vol. 61. No. 5. P. 1261-1280.

Calderado, 2021 – *Calderaro A., Blumfelde S.* Artificial intelligence and EU security: The false promise of digital sovereignty //European Security. 2022. Vol. 31. No. 3. P. 415-434.

Crespi et al., 2021 – *Crespi F. et al.* European technological sovereignty: an emerging framework for policy strategy //Intereconomics. 2021. Vol. 56. No. 6. P. 348-354.

Critical Raw Materials Act, 2023 – European Critical Raw Materials Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/european-critical-raw-materials-act_en (дата обращения: 11.11.2025)

Data Act – Data Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (дата обращения: 11.11.2025)

Edler et al., 2023 – Edler J. et al. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means //Research Policy. 2023. Vol. 52. No. 6. P. 104765.

European Chips Act, 2022 – European Chips Act. URL: https://digital-strategy.ec.europa.eu/en/policies/european-chips-act (дата обращения: 11.11.2025)

Fritasche, Spoiala, 2022 – *Fritzsche K., Spoiala D.* The EU–AU Digital Partnership: Between Digital Geopolitics and Digital Sovereignty //Africa–Europe Cooperation and Digital Transformation. Routledge, 2022. P. 17-31.

Global Gateway – Global Gateway. URl: https://commission.europa.eu/topics/international-partnerships/global-gateway_en (дата обращения: 19.10.2025)

Heldt, 2023 – *Heldt E. C.* Europe's Global Gateway: A New Instrument of Geopolitics // Politics and Governance. 2023. Vol. 4. No. 11. P. 223-234.

Ivic, Troitino, 2022 – *Ivic S., Troitiño D. R.* Digital sovereignty and identity in the European union: A challenge for building Europe //European Studies. 2022. Vol. 9. No. 2. P. 80-109.

Jiang, 2024 – *Jiang M.* Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa //Policy & Internet. 2024. Vol. 16. No. 4. P. 727-738.

Lambach, 2025 – *Lambach D., Monsees L.* Beyond sovereignty as authority: the multiplicity of European approaches to digital sovereignty //Global Political Economy. 2025. Vol. 4. No. 1. P. 71-88.

Nouveau, 2020 – *Nouveau P.* European Union’s digital governance versus United States’ digital dominance //Revue de la Faculté de droit de l’Université de Liège. 2020. Vol. 2.

Quantum Communication Infrastructure, 2019 – Quantum Communication Infrastructure. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (дата обращения: 11.11.2025)

Regulation, 2016 – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed: 09.11.2025)

Roberts et al., 2021 – *Roberts H. et al.* Safeguarding European values with digital sovereignty: An analysis of statements and policies //Internet Policy Review, Forthcoming. 2021.

Robles-Carrillo, 2023 – *Robles-Carrillo M.* Sovereignty vs. Digital Sovereignty //Journal of Digital Technologies and Law. 2023. Vol. 3. No. 1. P. 673-690.

Stephan, 2020 – *Stephan P. B.* Sovereignty and the World Economy //U. St. Thomas LJ. 2020. Vol. 17. P. 649.