УДК 339.54.012.435 **DOI 10.52928/2070-1632-2025-73-4-42-49**

ЦИФРОВОЙ ПРОТЕКЦИОНИЗМ: ТЕНДЕНЦИИ РЕГУЛИРОВАНИЯ ТРАНСГРАНИЧНЫХ ЦИФРОВЫХ ПОТОКОВ

М.В. МИЛЕНИН
(Белорусский государственный экономический университет, Минск)

В эпоху цифровизации экономики данные становятся стратегическим ресурсом, а трансграничные потоки информации – критически важным элементом глобальной торговли и инновационного развития. На фоне растущих угроз кибербезопасности, доминирования глобальных цифровых платформ и обострения геоэкономической конкуренции государства усиливают меры цифрового протекционизма, направленные на защиту суверенитета и поддержку отечественных компаний. В статье представлен комплексный анализ современных регуляторных практик, рассмотрены формы цифрового протекционизма, их институциональные основания и экономические последствия. Особое внимание уделено оценке влияния цифровых барьеров на малый и средний бизнес. Сформулированы рекомендации по обеспечению баланса между цифровым суверенитетом и необходимостью поддержания открытости глобального цифрового пространства.

Ключевые слова: *протекционизм, цифровой протекционизм, локализация, цифровой суверенитет, цифровые налоги, международная торговля.*

Введение. В XXI веке цифровая трансформация мировой экономики стала определяющим фактором изменения структуры производства, торговли и государственного управления. Данные превратились в стратегический ресурс, а трансграничные цифровые потоки – в основу глобальных экономических процессов. Однако рост объёмов данных сопровождается усилением угроз кибербезопасности, зависимостью от транснациональных цифровых корпораций и снижением национального контроля над цифровой инфраструктурой. В этих условиях государства активно прибегают к инструментам цифрового протекционизма, стремясь обеспечить цифровой суверенитет и защиту внутреннего рынка. Актуальность темы определяется тем, что цифровой протекционизм перестаёт быть реакцией на технологические вызовы и превращается в устойчивую форму государственной экономической политики. Он влияет не только на инновационное развитие и международную торговлю, но и на баланс глобальной конкуренции, усиливая процессы цифровой фрагментации. Отсутствие единых подходов к регулированию трансграничных потоков данных усиливает противоречие между национальными интересами и принципами открытой цифровой экономики.

Цель исследования заключается в комплексном анализе форм, инструментов и последствий цифрового протекционизма в контексте глобальной цифровой трансформации. Для достижения цели решаются следующие задачи:

– Систематизировать подходы к определению понятия «цифровой протекционизм» и выявить его теоретические основы.

– Определить ключевые формы цифрового протекционизма и проанализировать их институциональные характеристики.

– Исследовать влияние цифровых барьеров на экономическую эффективность и инновации.

– Сравнить национальные модели регулирования цифрового пространства.

– Выявить экономические последствия цифрового протекционизма для различных групп стран и предложить рекомендации по достижению баланса между цифровым суверенитетом и глобальной открытостью.

Проблематика цифрового протекционизма в научных исследованиях получила развитие на стыке международной экономики, цифрового права и информационной безопасности. Исследования цифрового протекционизма за последние годы демонстрируют рост внимания к проблемам регулирования трансграничных потоков данных, цифрового суверенитета и влияния цифровых барьеров на международную торговлю. Значительный вклад в развитие теоретической базы внесли аналитические материалы Организации экономического сотрудничества и развития (далее – ОЭСР), Всемирной торговой организации (далее – ВТО), Всемирного банка, где цифровые ограничения рассматриваются как новый тип нетарифных барьеров, формирующих структурные изменения в мировой торговле услугами. В трудах Ааронсон С. обосновывается взаимосвязь между локализацией данных и снижением международной инновационной активности. Автор указывает, что введение жестких правил хранения данных ведёт к росту операционных затрат и препятствует распространению облачных технологий [1]. Рана Сингх, Снехил Радж проводят количественную оценку влияния цифровых барьеров на конкурентоспособность фирм. Их исследования показывают, что жесткие требования к локализации повышают стоимость ведения бизнеса на 7–11% и особенно негативно влияют на малые и средние предприятия, которые не обладают ресурсами для соблюдения сложных требований [2]. Европейский академический дискурс представлен в исследовании ОЭСР, анализирующем влияние валового внутреннего продукта на трансграничные цифровые потоки. Авторы делают вывод, что строгие нормы Европейского Союза (далее – ЕС) фактически экспортируются за пределы Евросоюза, формируя новый тип «регуляторного протекционизма» [3].

Особое место занимают исследования азиатских авторов. Жао Луан и Ли Джонхва рассматривают цифровой протекционизм как центральный элемент китайской модели цифрового суверенитета. Они отмечают, что

Китай выстраивает замкнутую цифровую экосистему, формирующую преимущества для национальных компаний [4–5]. Шарма Р. анализирует последствия блокировки китайских приложений и показывают, что эти меры ускорили развитие собственных платформ [6].

В российской и белорусской литературе феномен цифрового протекционизма освещён ограниченно. В работах Марковой О.А. и Мелешкиной А.И. цифровой протекционизм трактуется преимущественно как совокупность ограничительных мер по защите персональных данных, без развития институциональной типологии инструментов [7]. В исследованиях А.А. Игнатова подчеркивается влияние цифровых барьеров на российский ИТ-сектор, однако недостаточно проработаны сравнительные аспекты международных моделей регулирования [8].

Таким образом, современная литература охватывает широкий спектр вопросов – от локализации данных до цифровых налогов и национальных моделей регулирования, однако носит фрагментарный характер. Исследователи концентрируются преимущественно на отдельных инструментах или отдельных странах, в то время как комплексный подход встречается редко.

Анализ литературы показывает, что:

– отсутствует цельное институциональное сравнение цифровых протекционистских моделей ЕС, США, Китая, Индии и ЕАЭС;

– недостаточно исследовано влияние цифровых барьеров и их доступ к глобальным цифровым рынкам;

– не разработана единая классификация инструментов цифрового протекционизма, учитывающая правовые, технические и фискальные механизмы;

– на сегодняшний день есть мало работ, оценивающих международные последствия цифровой фрагментации для инноваций и глобальных цепочек создания стоимости.

Настоящая статья восполняет этот пробел, предлагая комплексный сравнительный анализ, структурную классификацию инструментов и оценку их экономического воздействия.

Методологической основой исследования является комплексный междисциплинарный подход, объединяющий положения институциональной теории, неомеркантилизма, концепции цифрового суверенитета и прагматического национализма. Для решения поставленных задач применялись сравнительный анализ национальных моделей регулирования цифрового пространства, системный анализ взаимосвязей между инструментами цифрового протекционизма и их макроэкономическими последствиями, экономико-статистические методы – обработка и сопоставление данных ВТО, ОЭСР и национальных регуляторов, контент-анализ нормативных актов и программных документов стран-лидеров в цифровом регулировании.

Цифровая трансформация мировой экономики сопровождается глубинными изменениями в структуре производства, торговли и управления. Основой этих изменений становится стремительный рост объемов создаваемых, передаваемых и обрабатываемых данных. Информация, ранее рассматривавшаяся как вспомогательный элемент бизнес-процессов, приобретает статус самостоятельного экономического ресурса, сопоставимого по значимости с капиталом, трудом и природными ресурсами. Цифровая экономика характеризуется высокой степенью интеграции глобальных ИТ-инфраструктур, повсеместным распространением облачных сервисов, ростом роли платформенных бизнес-моделей и усилением взаимозависимости национальных экономик. В этом контексте трансграничные потоки данных становятся ключевым условием нормального функционирования как частного бизнеса, так и государственных институтов. Они обеспечивают возможность глобального взаимодействия в таких отраслях, как финансы, телекоммуникации, электронная коммерция, медицина, образование, научные исследования и государственное управление [7, с. 28].

Однако по мере нарастания интенсивности глобальных цифровых потоков усиливаются и риски, связанные с их бесконтрольным распространением. В первую очередь, речь идет об угрозах кибербезопасности, конфиденциальности персональных данных, зависимости от иностранных технологических гигантов, а также об ограничениях государственного контроля за важнейшими элементами цифровой инфраструктуры. Эти вызовы актуализируют дискуссию о необходимости защиты цифрового суверенитета как основы национальной безопасности в условиях глобализации.

В ответ на данные вызовы государства по всему миру начали внедрять широкий спектр регулирующих и ограничительных мер, направленных на обеспечение контроля за трансграничными потоками данных. Эти меры получили обобщающее название «цифровой протекционизм». Он охватывает такие инструменты, как обязательная локализация данных, запреты и ограничения на международную передачу информации, введение цифровых налогов, установление национальных стандартов сертификации и безопасности, блокировка цифровых сервисов иностранных компаний и целевая поддержка отечественных разработчиков цифровых решений. Возникает новая парадигма государственного вмешательства в цифровую экономику, которая характеризуется одновременным стремлением к стимулированию инноваций и защите стратегически значимых цифровых активов. Формируется противоречивое пространство, где с одной стороны – декларации о поддержке открытого интернета и глобального обмена данными, а с другой – последовательное выстраивание нормативных барьеров и усиление юрисдикционного контроля. Именно в этой напряженной плоскости находится феномен цифрового протекционизма.

Научная и практическая значимость данной темы обусловлена тем, что в условиях растущей цифровой фрагментации и обострения геоэкономической конкуренции государства вынуждены искать оптимальные регуляторные модели. Эти модели должны учитывать потребность в обеспечении безопасности и конфиденциальности,

необходимость поддержки национальных ИТ-секторов и одновременно избегать чрезмерных барьеров, снижающих эффективность глобального экономического взаимодействия.

Таким образом, исследование цифрового протекционизма как комплексного явления на стыке экономики, международного права и информационной безопасности становится особенно актуальным. Анализ регуляторных подходов различных стран и регионов, выявление их преимуществ и рисков, а также выработка рекомендаций по достижению баланса между интересами суверенитета и свободной торговли представляет собой основную цель настоящего исследования.

Основная часть. В последние два десятилетия понятие «протекционизм» претерпело заметную трансформацию. Если традиционно оно ассоциировалось с тарифными барьерами, квотами и субсидиями в отношении физических товаров, то с развитием цифровой экономики возникла необходимость осмысления иного, более гибкого и технологически обусловленного протекционизма. Цифровой протекционизм – это форма государственной политики, направленная на ограничение трансграничного обмена данными, предоставления цифровых услуг и доступа иностранных компаний к цифровым рынкам через меры правового, технического и организационного характера.

Исторически, первые элементы цифрового протекционизма начали появляться в странах с авторитарными политическими режимами, где контроль над информационными потоками рассматривался как инструмент внутренней стабильности. Однако в условиях роста цифровой зависимости даже демократические государства начали разрабатывать национальные стратегии по защите цифрового суверенитета. Это связано не только с угрозами кибербезопасности, но и с необходимостью создания условий для развития собственных технологических компаний, минимизации зависимости от иностранных платформ, а также защиты интересов граждан.

С усилением цифровой фрагментации глобального пространства возникает риск формирования так называемого «сплинтернета» – множества несвязанных между собой цифровых экосистем, функционирующих по различным стандартам и регулируемым разными юрисдикциями. Этот процесс сопровождается как легитимными стремлениями государств к защите своих стратегических интересов, так и скрытым протекционизмом в пользу национальных компаний. Особенность цифрового протекционизма заключается в его латентной природе. Он редко выражается в явных ограничениях, чаще – в усложнении доступа через комплекс требований к хранению, обработке и передаче данных, сертификации оборудования, соблюдению местных норм и стандартов. В то же время он тесно переплетается с другими глобальными вызовами: торговыми войнами, санкциями, конкуренцией за лидерство в сфере искусственного интеллекта (далее – ИИ) и технологий больших данных.

Термин «цифровой протекционизм» охватывает широкий спектр мер, включая обязательную локализацию данных, ограничение трансграничной передачи информации, налогообложение цифровых гигантов, требования к техстандартам и доступу к рынкам. Теоретически цифровой протекционизм опирается на концепции неомеркантилизма, цифрового суверенитета и прагматического национализма. Возникает дилемма: безопасность против эффективности, приватность против глобализации. Формы цифрового протекционизма являются отражением стратегий, с помощью которых государства стремятся одновременно защитить свои цифровые интересы и сохранить конкурентоспособность в условиях растущей зависимости от информации. Эти формы могут различаться по степени строгости, характеру правового регулирования и целевым эффектам. Основные формы цифрового протекционизма представлены на рисунке 1.

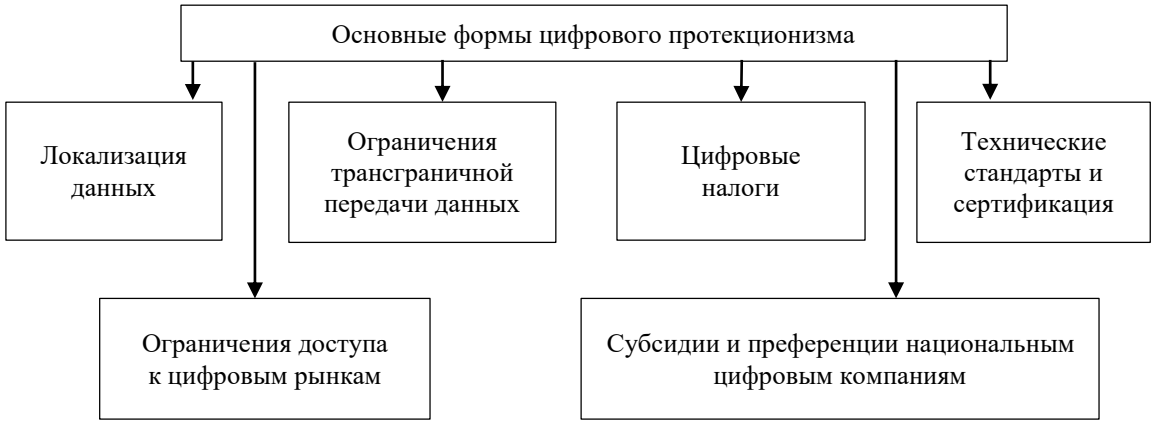

Рисунок 1. – Основные формы цифрового протекционизма

Таким образом, представленные на рисунке 1 основные формы цифрового протекционизма демонстрируют широкий спектр инструментов, применяемых в мировой практике. Каждая из форм направлена на решение определённого круга задач – от защиты персональных данных до поддержки национальных производителей цифровых решений. Для полноценного понимания сущности и значимости этих форм необходимо более подробно рассмотреть механизмы их реализации, особенности правового регулирования, а также последствия, возникающие в результате их применения в различных странах и юрисдикциях.

Локализация данных представляет собой требование к компаниям осуществлять хранение и/или обработку определенных категорий данных исключительно на территории конкретной страны. Как правило, под такие требования попадают персональные данные, медицинская и финансовая информация, а также данные, имеющие стратегическое значение. Наиболее жесткий подход в этом вопросе демонстрирует Китай, где действует прямая обязательность локализации, в том числе для всех операторов критической информационной инфраструктуры. С 2021 г. в Китае действует Закон о защите персональной информации, обязывающий компании, обрабатывающие персональные данные более 1 млн пользователей, проходить обязательную проверку при передаче данных за рубеж. В 2022 г. власти заблокировали зарубежный листинг платформы Didi после того, как выяснилось, что компания экспортировала пользовательские данные без согласования с регуляторами. В России аналогичные нормы зафиксированы в Федеральном законе «О персональных данных», а в Индии в 2023 г. был принят проект закона, требующий локализации чувствительных данных.

Ограничения трансграничной передачи данных дополняют политику локализации и устанавливают условия, при которых передача данных за рубеж возможна. Это может включать необходимость получения разрешения от уполномоченного органа, заключения договоров с иностранными контрагентами, обеспечивающих эквивалентную защиту, или прохождения сертификации. Например, в ЕС передача персональных данных за пределы Европейской экономической зоны регулируется пятой главой «Общего регламента по защите данных» (далее – GDPR), требующей оценки «адекватности» законодательства третьей страны. В 2023 г. компания Meta была оштрафована на 1,2 млрд евро за передачу пользовательских данных из ЕС в США без должной правовой основы. Это крупнейший на данный момент штраф в рамках GDPR и прецедент в области трансграничного регулирования.

Цифровые налоги (Digital Services Taxes, далее – DST) стали одним из инструментов фискального протекционизма. Они направлены на обложение доходов транснациональных цифровых компаний, действующих на национальных рынках без физического присутствия. В 2019 г. Франция первой в ЕС ввела 3%-й налог на доходы крупных цифровых компаний (Google, Amazon, Facebook), полученные на французском рынке. Это вызвало торговый конфликт с США, пригрозившими импортными пошлинами. В 2022 г. соглашение в рамках ОЭСР временно смягчило напряжённость, но вопрос остаётся открытым. В рамках Евразийского экономического союза (далее – ЕАЭС) рассматривается возможность введения унифицированного DST как меры бюджетного выравнивания и справедливой конкуренции. Введение цифровых налогов стало одной из ключевых форм фискального протекционизма, направленного на перераспределение доходов глобальных ИТ-компаний. Таблица 1 отражает основные параметры DST в ряде стран.

Таблица 1. – Цифровые налоги в международной практике[1]

Страна	Ставка DST, %	Порог применения (выручка)	Год	Особенности / последствия
Франция	3	> €750 млн глобально, > €25 млн во Франции	2019	Под угрозой ответных мер США
Великобритания	2	> £500 млн глобально, > £25 млн в Великобритании	2020	Временно до реализации реформы ОЭСР
Италия	3	> €750 млн глобально	2020	Активное давление США
ЕАЭС	Планируется	Унифицированная ставка обсуждается	–	В стадии координации

Анализ DST-практик показывает, что цифровые налоги становятся важным инструментом налогового выравнивания, но при этом вызывают геоэкономические трения. Инициатива ОЭСР по введению согласованного подхода может сгладить напряженность, но до её полной реализации страны продолжают действовать самостоятельно.

Технические стандарты и сертификация включают нормативные требования к цифровым продуктам и услугам, направленные на обеспечение безопасности, совместимости и прозрачности. В ЕС принят Закон об ИИ, который классифицирует ИИ-системы по уровню риска и вводит жёсткие регуляции. Китай требует обязательной сертификации программного обеспечения, а также импорта ИТ-оборудования согласно национальным стандартам кибербезопасности.

Ограничения доступа к цифровым рынкам охватывают блокировки отдельных платформ, приложений и сервисов. Это может объясняться как обеспечением национальной безопасности, так и стратегией поддержки локальных цифровых компаний. Так, Индия в 2020 г. ограничила доступ к более чем 200 китайским приложениям, включая TikTok, что сопровождалось развитием внутренних альтернативных решений. В Китае действует система фильтрации западных онлайн-сервисов, а в России ограничен доступ к иностранным цифровым платформам в ряде отраслей.

Субсидирование национальных цифровых компаний используется в виде налоговых льгот, грантов, государственных закупок и преференциальных режимов сертификации. Примером служит американский CHIPS Act, предусматривающий поддержку производителей полупроводников, и стратегия ЕС «Цифровой компас», предполагающая развитие локальной цифровой инфраструктуры. Следует отметить, что в большинстве случаев страны применяют не один, а совокупность различных инструментов цифрового регулирования, формируя уникальные модели, основанные на собственных приоритетах. Эти подходы определяют конфигурацию цифровых рынков, уровень конкуренции и перспективы технологического развития.

[1] URL: https://www.wto.org/english/res_e/booksp_e/world_tariff_profiles25_e.pdf

Одним из наиболее распространённых механизмов цифрового протекционизма остаётся требование локализации данных. В таблице 2 показаны различия в подходах к локализации персональной информации в разных странах и интеграционных объединениях.

Таблица 2. – География локализации данных[2]

Страна	Требование к локализации	Категории охвата	Год введения / последний пересмотр
Китай	Обязательная	Все персональные и критические данные	2017 / 2021
Россия	Обязательная	Персональные данные граждан страны	2006 / 2024
Индия	Частичная	Чувствительные и платежные данные	2023 (законопроект)
ЕС	Косвенная через GDPR	Персональные данные при передаче за рубеж	2018 / 2021
США	Отсутствует на федеральном уровне	–	–
ЕАЭС	Рекомендуемая локализация	Персональные данные	–

Из данных таблицы 2 видно, что наиболее строгие требования к локализации существуют в странах с централизованными моделями регулирования. В США отсутствует единая федеральная норма, тогда как в ЕС действует косвенный механизм через GDPR. Это вызывает сложности для транснациональных компаний, которым необходимо учитывать требования разных юрисдикций.

Национальные модели цифрового регулирования различаются в зависимости от стратегических приоритетов и правовых традиций. Например, Европейский союз продвигает концепцию «регуляторного суверенитета», экспортируя свои стандарты за рубеж. GDPR, вступивший в силу в 2018 году, стал ориентиром для многих стран. ЕС также реализует нормативные пакеты DMA и DSA, направленные на ограничение рыночной власти цифровых платформ. США традиционно отстаивают принцип свободного обращения цифровых потоков. Однако с усилением геополитической конкуренции они усиливают экспортный контроль и формируют элементы стратегического протекционизма. В качестве примера можно привести «CLOUD Act», который позволяет американским властям запрашивать данные, хранящиеся за рубежом, при наличии судебного разрешения. Китай выстраивает модель цифрового суверенитета, предполагающую приоритет внутреннего регулирования и поддержку национальных компаний. Принятые законы о кибербезопасности и защите персональных данных создают замкнутую экосистему с чёткими требованиями к локализации и сертификации цифровых продуктов. В рамках ЕАЭС формируется собственная модель цифровой интеграции, однако она сталкивается с институциональными барьерами и различиями в национальных законодательствах. В результате наблюдается разнородность практик по локализации и защите данных, несмотря на наличие координирующих решений на уровне Евразийской экономической комиссии. Таким образом, понимание различий между этими моделями необходимо для выработки эффективной стратегии цифрового регулирования, обеспечивающей баланс между национальной безопасностью, инновациями и международным сотрудничеством.

Рассмотрим экономические последствия цифрового протекционизма (таблица 3).

Таблица 3. – Матрица воздействия цифрового протекционизма на экономику

Показатель	Локализация	DST	Ограничения	Субсидии
Издержки	Рост транзакционных затрат	Рост налоговых издержек	Задержки в передаче данных	Риски неэффективного распределения ресурсов
Инновации	Замедление прогресса	Замедление цифрового развития	Снижение инвестиционной активности	
Защита данных	Усиление безопасности	–	Повышение конфиденциальности	Торможение конкуренции в инновациях
Конкуренция	Нарушение принципов свободной торговли	Укрепление позиций местных компаний	Создание преимуществ для локальных игроков	
Фрагментация	Создание барьеров	Рост различий в налогообложении	Разделение цифровых экосистем	Регионализация цифрового рынка

Экономические последствия цифрового протекционизма многогранны и затрагивают широкий спектр участников цифровой экономики – от транснациональных корпораций до малых и средних предприятий, от индивидуальных пользователей до государственных структур. Анализ практики разных стран позволяет выделить как негативные, так и условно позитивные эффекты от применения протекционистских мер в цифровой сфере.

Среди наиболее очевидных негативных последствий следует назвать:

1) рост затрат на соответствие требованиям. Для международных компаний, работающих в нескольких юрисдикциях, соблюдение национальных требований по локализации, сертификации и передаче данных приводит

[2] URL: https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf

к существенным административным и юридическим издержкам. По оценкам ОЭСР расходы на соответствие цифровым требованиям в странах с жёсткими регуляциями могут достигать 5–10% от оборота компании в данной стране, особенно это ощутимо для малых и средних предприятий;

2) снижение темпов инноваций. Ограничение трансграничных потоков данных затрудняет международное научное и технологическое сотрудничество, обмен большими данными, разработку и обучение алгоритмов ИИ. Это снижает конкурентоспособность национальных ИТ-компаний и тормозит внедрение новшеств, особенно в странах с узким внутренним рынком;

3) дублирование цифровой инфраструктуры. Введение обязательной локализации данных требует строительства дополнительных центров обработки данных, создания локальных облачных сервисов и разработки собственных цифровых решений. Эти меры увеличивают капитальные и эксплуатационные расходы, что отражается на конечных ценах для потребителей;

4) фрагментация цифрового рынка. Возникает эффект «сплинтернета» – разделения единого глобального пространства на множество несовместимых цифровых экосистем. Это затрудняет масштабирование бизнеса, усиливает регуляторную неопределенность и снижает эффективность глобальных цифровых платформ;

5) угрозы международным экономическим отношениям. Введение цифровых налогов без согласования с международными партнерами вызывает напряженность в торговых отношениях, провоцирует споры в рамках ВТО и может привести к ответным мерам. США, например, в 2021 г. угрожали введением санкций против стран, применивших односторонние DST в отношении американских компаний.

Однако цифровой протекционизм порождает и условно позитивные эффекты, особенно с точки зрения стран-инициаторов:

1) укрепление национального контроля и суверенитета. Государства получают возможность лучше контролировать оборот чувствительной информации, обеспечивать соответствие хранения данных внутреннему законодательству и реагировать на киберугрозы;

2) развитие локальных ИТ-рынков и стимулирование инвестиций. Обязательная локализация и меры поддержки национальных компаний способствуют росту числа дата-центров, появлению локальных облачных провайдеров и повышению ИТ-грамотности среди населения;

3) справедливое налогообложение глобальных платформ. Цифровые налоги позволяют странам перераспределить часть сверхприбыли транснациональных корпораций, получаемой за счёт локального потребления, в пользу национальных бюджетов.

Тем не менее, в долгосрочной перспективе чрезмерная регуляторная жесткость может привести к снижению глобальной конкурентоспособности, оттоку инвестиций и технологическому отставанию. По этой причине вопросы цифрового протекционизма приобретают острое значение не только для экономической политики, но и для стратегического развития. Современный этап развития мировой цифровой экономики характеризуется всё большей дифференциацией национальных подходов к регулированию цифрового пространства. Это, в свою очередь, приводит к росту числа межгосударственных коллизий, юридической фрагментации и снижению доверия между участниками глобальной цифровой экосистемы. В этих условиях становится очевидной необходимость поиска согласованных решений и создания универсальных или хотя бы регионально совместимых стандартов регулирования трансграничных потоков данных.

Один из ключевых вызовов на пути к глобальной гармонизации заключается в противоречии между правом государств на цифровой суверенитет и интересами международной торговли и инвестиций. Как показывает практика, наиболее эффективным механизмом для разрешения таких противоречий являются многосторонние или региональные платформы, обеспечивающие выработку сбалансированных решений. В этом контексте важное значение приобретают усилия международных организаций и инициатив. Примером является концепция «Data Free Flow with Trust» (далее – DFFT), предложенная Японией и поддержанная странами G20. Её идея заключается в обеспечении свободного движения данных между странами при сохранении высокого уровня доверия, основанного на прозрачности, безопасности и защите персональных данных. Несмотря на декларативную поддержку, механизмов имплементации DFFT пока недостаточно, а реальное продвижение ограничено разногласиями между основными геоэкономическими блоками.

Другим перспективным направлением является развитие соглашений нового поколения, таких как «Соглашение о партнерстве в области цифровой экономики» (Digital Economy Partnership Agreement, далее – DEPA), заключённого между Сингапуром, Чили и Новой Зеландией. Одним из первых результатов этого Соглашения стало создание «песочниц» для тестирования трансграничной идентификации и цифровой сертификации без барьеров. Сингапур и Новая Зеландия начали пилотные проекты, позволяющие компаниям обмениваться данными в режиме «доверенного потока», при этом соблюдая стандарты конфиденциальности обеих сторон. DEPA – это первое специализированное цифровое Соглашение, охватывающее не только традиционные аспекты торговли, но и вопросы совместимости регуляторных режимов, доверия к ИИ, цифровой идентификации и межгосударственного обмена данными. DEPA рассматривается как прототип будущих многосторонних соглашений, способных интегрировать принципы DFFT в практику международного регулирования.

Важнейшим игроком в области глобального регулирования остаётся ОЭСР, продвигающая концепцию в международной налоговой реформе, направленную на справедливое распределение доходов цифровых корпораций между странами. Реализация этого механизма может снизить напряженность, вызванную односторонним введением DST, и стать примером многостороннего компромисса.

Всемирная торговая организация также предпринимает усилия по выработке правил для цифровой торговли. С 2019 г. действует инициатива «О совместном заявлении по электронной коммерции», в рамках которой обсуждаются принципы трансграничной передачи данных, мораторий на цифровые таможенные пошлины, электронная идентификация и аутентификация. Однако переговорный процесс идёт медленно из-за расхождения позиций развитых и развивающихся стран. Развивающиеся государства и региональные объединения, такие как ЕАЭС, АСЕАН, Африканский союз, должны активно участвовать в этих процессах, чтобы избежать навязывания стандартов без учёта их специфики и интересов. Для этого важно использовать потенциал региональных институтов и формировать собственные предложения по регулированию цифровых потоков, включая создание доверенных трансграничных зон хранения и обработки данных. Таким образом, перспективы глобального согласования в сфере цифрового протекционизма зависят от способности стран и международных организаций преодолеть институциональные и геополитические барьеры. Основной задачей является разработка согласованных и взаимопризнаваемых стандартов, обеспечивающих баланс между безопасностью, инновациями и справедливой конкуренцией. Успех в этом направлении станет залогом устойчивого и инклюзивного развития глобальной цифровой экономики. Выработка таких решений невозможна без учёта потребностей всех участников цифрового взаимодействия – от крупных экономик до малых государств и отдельных потребителей.

Заключение. Цифровой протекционизм, будучи относительно новым явлением, стремительно трансформируется из реактивной меры отдельных государств в структурный элемент глобальной экономической архитектуры. С одной стороны, он отвечает на растущие вызовы кибербезопасности, цифровой зависимости и технологической уязвимости, а с другой – влечёт за собой рост фрагментации, снижение эффективности международного взаимодействия и риски замедления технологического прогресса. В условиях цифровизации все большего числа сфер жизни и производства, именно трансграничные потоки данных становятся критической инфраструктурой нового типа, и регулирование этой сферы приобретает экзистенциальное значение для государств. Цифровой протекционизм принимает разнообразные формы: от жёсткой локализации и блокировок до гибких механизмов налогообложения и стандартов сертификации. Эти меры позволяют государствам защищать свои интересы, но требуют высокой точности в применении, чтобы избежать избыточных барьеров для инноваций, особенно в малом и среднем бизнесе. Сравнительный анализ регуляторных моделей показал, что ни одна из существующих стратегий не является универсальной: ЕС стремится экспортировать свои правовые нормы, США балансируют между свободой и стратегическим контролем, Китай строит внутренне ориентированную систему, а ЕАЭС делает попытки согласования на фоне институциональной разнородности. Экономический анализ свидетельствует о высоких издержках цифрового протекционизма в долгосрочной перспективе, включая рост транзакционных затрат, снижение эффективности цифровых рынков и потенциальную утрату инновационного темпа. При этом важно отметить, что частичная протекция может быть оправдана в целях развития собственных ИТ-отраслей, защиты приватности граждан и управления критическими данными. Выход из данной дихотомии – в выработке гибких международных механизмов согласования, сочетающих принцип доверия, прозрачности и технологического нейтралитета. Важными шагами в этом направлении могут стать дальнейшее развитие инициатив DFFT и DEPA, а также укрепление роли ВТО и ОЭСР в координации цифровой торговли. Без участия всех акторов – от малых стран до крупнейших экономик – выработка сбалансированных решений невозможна.

Таким образом, цифровой протекционизм следует рассматривать не как временный инструмент, а как долгосрочную стратегическую задачу. Его регуляция требует тонкой настройки, институциональной гибкости и постоянного международного диалога. Лишь при этих условиях можно достичь баланса между цифровым суверенитетом и сохранением глобальной открытости, обеспечив тем самым устойчивость и инклюзивность цифровой экономики будущего. Международные усилия должны быть направлены на выработку сбалансированных решений, учитывающих легитимные интересы всех сторон.

ЛИТЕРАТУРА

1. Aaronson S. Could a Global «Wicked Problems Agency» Incentivize Data Sharing? [Electronic resource]. – URL: https://www.cigionline.org/static/documents/no.273_2r5SkXF.pdf (date of access: 23.10.2025).
2. Rana S., Snehil R. Data Localization And Its Impact On Cross-Border Digital Trade In India: Legal, Economic, And Strategic Implications // Educational Administration: Theory and Practice. – 2024. – № 30(3). – P. 3327-3333.
3. Measuring digital trade [Electronic resource]. – URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/measuring-digital-trade_bd0df576/48e68967-en.pdf (date of access: 23.10.2025).
4. Zhao L. China’s Data Sovereignty Strategy // China Economic Review. – 2023. – № 78. – P. 5–18.
5. Li W. Cybersecurity Regulation and Digital Protectionism in China // Journal of Information Policy. – 2022. – №. 12 – P. 45–58.
6. Sharma R. Digital Sovereignty in India: Policy Evolution and Economic Implications // Journal of Asian Public Policy. – 2021. – № 14(3). – P. 310-319.
7. Маркова О.А., Мелешкина А.И. Цифровой протекционизм: миф или реальность? [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/tsifrovoy-protektsionizm-mif-ili-realnost/viewer (дата обращения: 23.10.2025).
8. Игнатов А.А. Сравнительное исследование политики по реализации цифрового суверенитета государства странами-членами БРИКС // Вестник международных организаций. – 2025. – Т. 20. № 3. – С. 54–74.

Поступила 13.11.2025

DIGITAL PROTECTIONISM: TRENDS IN REGULATING CROSS-BORDER DIGITAL FLOWS

M. MILENIN
(Belarus State Economic University, Minsk)

In the digital economy era, data has become a strategic asset, and cross-border flows of information are essential to global trade and innovation. Amid rising cybersecurity threats, the dominance of major digital platforms, and intensified geoeconomic rivalry, states have adopted digital protectionist measures to safeguard sovereignty and support national firms. This article offers a comprehensive analysis of digital protectionism practices, identifies core instruments, institutional underpinnings, and economic impacts – especially on SMEs and innovation – and outlines policy recommendations to balance national interests and global digital openness.

Keywords: *protectionism, digital protectionism, cross-border data flows, data localization, digital sovereignty, digital taxes, international trade.*