

На пути к цифровому суверенитету. Новая повестка дня

Б. Н. Паньшин,
профессор
экономического факультета БГУ



■ Острота проблемы

Суверенитет всегда означает прежде всего независимость государства по отношению к другим странам и возможность осуществлять верховную власть по управлению всеми

полномочиями на своей территории. За годы независимости Беларусь последовательно и успешно формировала и укрепляла государственный суверенитет и его политические и экономические составляющие, в первую очередь продовольственный, энергетический и информационный суверенитет.

С ростом цифровой экономики все более актуальной становится проблема обеспечения национального цифрового суверенитета, который все более становится ключевой категорией в отношении государств к цифровым технологиям.

Если ранее в сфере информации рассматривалась проблема информационного суверенитета как осуществление контроля государства за информационными потоками и киберугрозами извне, то концепция цифрового

суверенитета учитывает новые риски широкого использования цифровых технологий для генерации и распространения контента. Дополнительно она ориентирована на защиту и эффективное использование внутренних потоков данных, которые фиксируются на территории страны. Речь идет как об оставляемых пользователями интернета «цифровых следах» в социальных сетях, в различных интернет-сервисах, в системах электронной торговли и т. д., так и потоках данных, генерируемых предприятиями и органами государственного управления.

Произошел качественный переход – данные стали рассматриваться как «новая нефть», а их маркетинговый анализ и сбыт послужили причиной образования интернет-гигантов, так называемой группы компаний



GAFA (Google, Apple, Facebook и Amazon), а также становления крупных отечественных и зарубежных ИТ-компаний. Для них масштабы сбора и алгоритмы систематизации и обработки данных составили основное конкурентное преимущество и стали источником огромных прибылей. Это явилось результатом первого этапа глобальной цифровизации, который можно определить как период анализа и использования большого количества данных преимущественно в потребительском сегменте Сети.

Теперь, с ростом цифровой экономики, на повестке дня встает вопрос повышения качества данных и их применения как в потребительском сегменте, так и в производственном сегменте Сети. Это «интернет вещей» для систем управления производством, энергетикой и

транспортом, сельским хозяйством, системами социального обеспечения и т. д. Здесь данные генерируются и фиксируются в ходе маркировки товаров для логистики, при создании «цифровых двойников» предприятий, формировании цифровых профилей населения и т. д. По сути, речь идет об обеспечении информационно-цифрового суверенитета страны. Все это требует как корректировки законодательства в информационной сфере и развития информационной инфраструктуры, так и соответствующей подготовки кадров предприятий и организаций, роста цифровой культуры подготовки данных и их защиты и применения, изменения бизнес-моделей производства и схем организационного управления.

Более того, анализ признаков качественного перехода в использовании первичных данных и роста их значения в период глобальной цифровизации приводит нас к выводу, что «новой нефтью» для экономики во все времена являются люди, обладающие знаниями и умениями применять новые технологии для достижения целей предприятия, отрасли, страны в целом и личностного становления и роста.

■ Цифровой суверенитет страны: как это понимать?

Ключевая идея цифрового суверенитета как информационного состоит в том, что страна должна иметь суверенитет над

всеми информационными потоками и цифровыми данными, которые генерируются, хранятся и обрабатываются на ее территории. Это может использоваться как в одностороннем порядке, так и в рамках межгосударственных и международных отношений.

Важно также отметить, что понятие цифрового суверенитета базируется на достаточно глубоко проработанной концепции информационного суверенитета как права государства самостоятельно формировать информационную политику, распоряжаться информационными потоками, обеспечивать информационную безопасность независимо от внешнего влияния. На это постоянно обращает внимание А. Г. Лукашенко, выступая с инициативой формирования «Пояса цифрового добрососедства». На решение этих задач направлена принятая Правительством Концепция информационной безопасности страны. Для достижения этих целей Беларусь стремится использовать возможности международных организаций и форумов (в сентябре 2019 года Беларусь выступила в ООН с идеей обеспечения цифрового суверенитета и нейтралитета стран).

Впервые понятие цифровой суверенитет возникло в начале 2011 года, когда генеральный директор французской радиостанции Skyrock Пьер Белланжер определил «цифровой суверенитет» как контроль над нашим настоящим и судьбой,

Информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

проявляемый и управляемый с использованием технологий и компьютерных сетей [1]. В отчете Сената Франции о цифровом суверенитете, опубликованном в 2019 году, цифровой суверенитет определяется как способность государства действовать в киберпространстве, что рассматривается как необходимое условие защиты национальных ценностей, требующее как способности выносить независимые государственные суждения, так и государственные решения в киберпространстве и осуществлять контроль над отечественными сетями, электронными коммуникациями и данными.

Иными словами, цифровой суверенитет не ограничивается контролем государства над информационными потоками и проектированием и использованием важнейших цифровых систем (критической инфраструктуры), а означает более широкий контекст реализации государственного права, как в политике информационной безопасности, так и в экономике и социальной сфере путем осуществления контроля над основными цифровыми экосистемами на территории страны.

В мировой практике одним из часто упоминаемых примеров действующего принципа цифрового суверенитета является Европейский общий регламент по защите данных (GDPR), который устанавливает ключевые требования к обработке данных, касающихся физических и юридических лиц в Европейском союзе.

■ Новые реалии и проблемы

С ростом конкуренции на мировых рынках приходит осознание того, что концепция интернета как абсолютно свободного информационного пространства претерпевает кардинальные

изменения. Все большее количество стран разрабатывает и применяет меры по его регулированию.

Одна из самых больших проблем, связанных с цифровым суверенитетом, заключается в том, что в настоящее время всего несколько крупных технологических компаний контролирует огромные объемы данных о своих пользователях. В ходе формирования потребительского сегмента цифровой экономики возникли ИТ-гиганты с юрисдикцией в США. В результате свыше 90 % данных, сгенерированных в странах ЕС и других европейских странах, размещается в США, что автоматически превращает глобальные ИТ-корпорации в новые центры силы, которые, в значительной степени неподотчетны национальным правительствам.

Основные причины, по которым цифровой суверенитет государств находится под давлением глобальных компаний, можно охарактеризовать следующим образом:

- растущая зависимость государственных органов и поставщиков критически важной цифровой инфраструктуры от ограниченного числа доминирующих игроков на мировых рынках информационных услуг;

- возрастающие киберугрозы для критически важной инфраструктуры, включая систематическое хищение интеллектуальной собственности из наукоемких секторов промышленности, цифровое мошенничество и прямое вымогательство денежных средств у населения и предприятий, целенаправленную дезинформацию и систематическое проникновение в социальные сети с целью влияния на выборы и социальные процессы;

- растущая геополитическая напряженность, ведущая

к экстерриториальным притязаниям иностранных держав по самым различным направлениям.

Поэтому, если ранее стремление к цифровому суверенитету состояло в том, чтобы предоставить предприятиям и органам гоуправления удаленно доступную и безопасную вычислительную инфраструктуру, способную размещать различные данные и приложения, то в новых реалиях для снижения уровня экономического влияния GAFA на экономику и общество потребовались выработка и применение инструментов государственного контроля и регулирования национального онлайн-пространства.

Предлагаемые средства для достижения такого суверенитета в цифровой сфере включают как экономические стимулы для разработки удобных для пользователей отечественных платформ и приложений, так и внедрение технологий, позволяющих обеспечить эффективное шифрование, защиту данных и большую прозрачность бизнес-моделей использования данных пользователей. При этом подавляющее большинство мер, направленных на обеспечение информационно-цифрового суверенитета, состоит как в повышении медийной и цифровой грамотности пользователей Сети, так и в укреплении компетенций и доверия пользователей и потребителей в ходе их взаимодействий в цифровой сфере.

■ Структура цифрового суверенитета

В документах Европейской комиссии определены три основные области цифрового суверенитета:

- вычислительная мощность,
- контроль европейцев над своими данными,
- безопасное соединение.

Более полно структуру и содержание цифрового суверенитета можно рассмотреть с позиций современной концепции сетевой экономики, в которой исследователи выделяют следующие уровни экономических отношений [2]:

- наноэкономика – экономика физических лиц и семей (индивидуальная, или семейная экономика), которая выстраивается на личностных и межличностных отношениях, где имеет место многообразие экономических связей и формируются потребительские стоимости и спрос. Именно здесь формируются первичные данные о потребительском спросе, фиксируются оценки качества продукции (товаров и услуг) и потребительские предпочтения;

- микроэкономика (экономика предприятий всех форм собственности), в которой экономические отношения выстраиваются как на рыночных принципах спроса и предложения, так и в соответствии с государственными интересами и приоритетами. На этом уровне формируются первичные массивы данных реального сектора экономики в ходе цифровизации бизнес-моделей предприятий и их взаимодействия в стране и с зарубежными партнерами;

- мезоэкономика (экономика регионов и отраслей), где доминируют территориальные и отраслевые интересы проживающих и занятых в них людей и формируются данные предприятий и населения в привязке к определенной местности или отрасли, используемые для создания наиболее благоприятных условий реализации местных и отраслевых ресурсов (природных, технологических и человеческих);

- макроэкономика (экономика страны), выражающаяся в принципах, механизмах и

инструментах формирования и использования государственного бюджета, на основе которого достигаются многие социальные, экономические, общественные и политические цели. Здесь фиксируются и интегрируются стратегически важные данные о налогах, кредитах, инвестициях, ценах, научно-технических, торговых и иных отношениях, обеспечивающих необходимый уровень благосостояния общества и качество жизни человека. Защита и эффективное использование этих данных является ключевым фактором устойчивого социально-экономического развития страны;

- мегаэкономика (система вхождения экономики страны в мировое экономическое пространство и состояние самой мировой экономики). Здесь формируются информационные активы для взаимодействия, сотрудничества и интеграции национальных предприятий и их участия в мировом разделении труда путем фиксации данных о занятости, демографии, перетоках финансовых капиталов, миграционных процессах человеческого и интеллектуального капиталов и многое другое.

Соответственно этим уровням выстраиваются и уровни обеспечения цифрового суверенитета: защиты и использования персональных данных, защиты интересов предприятий и организаций через данные, которые являются их основным ресурсом и составляют основу их добавленной стоимости; обеспечения суверенитета государств и межгосударственных объединений.

При этом важно отметить, что целью цифрового суверенитета является не изоляция страны, а защита ее стратегических интересов, позволяющая стране развивать свои собственные цифровые возможности в достижении

целей устойчивого социально-экономического развития.

■ Заслон цифровой независимости. Мировой опыт

С точки зрения данных цифровой суверенитет предполагает, что персональные данные, которые собираются и обрабатываются разными компаниями в интернете с согласия пользователей или без него, должны храниться в стране, в которой человек проживает, и, следовательно, должны регулироваться законодательством страны, что позволяет людям контролировать свое присутствие и представительство в цифровом мире.

На индивидуальном уровне цифровой суверенитет связан с тем, что люди владеют своими данными и контролируют их использование. Так как эти данные часто собираются корпорациями и продаются с целью получения прибыли, то вопрос использования персональных данных раскрывает суть важности цифрового суверенитета.

С появлением феномена больших данных предприятия и организации начали пересматривать свои стратегии онлайн-взаимодействий с тем, чтобы спрогнозировать потребности потребителей в режиме реального времени и взаимодействовать с ними как можно более эффективно. Это означает, что стремление государств к цифровому суверенитету носит не только политический, но экономический характер как с точки зрения уплаты ИТ-гигантами налогов, антимонопольной практики, так и использования личных данных потребителей онлайн-услуг.

При этом важно учесть, что все большее количество инструментов государственного

регулируемая сосредоточено на цифровой торговле и потоках данных, доставляемых через цифровые сети. Как следствие, ЕС и ряд других стран все более ужесточают свою позицию в отношении гигантов интернета, заставляя компании GAFA играть по национальным правилам. Примерами могут служить: Закон об облачных технологиях, принятый в США в мае 2018 года, который обязывает американские технологические компании передавать свои данные по требованию правительству, независимо от того, где эти данные хранятся; принятие ЕС решения об уплате компанией Amazon налогов во всех странах, где у компании есть дочерние компании, тогда как ранее компания централизовала свои доходы в Люксембурге; меры, принимаемые Австралией и Канадой по принуждению компании Facebook к уплате налогов от доходов от рекламы в национальные бюджеты. И это давление начинает приносить результаты – ИТ-гиганты начинают не только делиться доходами, но принимают меры, чтобы соответствовать новым требованиям с точки зрения конфиденциальности, прозрачности, поддержки и безопасности обработки как личных, так и корпоративных данных.

Исходя из международного опыта, решения по обеспечению цифрового суверенитета данных могут включать в себя следующие меры:

- создание сети национальных отраслевых и межотраслевых центров обработки данных на принципах государственно-частного партнерства,
- создание межотраслевого фонда отечественного программного обеспечения,
- внедрение национальных регламентов электронной идентификации пользователей

интернета, товаров, услуг и транзакций и систем обеспечения информационной и кибербезопасности.

Таким образом, защита и правовой надзор за данными постепенно становятся ключевым фактором политики укрепления цифрового суверенитета, поскольку данные стали новым ликвидным товаром. А для производственных предприятий реального сектора работа с данными становится частью промышленной политики.

Общая основа для превращения суверенитета данных в реальность обеспечивается распределенной информационной и программной инфраструктурой, на основе которой предприятия и население могут обмениваться данными и использовать их в безопасной и надежной среде, при этом владелец данных всегда сохраняет контроль над своими данными.

■ Противоречия в реализации принципов

Обеспечение цифрового суверенитета страны представляет собой достаточно трудную задачу вследствие необходимости разрешения ряда ключевых противоречий в использовании возможностей Сети и цифровых технологий, таких как:

- требования безопасности для государств и предприятий не должны преобладать над правами защиты личных данных,
- стремление к защите национального информационного и киберпространства противоречит целям международного сотрудничества, например, в борьбе с киберпреступностью,
- защита данных предприятий противоречит задачам создания, поддержания

и сохранения открытой и совместно используемой информационно-цифровой среды для развития и расширения коммерческой деятельности и внедрению инноваций,

- принципы территориальности и государственной иерархии вступают в противоречие с целесообразностью формирования предприятиями и предпринимателями гибких цепочек создания добавленной стоимости посредством глобальных цифровых сетей.

- цифровой суверенитет затрагивает национальную безопасность государств – членом межгосударственных объединений, которая является прерогативой государств.

Разрешение этих противоречий потребует времени и многих усилий государства в обеспечении рационального сочетания приоритета национальных интересов с эффективным использованием возможностей всестороннего взаимодействия и сотрудничества предприятий и населения в мировом информационно-цифровом пространстве.

■ Цель – справедливость

Концепция цифрового суверенитета продолжит приобретать все большее политическое и экономическое значение как в настоящее время, так и в долгосрочной перспективе. Все более широкое распространение и «включенность» в повседневную жизнь цифровых технологий, от искусственного интеллекта и до технологий больших данных и «интернета вещей», затрагивает не только вопросы интернет-коммуникаций и подключений, но и гораздо более широкий контекст цифровой трансформации экономики и общества.



Задача цифрового суверенитета состоит в контроле государства над формированием упорядоченной, ориентированной на национальные ценности, регулируемой и, следовательно, разумной и безопасной информационно-цифровой среды для социального сотрудничества и обеспечения справедливой экономической конкуренции отечественных и зарубежных компаний и предприятий.

Цифровой суверенитет государства реализуется путем обеспечения соблюдения национального законодательства в информационно-цифровой среде на территории государства.

Одновременно государство стремится формировать единые и гармонизированные информационно-цифровые рынки и правила, способствующие распространению инноваций и укреплению правовой определенности взаимодействий в цифровой среде для всех участников. В том числе правила ответственного применения данных при их совместном использовании и обмене между различными сторонами. Для этого важно сосредоточиться на суверенитете данных и критической информационной и программной инфраструктуре.

Цель состоит в том, чтобы государство могло гарантировать, что услуги зарубежных и транснациональных компаний могут использоваться в интересах социального и экономического развития государства с одновременной защитой национальных интересов, ценностей и приоритетов в условиях глобальной цифровизации экономики и общества. В том числе и путем развития механизмов укрепления доверия и взаимовыгодного многостороннего межгосударственного и международного сотрудничества в информационно-цифровой среде.

ЛИТЕРАТУРА

1. Bellanger P (2012). De la souveraineté numérique. Le Débat 170 (3): 149–159.
2. Гусаков, В. Г. Основы системной экономики / В. Г. Гусаков // Докл. Нац. акад. наук Беларуси. – 2018. – Т. 62. – № 4. – С. 488–494.
3. Интернет-источники.