DOI 10.37882/2223-2966.2025.11.34

ЭВОЛЮЦИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОБЛАЧНЫХ СТРАТЕГИЙ

THE EVOLUTION OF DIGITAL SOVEREIGNTY IN PUBLIC GOVERNANCE: A COMPARATIVE ANALYSIS OF CLOUD STRATEGIES

I. Superekin
M. Osorkina

Summary. The article examines the evolution and diversification of governmental cloud strategies through the lens of digital sovereignty as a key priority of contemporary public policy. Using the examples of the United States of America, Italy, Singapore, and the United Arab Emirates, the study identifies a shift from the early «Cloud First» paradigm toward more mature hybrid, multi-cloud, and sovereign architectures. The analysis demonstrates that digital sovereignty possesses a multidimensional nature — legal, institutional, technological, and human. A comparative assessment of the four cases reveals that federal states tend to adopt decentralized, multi-cloud models that enhance flexibility and risk diversification, whereas unitary systems favor the development of centralized sovereign platforms. The findings indicate that there is no universal model of digital sovereignty; its configuration depends on the form of government, the level of institutional digital maturity, and priorities of security and cost optimization. As a persistent trend, the paper highlights the «Cloud Smart + Cloud Native» nexus, which ensures data portability across cloud environments, enables managed security, and reduces dependence on a single provider. The research contributes to understanding how national governments approach cloud transformation amid increasing geopolitical and digital fragmentation.

Keywords: digital sovereignty, governmental cloud strategies, sovereign cloud, digital transformation, public sector governance.

Суперекин Игорь Юрьевич
Руководитель направления по стратегическому развитию ООО «Единая цифровая платформа», г. Москва
Igor.superekin@yandex.ru
Осоркина Маргарита Александровна
Главный специалист по стратегическому развитию ООО «Единая цифровая платформа», г. Москва
margo21@yandex.ru

Аннотация. Статья исследует эволюцию и диверсификацию государственных облачных стратегий сквозь призму формирования цифрового суверенитета как ключевого приоритета современной государственной политики на примере Соединенных Штатов Америки, Италии, Сингапура и Объединенных Арабских Эмиратов, фиксируя сдвиг от облачной стратегии «Cloud First» к более зрелым гибридным, мультиоблачным и суверенным архитектурам. Показано, что цифровой суверенитет имеет многомерную природу — правовую, институциональную, технологическую и кадровую. На примере сопоставления четырех стран отмечается, что федеративные государства склонны к децентрализации и использованию мультиоблачных решений, обеспечивающих гибкость и диверсификацию рисков, тогда как унитарное государственное устройство предполагает развитие централизованных суверенных платформ. Методологически работа опирается на сравнительный и аналитический подходы с использованием официальных документов и современной научной литературы. Сделан вывод, что универсальной модели цифрового суверенитета не существует; выбор конфигурации определяется формой государственного устройства, уровнем цифровой зрелости институтов и приоритетами безопасности и стоимости. В качестве устойчивого тренда выделяется связка «Cloud Smart + Cloud Native», обеспечивающая переносимость данных в облачную среду, управляемую безопасность и снижение зависимости от одного поставщика. Статья позволяет оценить различные государственные подходы к облачной трансформации в контексте растущей геополитической и цифровой фрагментации.

Ключевые слова: цифровой суверенитет, государственные облачные стратегии, суверенные облака, цифровая трансформация, государственное управление.

Введение

Развитие цифровых сервисов вынуждает государства ускоренно модернизировать ИТ-инфраструктуру. International Data Corporation (IDC)[1] и ряд других источников [2], прогнозируют, что объём ежегодно генерируемых глобальных цифровых данных вырастет до 175 зеттабайт в 2025 году, что соответствует среднегодовому темпу роста около 27–30 %. Такой рост цифрового трафика, объёмов хранения данных, числа подключённых устройств и облачных сервисов оказывает беспрецедентное давление на государственные и корпоративные ИТ-системы, требуя масштабируемых и устойчивых архитектур.

В 2011 году в США в рамках Federal Cloud Computing Policy была представлена политика Cloud First. Предпосылками её появления являлись: низкий уровень

использования государственных ИТ-активов, фрагментарный спрос на ресурсы, дублирующие друг друга ИТ-системы, а также длительные сроки закупок, что в итоге в комплексе негативно влияло на способность Правительства США эффективно выполнять свои функции [3]. Таким образом, первые облачные решения ориентировались на скорость миграции, зачастую игнорируя риски зависимости от поставщиков облачных решений (vendor lock in), юрисдикции переносимых в облачные инфраструктуры данных и устойчивости операций в облачной среде. После проведения массовой миграции сервисов и внедрения облачно-ориентированных подходов, акцент от перехода в облачную инфраструктуру сместился к защите данных и ценовой политике. В статье рассматривается переход от модели Cloud First к моделям Cloud Smart и «суверенных облаков» как способ нивелирования перечисленных выше рисков.

Несмотря на активное внедрение облачных технологий в государственном секторе, на сегодняшний день не найдена единая устойчивая и универсальная модель, эффективно сочетающая цифровую эффективность, безопасность и государственный суверенитет. Разные страны выбирают разные траектории — от децентрализованной мультиоблачной архитектуры до централизованного подхода с государственным контролем. Такая фрагментарность и разнообразие стратегий в сфере цифрового управления требует теоретического осмысления, сравнительного анализа и выявления основных факторов выбора определенной модели.

Цели и задачи исследования

Целью исследования является проведение анализа эволюции облачных стратегий в государственном секторе в контексте возрастающей значимости цифрового суверенитета и выявление ключевых типологических моделей, формирующихся в различных странах. В качестве эмпирической базы рассматриваются кейсы США, Италии, Сингапура и ОАЭ с различными геополитическими, экономическими и регуляторными условиями.

Задачами исследования являются:

1. Оценка концепции цифрового суверенитета с идеологической, институциональной и технологической точек зрения.
2. Анализ роли гибридных, мультиоблачных и суверенных моделей в формировании государственной цифровой инфраструктуры и их вклад в достижение цифрового суверенитета страны.
3. Проведение системного сравнительного анализа подходов к облачной трансформации и реализации цифрового суверенитета в выбранных странах, выявляя сходства, различия и определяющие факторы, включая форму государственного устройства.

Концептуальные рамки и Методология

1. Цифровой суверенитет как многомерное явление

Цифровой суверенитет представляет собой не только нормативную позицию о контроле над данными, но и стратегическую реакцию государств на вызовы глобализации. Как политика, он включает разработку нормативно-правовых актов, регулирующих хранение, передачу и обработку данных в рамках национальной юрисдикции.

Научная литература подчёркивает неоднозначный характер цифрового суверенитета как концепции. В статье «Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace» (Digital Society, 2025) [4] отмечается трансформация понятия суверенитета в условиях киберпространства. Авторы показывают, что государства стремятся формализовать контроль над цифровой инфраструктурой через юридические, технические и территориальные механизмы, тем самым адаптируя классическое понимание юрисдикции к глобальной цифровой среде. К числу юридических инструментов относятся нормативные инициативы Европейского союза, такие как General Data Protection Regulation (GDPR), Data Governance Act (2022) и Data Act (2023), в качестве технических механизмов анализируются китайская система обязательной идентификации пользователей (real-name registration), а также проекты по созданию национальных дата-центров и облачных сервисов. Территориальные механизмы проявляются в стремлении государств контролировать критическую инфраструктуру, включая подводные кабели, в политике локализации хранения данных и в формировании обособленных цифровых сегментов.

Современные трактовки цифрового суверенитета выходят за пределы юридического обладания данными. В статье «Data Sovereignty in Information Systems» (Electronic Markets, 2024) [5] под данным понятием понимается способность субъектов — включая государства — самостоятельно устанавливать правила хранения и передачи данных, а также управлять правами на цифровые ресурсы. Речь идёт не только о защите или локализации информации, но и о создании системной архитектуры управления, в рамках которой операторы цифровых сервисов обязаны действовать в соответствии с политическими и правовыми нормами конкретной юрисдикции.

Дополнительный контекст даёт анализ стран БРИКС (2024) [6], согласно которому контроль над трансграничной передачей, хранением и использованием данных стал ключевым элементом цифровой трансформации. В этой модели цифровой суверенитет — не только защита от внешних угроз, но и формирование автономной

инфраструктуры и правил обработки информации, соответствующих национальным интересам. Важным аспектом цифрового суверенитета становится не только и не столько контроль над данными, но и развитие собственной ИТ-экосистемы.

Важным аспектом цифрового суверенитета является развитие собственной ИТ-инфраструктуры, включая локальные дата-центры. Авторы подчеркивают, что устойчивое управление данными в условиях цифрового суверенитета требует локализованных облачных платформ и совместимых архитектур, подкреплённых национальными компетенциями в сфере администрирования, безопасности и разработки. Без наличия кадрового ресурса и физической инфраструктуры, обладающей гарантированной территориальной юрисдикцией, цифровая автономия государств остаётся формальной (Galij et al., 2024) [7]. Обзор «Developing Skills for Digital Government» (OECD, 2024) подтверждает, что успешная цифровая трансформация и автономность цифровых сервисов невозможны без системного подхода к развитию компетенций в государственном секторе: облачные технологии, кибербезопасность и управление данными должны быть включены в образовательные программы для госслужащих и технических кадров [8].

Соответственно, цифровой суверенитет формируется через комплексный подход, объединяющий развитие инфраструктуры с целенаправленной кадровой политикой, ориентированной на подготовку специалистов, способных управлять критичной цифровой средой независимо от внешних поставщиков.

Политическая реализация цифрового суверенитета существенно различается между странами в зависимости от формы государственного устройства, которая предопределяет институциональные и инфраструктурные стратегии в сфере облачных технологий, контроля над данными и цифровой трансформации.

США как федерация демонстрируют модель, при которой суверенитет рассматривается как функция рыночной конкурентоспособности и агентской автономии. Исследователи из Brookings Institution подчёркивают, что американский подход способствует инновациям частного сектора, используя экспортные ограничения и развитие национальных цепочек поставок, а не централизованный контроль данных [9].

В Европейском Союзе как надгосударственном образовании цифровой суверенитет трактуется как средство защиты прав человека, конфиденциальности и цифрового гражданства. Исследование «Contested Spatialities of Digital Sovereignty» подчёркивает, что инициативы Gaia-X и политик Европейского совета создают инфраструктуру, обеспечивающую «технологическую автономию», при этом балансируя интересы государств-членов [10]

В странах Персидского залива (смешанная модель, с элементами как федерализма, так и унитаризма) суверенитет представляет собой инструмент контроля национальной безопасности и развития кадрового потенциала внутри страны.

Анализ ECFR указывает, что централизованные цифровые платформы и жесткое государственное регулирование — модели, сочетающие элементы федерализма (например, в ОАЭ) с авторитарным управлением [11].

Таким образом, цифровой суверенитет представляет собой многомерное явление, формирующееся на пересечении политических решений, экономических интересов, технологических возможностей и общественных представлений о контроле над данными. Его реализация опирается как на инфраструктурные компоненты (например, облачные платформы и дата-центры), так и на институциональные механизмы (нормативное регулирование, стратегическое планирование), а также на ориентиры, определяющие, какие цифровые ресурсы считаются критически важными для государства и общества.

Дополнительно, форма государственного устройства влияет на конфигурацию цифровой политики и степень распределения ответственности за управление данными и инфраструктурой.

2. Ключевые облачные модели и типы облачной архитектуры.

2.1. Стратегия Cloud First Стратегия Cloud First была официально объявлена в США как часть плана реформирования федеральной ИТ-сферы. 9 декабря 2010 г. главный федеральный CIO США Вивек Кундра опубликовал 25-пунктный план «A 25-Point Implementation Plan to Reform Federal IT Management» [12], где впервые был предложен перенос приложений и данных в облачные инфраструктуры: «Каждое агентство должно внедрять облачные решения, если они надёжные, безопасные и экономически эффективные».

8 февраля 2011 года, Административно-бюджетное управление США выпустило «Federal Cloud Computing Strategy», закрепляющую стратегию Cloud First как обязательную политику при планировании и приобретении ИТ-услуг федеральными агентствами [3]. Однако, исследования показывают, что правительственные инициативы Cloud First, хотя и стимулировали быстрый переход к облачным решениям, столкнулись с рядом сложностей:

— Vendor lock-in и технологическая замкнутость — Khajeh-Hosseini и соавт. (2010) в работе The Cloud Adoption Toolkit указывают, что миграция в публичное облако усиливает зависимость от конкретного провайдера, особенно в условиях отсутствия единых стандартов API и переносимых

архитектур. Это осложняет возврат к альтернативным системам или переход к другой облачной платформе без существенных затрат и технических рисков [13].

— Legacy-системы и институциональная неподготовленность — Fahmideh et al. (2020) выявили, что ключевым барьером при реализации облачных стратегий является неподготовленность устаревших систем (legacy software) и ограниченность компетенций ИТ-персонала. Даже при наличии политической воли, техническая и организационная среда не всегда позволяет реализовать миграцию эффективно и безопасно [14].
— Восприятие рисков в государственном секторе — Elena & Johnson (2015), исследуя стратегию Cloud First в контексте Великобритании, показывают, что восприятие рисков безопасности и приватности может снижать готовность к миграции в 26 раз. Это особенно характерно для министерств и ведомств, работающих с персональными и чувствительными данными. Несмотря на внедрение стратегии Cloud First в Великобритании в 2013 году в рамках программы G-Cloud, реальные темпы миграции зависели от культурной и институциональной восприимчивости к цифровым рискам [15].

2.2. Стратегия Cloud Smart

В итоге все эти аспекты привели к пересмотру стратегии Cloud First и ее последующей эволюции в стратегию Cloud Smart, которая предполагает более взвешенный подход к выбору облачных решений, учитывающий безопасность, стоимость, эффективность и соответствие регуляторным требованиям.

В 2018 году была опубликована обновленная федеральная стратегия облачных вычислений Federal Cloud Computing Strategy [16]. Стратегия Cloud Smart подчёркивала, что государственные органы должны оценивать не только технические и финансовые аспекты миграции сервисов и приложений в облачную среду, но и влияние облачных решений на конечных пользователей. Этот подход отражён в докладе Административно-бюджетного управления США (2018), где подчёркивается необходимость «информационно обоснованного принятия решений, в которых госорганы оценивают затраты и выгоды в свете миссии, пользователя и риска».

Кроме того, отличием Cloud Smart от Cloud First стала гибкость принимаемых решений: госорганы получили больше автономии в решении, какие приложения переводить в облако, а какие оставить в локальной инфраструктуре, исходя из своих целей, миссии и технической готовности.

2.3. Мультиоблачная архитектура

Стратегия Cloud Smart заложила мультиоблачный подход к получению облачных услуг с возможностью вовлечения множества поставщиков услуг. Согласно исследованию в «Journal of Cloud Computing & e-Government» (2025) [17], правительства демонстрируют наиболее устойчивые и масштабные модели миграции в облако именно тогда, когда переход сопровождается институциональными механизмами, включая стандарты, сертификацию и обучение кадров, что подтверждает, что зрелая стратегия обеспечивает не просто перенос в облако, а формирование цифровой зрелости на уровне государственной ИТ-инфраструктуры.

Мультиоблачная архитектура (multi-cloud) представляет собой модель, при которой организация использует услуги более чем одного облачного провайдера (обычно публичных), распределяя рабочие нагрузки между различными платформами в зависимости от функциональных, экономических и регуляторных требований. Такая стратегия не обязательно включает локальные инфраструктуры, а сосредоточено на диверсификации поставщиков облачных услуг. Согласно исследованию Saxena et al. (2021) [18], мультиоблачная модель позволяет избежать зависимости от одного поставщика (vendor lock-in), повысить отказоустойчивость и гибкость размещения сервисов с учётом требований локализации данных и законодательных ограничений в различных юрисдикциях. Мультиоблако также обеспечивает возможность оптимизации затрат за счёт выбора наиболее выгодных сервисов у разных провайдеров (Saxena et al., 2021) [18]. Также исследования показывают, что мультиоблачные конфигурации требуют довольно высокого уровня зрелости ИТ-управления: от архитектурного моделирования до внедрения механизмов мониторинга, идентификации угроз и реализации стандартов, таких как zero-trust и автоматизированные CI/CD процессы (Polinati, 2025) [19] .

Мультиоблачные стратегии становятся всё более значимыми в государственных информационных системах, особенно в контексте цифрового суверенитета, распределения рисков и соответствия международным регуляциям. Их применение требует зрелой ИТ-инфраструктуры, развитых механизмов управления и унификации стандартов безопасности.

2.4. Гибридная архитектура

Гибридная архитектура — это комбинация публичных и частных облаков с возможностью избирательного размещения сервисов в зависимости от уровня чувствительности данных. Преимуществами гибридной архитектуры являются гибкость и снижение издержек (Polinati, 2025) [19]; обеспечение безопасности за счёт

локального контроля над критичной информацией (Khadilkar et al., 2011) [20]; архитектурную совместимость (Venkateswaran & Sarkar, 2018)[21].

Гибридное облако позволяет использовать ресурсы публичного облака для масштабируемости и инноваций, сохраняя при этом суверенитет и соответствие регуляторным требованиям.

2.5. Суверенная архитектура

Суверенное облако — специальная облачная платформа, разработанная для обеспечения полного контроля над инфраструктурой, операциями и данными в рамках конкретной юрисдикции, что позволяет государству сохранять суверенитет над критически важной цифровой средой.

Основные преимущества:
- — Юридический контроль. Суверенные облачные решения разворачиваются на территории государства и подпадают под действие его законов, что устраняет риск экстерриториальных претензий (например, по CLOUD Act США).
- — Повышенная безопасность. Архитектура таких облаков часто включает механизмы zero-trust, шифрование, ключи, хранящиеся на территории государства, и участие в эксплуатации только аккредитованных сотрудников-граждан.
- — Соответствие регуляторным требованиям. Суверенные облака позволяют соответствовать локальным законам о защите персональных данных (таких, как например, General Data Protection Regulation, включая обязательства по локализации и защите критической инфраструктуры.
- — Интеграция в мульти- и гибридную экосистему. Суверенные облака выступают как надежная база для размещения чувствительных сервисов, интегрируясь с публичными облаками для масштабируемых нагрузок, что делает их важной частью зрелых архитектурных стратегий (мульти+гибрид).

В то же время всё чаще используется концепция «суверенитета как сервиса» (*sovereignty-as-a-service*), активно продвигаемая глобальными облачными провайдерами и представляющая цифровую независимость в форме внешних технологических решений. Grohmann и Barbosa (2025) [22] отмечают, что технологические гиганты, такие как Amazon, Microsoft и Google, предлагают «суверенитет как сервис», позиционируя свои облачные решения как инструменты для достижения цифрового суверенитета государствами. Однако, по мнению авторов, эта концепция представляет собой коммерческую стратегию, которая может создавать иллюзию контроля при фактической зависимости государства от внешней инфраструктуры и сервисов.

В отличие от предложения облачных провайдеров, национальные стратегии цифрового суверенитета ориентируются на реальный контроль, институционализацию и автономное управление инфраструктурой. Суверенные облака обеспечивают контроль на архитектурном, правовом и операционном уровнях, снижая зависимость от внешних платформенных решений и укрепляя долгосрочную цифровую устойчивость государства.

Исследование «Government Cloud Computing and National Data Sovereignty» (Irion K., 2012) подчёркивает факт, что государства не могут полагаться на технологии или договоры для защиты государственных данных, им нужны суверенные облачные стратегии [23] и инфраструктуры, разработанные с учетом национального суверенитета, обеспечивающие контроль над цифровыми активами[24].

2.6. Использование подхода Cloud native при разработке приложений.

Согласно прогнозу IDC FutureScape: Worldwide Cloud 2024 Predictions — Asia/Pacific (Excluding Japan) (IDC, 2023), в Азиатско-Тихоокеанском регионе наблюдается устойчивый сдвиг в сторону cloud-native архитектуры и интеграции искусственного интеллекта в процессы обеспечения безопасности. По оценке IDC, к 2025 году около 50 % организаций региона сформируют стратегические партнёрства с облачными провайдерами, что позволит ускорить внедрение решений на базе cloud-native-технологий, включая платформы для генеративного искусственного интеллекта, инструменты для разработчиков и инфраструктурные сервисы [25]. Аналитики Gartner (2023) выносят в топ государственных трендов облачную модернизацию устаревших систем и «суверенные облака», что подтверждает движение к cloud-native архитектурам в госуправлении [26].

Таким образом, подход «Cloud Smart + Cloud Native» обеспечивает долгосрочную устойчивость, снижает зависимость от одного поставщика и становится технологической основой для мультиоблачности и цифрового суверенитета.

3. Материалы и методы исследования

Материалами для исследования послужили официальные государственные документы (стратегии, национальные программы развития облачных вычислений, нормативно-правовые акты), аналитические отчеты ведущих консалтинговых компаний: «Gartner», «IDC» и другие. Также использована информация из современных научных статей, монографий и публикаций профильных сайтов. При описании моделей цифрового суверенитета и облачных вычислений в выбранных странах применены сравнительный и аналитический методы.

Для качественного сравнительного анализа выбраны США, Италия, Сингапур и ОАЭ — страны, являющиеся примерами разных политических, институциональных, экономических и географических условий, оказывающих непосредственное влияние на стратегии облачных решений и цифрового суверенитета.

Соединённые Штаты Америки были первой страной, системно внедрившей государственную стратегию облачной трансформации [3,16]. Благодаря своему экономическому и научному потенциалу, технологической инфраструктуре, США выступают не столько как потребитель, сколько, как экспортер облачных стандартов.

Академический обзор Columbia Law Review [27] подчёркивает, что облачные архитектуры, созданные на территории США, становятся основой юридической юрисдикции и цифрового контроля, включая механизм CLOUD Act.

Это делает США репрезентативным примером не только с точки зрения технологической инициативы, но и юридического воздействия на архитектуру глобальных облаков, что принципиально для целей настоящего сравнительного анализа.

Выбор Италии для анализа обусловлен ее членством в ЕС, реализацией Strategia Cloud Italia и National Strategic Hub и встраиванием интересов национального суверенитета в рамки наднационального GDPR/GAIA-X.

В европейском контексте цифровой суверенитет рассматривается и как способ объединить инновации с контролем отмечается при анализе облачных инициатив ЕС с цифровым суверенитетом [28].

Сингапур представляет собой унитарное технократическое государство, реализующее программу «Smart Nation» с 2014 г., проводящее активную политику переноса систем государственного управления в облачную среду и управлением идентификацией граждан посредством единого SingPass.

В статье Cloud Computing in Singapore [29] указаны пять ключевых драйверов цифровизации госучреждений Сингапура, включая стратегическое реформирование агентств и создание платформ национального уровня.

ОАЭ — единственная в данном перечне федеративная монархия с суверенной облачной платформой FedNet.

Источники указывают на активную роль государства в разработке суверенных облаков как ключевого инструмента национальной безопасности.

В заключении можно отметить, что выбранные для анализа страны обеспечивают не только разнообразие институциональных моделей: от федерации до централизованной монархии и стратегий облачных решений, но и баланс между инновациями, юрисдикцией и безопасностью, необходимый для качественного анализа цифрового суверенитета и облачной зрелости.

4. Тренды

4.1. Суверенизация данных

Суверенизация данных — это институционально оформленный процесс, в рамках которого государства стремятся установить полный контроль над данными, находящимися в пределах их юрисдикции. Включает два ключевых направления:

- Строительство национальных дата-центров — физическая локализация хранения и обработки данных на территории государства.
- Создание локальных технических команд и подразделений, обеспечивающих эксплуатацию в соответствии с национальными требованиями.

Исследования подтверждают, что такие меры являются не просто регуляторными, но и стратегически оправданными, направленными на укрепление технологической автономии и устойчивости к внешним рискам:

В публикации «"Data localization": The internet in the balance» (Taylor, Telecommunications Policy, 2020) подчёркивается глобальный тренд к обязательной локализации данных, мотивированный соображениями национальной безопасности и цифрового суверенитета, особенно в отношении критичной инфраструктуры [30].

Fratini (2024) в статье «Data localization as contested and narrated security in the age of digital sovereignity» показывают на примере Швейцарии, что локализация данных рассматривается как комплекс технологических и институциональных мер, формирующий цифровую автономию через контроль над данными и национальными сегментами сети. [31].

Таким образом, суверенизация данных является системным компонентом государственной цифровой политики, направленным на снижение зависимости от иностранных поставщиков, создание инфраструктурной и кадровой устойчивости, а также укрепление общественного доверия через визуализацию контроля над цифровыми границами.

4.2. Перевод в облако вычислений и хранения данных

Переход вычислительных ресурсов и систем хранения данных в облачные инфраструктуры остаётся ключевым направлением цифровой трансформации.

В последние годы наблюдается значительный рост облачной инфраструктуры: компании активно переходят от локальных ИТ-решений к облачным платформам. Согласно данным отчёта SQ Magazine Cloud Adoption Statistics (2025) [32], более 80 % компаний среднего бизнеса перенесли более половины рабочих нагрузок в облачную среду. всех корпоративных рабочих нагрузок, более 90 % предприятий в 2025 году будут использовать облачные сервисы, что подтверждает устойчивую тенденцию к доминированию облачных архитектур в корпоративных ИТ-системах. Этот показатель отражает общий вектор цифровой трансформации — переход от капиталоёмких дата-центров к гибким облачным моделям обслуживания. Наряду с этим развиваются ключевые технологии, такие как искусственный интеллект, периферийные вычисления, которые становятся неотъемлемой частью облачных платформ.

В условиях динамической масштабируемости облака позволяют обрабатывать огромные объёмы данных с минимальными задержками и высокой доступностью. При этом архитектуры, основанные на периферийных и бессерверных вычислениях, обеспечивают экономию затрат, ускоренное развёртывание сервисов и снижение необходимости в капитальных вложениях.

Основные выводы:

— ИТ-инфраструктуры переориентируются на модель, где облачные сервисы являются центром при разработке и масштабировании;
— Облачное хранение и вычисления становятся не опцией, а стратегическим выбором для реализации сложных задач;
— Использование современных подходов (бессерверные вычисления, автоматизация, zero-trust) обеспечивает устойчивость при росте нагрузки и требований;
— Таким образом, массовый переход на облачные вычисления и хранение — это не просто техническая переориентация, а институционально поддерживаемая стратегия, лежащая в основе цифровой зрелости организаций и государства.

4.3. Репатриация чувствительных данных и вычислений на приватные облака

Обязательное соблюдение требований законодательства по обработке данных (например, GDPR в ЕС) делает публичные инфраструктуры менее предпочтительными для регламентированных данных. Исследование Jewargi (2023), опубликованное в Scholars Journal of Engineering and Technology [33], указывает, что более 80 % организаций в США вернули некоторые нагрузочные задачи на собственную инфраструктуру для обеспечения безопасности и снижения рисков контроля данных.

Меры по репатриации, согласно Wu (2021) [34], являются важным элементом институционального контроля над цифровыми инфраструктурами, направленным на защиту национального суверенитета над данными . Fratini et al. (2024) [35] подтверждают, что контроль над инфраструктурой и юрисдикцией является ключевой составляющей цифрового суверенитета, причём репатриация данных выступает одним из ключевых инструментов этой стратегии .

5. Сравнительный анализ моделей цифрового суверенитета

5.1. США: федеративная модель облачных стратегий

США представляют собой федеративное государство с высоким уровнем децентрализации, где федеральные и региональные органы исполнительной власти обладают автономией в разработке и реализации ИТ-стратегий. Это обусловливает реализацию модели облачного управления, основанную не на централизованном внедрении, а на политике координирования, в рамках которой каждое агентство адаптирует облачные решения под свои цели.

Стратегия Cloud First (2010)[3] была разработана как мера ускоренного перехода к использованию публичных облаков, ориентированная на сокращение затрат и повышение эффективности. Однако, принимая во внимание все сложности, с которыми столкнулись органы власти при ее внедрении, описанные во введении к статье, стратегия эволюционировала в стратегию Cloud Smart с акцентом на оценку рисков кибербезопасности, соответствие требованиям регулятора и оптимизацию затрат и пользовательского опыта.

Согласно отчёту Конгресса США *Cloud Smart: Federal Cloud Computing Strategy* (CRS Report R46119, 2020), стратегия *Cloud Smart* была направлена на повышение эффективности и гибкости государственных ИТ-закупок, включая сокращение избыточных централизованных закупочных моделей и дублирующих расходов [36], благодаря использованию облачных сервисов федеральные агентства сэкономили почти 300 млн долларов. Нормативное регулирование обеспечивается посредством применения FedRAMP (Federal Risk and Authorization Management Program) [37], механизма стандартизированной оценки безопасности облачных сервисов для федеральных учреждений. Он обеспечивает соответствие NIST 800-53 и предоставляет единый каталог аккредитованных провайдеров и NIST Cloud Computing Standards [38], которые формируют технические рамки для идентификации облачных моделей и обеспечения совместимости, безопасности и управления доступом.

Эти инструменты позволяют сочетать открытость инфраструктурных решений с регламентированной безопасностью и управляемостью.

Несмотря на то, что США не декларируют цифровой суверенитет как отдельную политику на уровне государства, он де-факто реализуется через развитие специализированной инфраструктуры для предоставления услуг облачных вычислений для государственных органов (AmazonWeb Services GovCloud, Azure Government, Google Cloud for Gov); контроль над облачными технологиями и их экспортом через экстерриториальное правоприменение CLOUD Act[39]).

Таким образом, сочетание экономического лидерства, правовой экстерриториальности и технической стандартизации обеспечивает Соединённым Штатам Америки уникальное положение, где мы можем рассматривать облачные сервисы как инфраструктуру глобального технологического влияния.

5.2. Италия: европейская модель суверенного облака

Италия как член Европейского Союза реализует цифровой суверенитет в рамках общеевропейской нормативной архитектуры, включая применение Общего регламента защиты данных (General Data Protection Regulation) и требований GAIA-X. Национальная стратегия ориентирована на снижение зависимости от неевропейских поставщиков облачных решений, усиление институционального контроля и защиту цифровой инфраструктуры. По мнению Jean-Pierre Darnis (2018)[40], облачные архитектуры и технологические платформы всё чаще рассматриваются как новые границы государственного суверенитета, требующие политического и правового закрепления: «Нация должна учитывать технологические границы как часть суверенных интересов».

В 2021 году была утверждена Strategia Cloud Italia[41], предполагающая создание Polo Strategico Nazionale (NSH) — суверенного национального облака. Его цель — объединить критичные государственные сервисы в централизованной, управляемой на территории Италии облачной инфраструктуре, контролируемой государством.

Проект реализуется консорциумом компаний, среди которых TIM, Leonardo, Sogei и CDP Equity при координации Агентства цифровой Италии Департамента цифровой трансформации. Этот шаг рассматривается как попытка выстроить национальную облачную платформу, способную обеспечить независимость от крупных транснациональных поставщиков облачных решений.

Италия активно участвует в GAIA-X, инициативе Европейского Союза, направленной на создание федеративной, безопасной и открытой инфраструктуры данных для Европы. По данным Fratini et al. (2024) [35], такой подход представляет собой модель институционального цифрового суверенитета, при котором контроль над данными, инфраструктурой и политиками доступа осуществляется национальными органами: «Государственное управление инфраструктурой цифровых данных и потоков становится основой современного цифрового суверенитета».

Италия реализует цифровой суверенитет институциональными методами через Strategia Cloud Italia и инфраструктуру NSH, таким образом страна стремится обеспечить контроль над критичной облачной инфраструктурой, интегрируясь при этом в общую архитектуру европейского суверенного облака. Как отмечает Darnis (2018) [40], это отражает новое понимание границ суверенитета в цифровую эпоху, где контроль над технологической инфраструктурой приобретает статус стратегического ресурса.

5.3. Сингапур: централизованная модель облачной государственности

Сингапур является одним из мировых лидеров по уровню цифровизации государственного управления, занимая третье место среди 193 стран по индексу развития электронного правительства (UN E-Government Survey 2024 [42]). Его стратегия Smart Nation сочетает централизованные принципы технократии, цифровую идентификацию и массовое внедрение искусственного интеллекта.

В стратегии Smart Nation и ее отдельной программе Digital Government Blueprint [43], запущенной в 2018 году, одной из целей стал перенос к 2023 году 70 % отвечающих требованиям безопасности систем в коммерческую облачную среду, Government on Commercial Cloud (GCC), инфраструктуру для которой предоставляют крупнейшие провайдеры Amazon Web Service, Azure Microsoft, Google Cloud.

Reuben Ng (2018) [29] в работе Cloud Computing in Singapore: Key Drivers and Recommendations for a Smart Nation выделил пять ключевых драйверов облачной интеграции в Сингапуре в публичный сектор — от спроса на e-government до развития платформы Smart Nation. Он подчёркивает, что облако является не только технологической основой, но и структурным элементом государственной политики.

В целях соблюдения принципов цифрового суверенитета в Сингапуре ввёден национальный стандарт SS584 (MTCS), который устанавливает три уровня безопасности для облачных сервисов.

Этот стандарт обеспечивает соответствие требованиям безопасности и помогает государственным учреждениям выбирать подходящие облачные решения в зависимости от чувствительности данных, что повышает

доверие к облачным системам и представляет инфраструктуру как публичную, но под национальным управлением.

Таким образом, сингапурская модель демонстрирует, что централизованная технократия выстраивает облачную инфраструктуру, как систему государственного управления. Облачные платформы используются как:

— модуль для унификации государственной инфраструктуры;
— инструмент предоставления цифровых госуслуг (например, SingPass, health);
— единый подход к безопасности с проверенными локальными стандартами (MTCS).

Таким образом, облачные технологии в Сингапуре используются не просто как техническое решение, а как один из ключевых инструментов государственного управления. Через облачную инфраструктуру государство не только размещает цифровые сервисы, но и выстраивает централизованную систему принятия решений, контроля за данными и предоставления услуг гражданам. Облако становится частью политической и институциональной модели, в которой технологии напрямую поддерживают эффективность и управляемость государственного аппарата.

5.4. Объединённые Арабские Эмираты: федеративная модель облачного суверенитета

Облачная инфраструктура в ОАЭ развивается по федеративной модели, где существуют как федеральные облачные платформы (например, FedNet, развитие которой курирует Управление по регулированию телекоммуникаций и цифрового Правительства (TDRA)), так и облачные инициативы в отдельных эмиратах (например, Smart Dubai Government Cloud, Abu Dhabi Digital Authority).

В этом контексте Управление по регулированию телекоммуникаций и цифрового Правительства выступает как регулирующий и координирующий орган на федеральном уровне, отвечающий за:

— реализацию стратегии цифрового правительства;
— регуляцию телеком— и облачных услуг;
— разработку национальных стандартов безопасности;
— сертификацию облачных провайдеров в рамках IaaS и SaaS решений для государственных нужд.

FedNet — это государственная облачная платформа, предоставляющая сервисы IaaS для федеральных учреждений. Она является частью федерального уровня цифровой инфраструктуры, и не заменяет, а дополняет локальные инициативы эмиратов.

Исследование Baldoni & Di Luna (2025)[44] подчёркивает, что облачные платформы, контролируемые на национальном или квазигосударственном уровне, способствуют формированию устойчивого цифрового суверенитета.

Управление по регулированию телекоммуникаций и цифрового Правительства также играет ключевую роль в формализации стандартов безопасности (включая Information Assurance Regulation, IAR); внедрении требований по локализации и сертификации провайдеров облачных услуг. Ключевым вызовом для реализации цифрового суверенитета в ОАЭ является демографическая структура страны: граждане составляют менее 12 % населения, и в ИКТ-секторе их ещё меньше. Это приводит к зависимости от иностранной рабочей силы в управлении критической инфраструктурой, включая облачные платформы.

В ответ правительство реализует Emiratization Plan — стратегическую инициативу государственного стимулирования широкой интеграции граждан ОАЭ в высокотехнологичные отрасли. В контексте развития облачной инфраструктуры это означает:

— обязательства для поставщиков облачных услуг и операторов облачной инфраструктуры (федеральных и эмиратских) по набору и обучению эмиратских специалистов;
— локализацию ключевых компетенций — DevOps, сетевое администрирование, безопасность;
— создание Национального центра команд FedNet (Cloud Command Center), где работают граждане ОАЭ.

Эти меры являются стратегическим инструментом цифрового суверенитета, направленным на уменьшение технологической зависимости и создание кадровой базы под национальный контроль инфраструктуры.

В ОАЭ облачная инфраструктура развивается на уровне отдельных эмиратов, отражая федеративную модель цифрового управления. В частности, Дубай создало развитую экосистему на базе Smart Dubai Government Cloud и платформы Dubai Pulse, Абу-Даби в свою очередь реализует облачные инициативы через проекты Abu Dhabi Digital Authority (ADDA) и Core42.

Такой подход отражает федеративное устройство страны: создаётся многоуровневая система, где федеральные и региональные платформы сосуществуют и дополняют друг друга. Это позволяет гибко адаптировать цифровые стратегии под местные приоритеты, сохраняя при этом общенациональные стандарты управления и безопасности.

Все эти факторы позволяют говорить о федеративной архитектуре цифрового суверенитета с фокусом

Таблица 1.

Сравнительный анализ моделей цифрового суверенитета

Критерий/Страна	США	Италия	Сингапур	ОАЭ
Форма государственного устройства	Федерация	Унитарное государство в составе ЕС	Унитарное, технократическое	Федерация
Тип стратегии	Агентская автономия и рынок	Централизованная, институциализированная	Централизованная, технократическая	Координируемая федеративная
Облачная модель	Публичное/гибридное, GovCloud	Суверенное облако (NSH)	Государственный техстек (GovStack, Artificial Intelligence Government Cloud Cluster)	Суверенные платформы (FedNet + облачные сервисы эмиратов)
Регуляция данных	CLOUD Act, FedRAMP, NIST	GDPR, Strategia Cloud Italia	SS584 (MTCS)	IAR, TDRA, сертификация облачных провайдеров
Технологическая автономия	Высокая, доминирование транснациональных облачных провайдеров	Ограниченная	Средняя, приоритет локальных решений	Развивающаяся, с опорой на национальные платформы

на создание кадрового обеспечения для стратегической ИТ-отрасли страны, в которой облачные технологии служат как инструментом административной эффективности, так и политического контроля над данными.

Из отмеченного в данной статье можно сделать следующие выводы:

— США реализуют цифровой суверенитет через доминирование на глобальном рынке облаков, сочетая агентскую автономию с нормативной экстерриториальностью;
— Италия строит институциональную модель на базе инфраструктурного контроля и общеевропейских норм;
— Сингапур демонстрирует технократический подход, где государство — ведущий разработчик и интегратор цифровых сервисов;
— ОАЭ применяют федеративную стратегию с централизованными стандартами, фокусируясь на локализации данных, кадровом суверенитете и институциональной координации.

Политико-административное устройство государства оказывает непосредственное влияние на формирование стратегий цифровизации и архитектуру государственных технологических платформ. В централизованных унитарных государствах цифровая трансформация, как правило, реализуется в форме единых интегрированных платформ, управляемых централизованными агентствами (например, GovTech в Сингапуре). Это обеспечивает высокую степень унификации сервисов, стандартизацию данных и вертикальную координацию между уровнями власти. В федеративных системах (например, США или ОАЭ) цифровизация зачастую развивается по децентрализированной модели, где отдельные субъекты федерации (штаты, эмираты) обладают значительной автономией в выборе архитектур, поставщиков в рамках установленных законодательством требований. Это порождает систему, где сосуществуют различные цифровые решения при наличии координирующих структур на федеральном уровне.

Италия представляет собой интересный пример унитарного государства, встроенного в наднациональную архитектуру Европейского Союза, что формирует двойной вектор цифрового суверенитета. С одной стороны, страна реализует централизованную стратегию через *Strategia Cloud Italia* и проект Polo Strategico Nazionale (NSH), направленне. на консолидацию критических государственных сервисов в суверенной инфраструктуре. С другой стороны, Италия обязана соблюдать общеевропейские стандарты (например, GDPR, участие в GAIA-X), что требует постоянной координации между национальными и наднациональными институтами. Таким образом, в итальянском случае унитарная структура позволяет продвигать централизованные решения, но специфика членства в ЕС обуславливает гибридный подход к построению гостеха, где национальные интересы сочетаются с региональной цифровой интеграцией.

При этом в целом на данный момент концепция «Cloud Smart + Cloud Native» начинает преобладать как новая парадигма.

Эволюция государственных облачных стратегий движется от «Cloud First» к более зрелым схемам — «Cloud Smart», учитывающим безопасность, затраты и эффективность. Но для отказа от устаревших систем и обеспечения переносимости между облаками необходимо внедрение cloud-native подходов: контейнеризация, микросервисы, Kubernetes и DevSecOps.

Эта связка, которую можно назвать «Cloud Smart + Cloud Native», становится стратегическим трендом государственных информационных технологий — акцент на архитектуре, ориентированной на масштабируемость, безопасность и независимость.

Заключение

В условиях глобальной цифровизации концепция цифрового суверенитета становится неотъемлемым элементом государственной политики, отражающим стремление стран обеспечить контроль над стратегическими данными, инфраструктурой и технологиями. Сравнительный анализ моделей США, Италии, Сингапура и ОАЭ показывает, что цифровой суверенитет формируется как гибридная конструкция, включающая институциональные, технологические и кадровые компоненты.

- США реализуют модель рыночного доминирования, где ключевым инструментом выступает экстерриториальное регулирование (например, CLOUD Act) и глобальное влияние частных провайдеров. Такой подход обеспечивает инновационное лидерство, но усиливает зависимость других стран от американских стандартов.
- Италия демонстрирует институционально-европейскую модель, где национальные стратегии (Strategia Cloud Italia, NSH) встроены в наднациональные инициативы (GAIA-X, GDPR). Это позволяет обеспечивать баланс между инновациями и защитой данных, но требует постоянной координации между уровнями власти.
- Сингапур воплощает централизованную технократическую модель: государство выступает главным интегратором цифровой инфраструктуры, а облачные технологии становятся не только инструментом управления, но и частью политического контроля. Такой подход обеспечивает высокую скорость внедрения решений, но создаёт риск чрезмерной концентрации власти в руках государства.
- ОАЭ применяют федеративную стратегию: федеральные стандарты (FedNet, TDRA) сочетаются с автономными инициативами эмиратов (Smart Dubai, ADDA). Это позволяет развивать гибридные архитектуры и распределять риски, но требует значительных усилий по унификации безопасности и кадровой локализации в условиях зависимости от иностранной рабочей силы.

Таким образом, политико-административное устройство государства напрямую влияет на конфигурацию цифрового суверенитета: федерации (США, ОАЭ) склонны к децентрализации и мультиоблачным моделям, что повышает гибкость, но усложняет координацию, а унитарные государства (Сингапур, Италия) развивают централизованные суверенные облака, добиваясь единообразия и контроля, но рискуют ограничением конкуренции и инноваций.

Практический вывод состоит в том, что универсальной модели цифрового суверенитета не существует: успешная стратегия требует адаптации архитектурных решений к политической системе, уровню цифровой зрелости и кадровым возможностям страны. Наиболее перспективным трендом становится связка «Cloud Smart + Cloud Native», обеспечивающая одновременно гибкость, безопасность и устойчивость цифровой инфраструктуры.

Таким образом, цифровой суверенитет в XXI веке представляет собой многокомпонентное явление, где технологическая инфраструктура, нормативно-правовые механизмы и административная координация интегрируются в единую стратегию обеспечения независимости государства. Анализ современной литературы демонстрирует, что растущий интерес к концепции «суверенитета как сервиса» (*sovereignty-as-a-service*) отражает попытки глобальных облачных провайдеров позиционировать свои платформенные решения как инструмент цифровой автономии (Grohmann & Barbosa, 2025) [22].

Однако рассмотренные в статье примеры демонстрируют альтернативную траекторию: государства формируют собственные суверенные облачные платформы и инфраструктуры, обеспечивая институционализированный контроль над данными, операциями и технологическими процессами. Такой подход снижает зависимость от транснациональных облачных провайдеров и укрепляет долгосрочную устойчивость суверенной цифровой среды.

ЛИТЕРАТУРА

1. Reinsel D., Gantz J., Rydning J. The Digitization of the World: From Edge to Core [Электронный ресурс]. — IDC, 2018. — Режим доступа: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (дата обращения: 01.07.2025).
2. Clissa L., Lassnig M., Rinaldi L. How big is Big Data? A comprehensive survey of data production, storage, and streaming in science and industry [Электронный ресурс] // Frontiers in Big Data. — 2023. — Т. 6. — № 1271639. — Режим доступа: https://www.frontiersin.org/articles/10.3389/fdata.2023.1271639/full (дата обращения: 01.07.2025).
3. Federal Cloud Computing Strategy [Электронный ресурс]. — Вашингтон (Округ Колумбия): The White House, 2011. — Режим доступа: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf (дата обращения: 03.07.2025).

4. Pierucci F. Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace [Электронный ресурс] // Digital Society. — 2025. — Т. 4, № 1. — Статья 27. — Режим доступа: https://link.springer.com/article/10.1007/s44206-025-00189-4 (дата обращения: 25.07.2025).
5. Scherenberg F., Hellmeier M., Otto B. Data Sovereignty in Information Systems [Электронный ресурс] // Electronic Markets. — 2024. — Т.34. — Статья 15. — Режим доступа: https://link.springer.com/article/10.1007/s12525-024-00693-4 (дата обращения: 30.07.2025).
6. Belli L., Gaspar W.B., Singh J.S. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries [Электронный ресурс] // Computer Law & Security Review. — 2024. — Т. 54. — Статья 106017. — Режим доступа: https://ssrn.com/abstract=4903196 (дата обращения: 30.07.2025).
7. Galij S., Pawlak G., Grzyb S. Modeling Data Sovereignty in Public Cloud — A Comparison of Existing Solutions [Электронный ресурс] // Applied Sciences. — MDPI, 2024. — Т. 14, № 23. — Статья 10803. — Режим доступа: https://www.mdpi.com/2076-3417/14/23/10803 (дата обращения: 01.08.2025).
8. Burtscher M., Piano S., Welby B. Developing Skills for Digital Government: A Review of Good Practices across OECD Governments [Электронный ресурс] // OECD Social, Employment and Migration Working Papers. — № 303. — Париж: OECD Publishing, 2024. — Режим доступа: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/developing-skills-for-digital-government_ea7d9105/f4dab2e9-en.pdf (дата обращения: 10.08.2025).
9. Larsen B. The Geopolitics of AI and the Rise of Digital Sovereignty [Электронный ресурс] // Brookings Institution, 2022. — Режим доступа: https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/ (дата обращения: 10.08.2025).
10. Glasze G., Cattaruzza A., Douzet F. и др. Contested Spatialities of Digital Sovereignty [Электронный ресурс] // Geopolitics. — 2022. — Т. 28, № 2. — С. 919–958. — Режим доступа: https://www.tandfonline.com/doi/full/10.1080/14650045.2022.2050070 (дата обращения: 10.08.2025).
11. Hobbs C. (ред.) Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry [Электронный ресурс]. — Лондон: European Council on Foreign Relations, 2020. — Режим доступа: https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/ (дата обращения: 12.08.2025).
12. Kundra V. 25 Point Implementation Plan to Reform Federal Information Technology Management [Электронный ресурс]. — Вашингтон: The White House / OMB, 2010. — Режим доступа: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf (дата обращения: 25.06.2025).
13. Khajeh-Hosseini A., Greenwood D., Smith J.W., Sommerville I. The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise [Электронный ресурс] // arXiv preprint. — 2010. — arXiv:1003.3866. — Режим доступа: https://arxiv.org/abs/1003.3866 (дата обращения: 01.07.2025).
14. Fahmideh M., Daneshgar F., Beydoun G., Rabhi F. Challenges in Migrating Legacy Software Systems to the Cloud — an Empirical Study [Электронный ресурс] // Information Systems — 2017. — Режим доступа: https://arxiv.org/abs/2004.10724 (дата обращения: 05.07.2025).
15. Elena G., Johnson C.W. Factors influencing risk acceptance of Cloud Computing services in the UK Government [Электронный ресурс] // arXiv preprint. — 2015. — arXiv:1509.06533. — Режим доступа: https://arxiv.org/abs/1509.06533 (дата обращения: 08.07.2025)
16. Kent S. Federal Cloud Computing Strategy [Электронный ресурс]. — Вашингтон: The White House, 2019. — Режим доступа: https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf (дата обращения: 05.07.2025).
17. Younus M. и др. Analyzing the Trend of Government Support for Cloud Computing Usage in E-Government Architecture [Электронный ресурс] // Journal of Cloud Computing. — 2025. — Т. 14. — Статья 14. — Режим доступа: https://link.springer.com/article/10.1186/s13677-025-00735-y (дата обращения: 20.08.2025).
18. Saxena D., Gupta R., Singh A.K. A Survey and Comparative Study on Multi-Cloud Architectures [Электронный ресурс] // arXiv preprint. — 2021. — arXiv:2108.12831. — Режим доступа: https://arxiv.org/abs/2108.12831 (дата обращения: 22.08.2025).
19. Polinati A.K. Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments [Электронный ресурс] // arXiv preprint. — 2025. — arXiv:2506.00426. — Режим доступа: https://arxiv.org/abs/2506.00426 (дата обращения: 25.08.2025).
20. Khadilkar V., Chavan A., Kimmatkar N. и др. Secure Data Processing in a Hybrid Cloud [Электронный ресурс] // arXiv preprint. — 2011. — arXiv:1105.1982. — Режим доступа: https://arxiv.org/abs/1105.1982 (дата обращения: 26.08.2025)
21. Venkateswaran S., Sarkar S. Architectural Partitioning and Deployment Modeling on Hybrid Clouds // Software: Practice and Experience. — 2018. — Т. 48, № 2. — С. 345–365. — [Электронный ресурс] — Режим доступа: https://arxiv.org/abs/2205.04467 (дата обращения: 26.08.2025).
22. Grohmann R., Barbosa A.C. Big Tech Sovereignty: Platforms and Discourse of Sovereignty-as-a-Service [Электронный ресурс] // AoIR Selected Papers of Internet Research. — 2025. — Режим доступа: https://spir.aoir.org/ojs/index.php/spir/article/view/13948 (дата обращения: 10.09.2025).
23. Irion K. Government Cloud Computing and National Data Sovereignty [Электронный ресурс] // Policy & Internet. — 2012. — Т. 4, № 3–4. — С. 40–71. — Режим доступа: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.10 (дата обращения: 07.09.2025).
24. Kheng Leong T. Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization [Электронный ресурс]. — // arXiv preprint. — 2022. — arXiv:2202.10069. — Режим доступа: https://arxiv.org/abs/2202.10069 (дата обращения: 10.09.2025)
25. Hand L. IDC FutureScape: Worldwide Retail 2024 Predictions [Электронный ресурс]. — IDC, 2023. — Режим доступа: https://www.idc.com/getdoc.jsp?containerId=US51381823 (дата обращения: 15.09.2025).
26. Gartner Announces the Top 10 Government Technology Trends for 2023 [Электронный ресурс] // Gartner. — 2023. — Режим доступа: https://www.gartner.com/en/newsroom/press-releases/2023-04-17-gartner-announces-the-top-10-government-technology-trends-for-2023 (дата обращения: 15.09.2025).
27. Schwartz P.M. Legal Access to the Global Cloud [Электронный ресурс] // Columbia Law Review. — 2018. — Т. 118, №6. — Режим доступа: https://www.columbialawreview.org/content/legal-access-to-the-global-cloud/ (дата обращения: 06.07.2025).
28. Baur A. European Dreams of the Cloud: Imagining Innovation and Political Control [Электронный ресурс] // Geopolitics. — 2024. — Т. 29, № 3. — С. 796–820. — Режим доступа: https://www.tandfonline.com/doi/full/10.1080/14650045.2022.2151902 (дата обращения: 20.09.2025).
29. Ng R. Cloud Computing in Singapore: Key Drivers and Recommendations for a Smart Nation [Электронный ресурс] // Politics and Governance. — 2018. — Т. 6, № 4. — С. 39–47. — Режим доступа: https://www.cogitatiopress.com/politicsandgovernance/article/view/1757 (дата обращения: 30.09.2025).

30. Taylor R.D. «Data Localization»: The Internet in the Balance [Электронный ресурс] // Telecommunications Policy. — 2020. — Т. 44, № 8. — Статья 102003. — Режим доступа: https://linkinghub.elsevier.com/retrieve/pii/S0308596120300951 (дата обращения: 17.09.2025).
31. Fratini S. Data Localization as Contested and Narrated Security in the Age of Digital Sovereignty: the Case of Switzerland. [Электронный ресурс] // Information, Communication & Society. — 2024. — Т. 28, № 8. — Режим доступа: https://www.tandfonline.com/doi/full/10.1080/1369118X.2024.2362302 (дата обращения: 17.09.2025).
32. Ramirez S. Cloud Adoption Statistics 2024 [Электронный ресурс]// SQ Magazine. — 2025. — Режим доступа: https://sqmagazine.co.uk/cloud-adoption-statistics/ (дата обращения: 18.09.2025).
33. Jewargi K. Public Cloud to Cloud Repatriation Trend [Электронный ресурс] // Scholars Journal of Engineering and Technology. — 2023. — Т. 11, № 1. — С. 1–3. — Режим доступа: https://saspublishers.com/media/articles/SJET_111_1-3_FT.pdf (дата обращения: 20.09.2025).
34. Wu E. Sovereignty and Data Localization [Электронный ресурс]. — Belfer Center for Science and International Affairs Harvard Kennedy School, 2021. — Режим доступа: https://www.belfercenter.org/publication/sovereignty-and-data-localization (дата обращения: 21.09.2025).
35. Fratini S., Hine E., Novelli C. и др. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models [Электронный ресурс] // Digital Society. — 2024. — Т. 3, № 3. — С. 59. — Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4816020 (дата обращения: 21.09.2025).
36. Congressional Research Service. Cloud Smart: Federal Cloud Computing Strategy [Электронный ресурс] // CRS Report R46119. — Вашингтон, 2020. — Режим доступа: https://www.congress.gov/crs-product/R46119 (дата обращения: 05.07.2025).
37. FedRAMP 20x Standards and Authorization Framework [Электронный ресурс]. — Вашингтон: U.S. General Services Administration, 2023. — Режим доступа: https://www.fedramp.gov/20x/standards/ (дата обращения: 07.07.2025).
38. National Institute of Standards and Technology (NIST). The NIST Definition of Cloud Computing. Special Publication 800-145 [Электронный ресурс]. — Гейтерсберг: NIST, 2011. — Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата обращения: 07.07.2025).
39. CLOUD Act Resources [Электронный ресурс]. — Вашингтон: Criminal Division U.S. Department of Justice, 2019. — Режим доступа: https://www.justice.gov/criminal/cloud-act-resources (дата обращения: 09.07.2025)
40. Darnis J.P. Shifting Borders and New Technological Frontiers: The Case of Italy [Электронный ресурс] // Istituto Affari Internazionali, 2018. — Режим доступа: https://www.iai.it/sites/default/files/iaicom1846.pdf (дата обращения: 12.08.2025).
41. Strategia Cloud Italia [Электронный ресурс]/ — Рим: AGID, 2021. — Режим доступа: https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/index.html (дата обращения: 15.08.2025).
42. United Nations. EGOV Knowledge Base: Country Information — Singapore [Электронный ресурс]. — Режим доступа: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/154-Singapore (дата обращения: 28.09.2025).
43. Digital Government Blueprint [Электронный ресурс]. — Сингапур: Smart Nation and Digital Government Office, 2020. — Режим доступа: https://www.smartnation.gov.sg/files/publications/dgb-public-document_30dec20.pdf (дата обращения: 30.09.2025).
44. Baldoni R., Di Luna G. Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities [Электронный ресурс] // IEEE Security & Privacy. — 2025. — Т. 23, № 1. — С. 91–96. — Режим доступа: https://arxiv.org/abs/2503.10140 (дата обращения: 01.10.2025).