

## Центры обработки данных как стратегический актив в контексте цифрового суверенитета России

Научный руководитель – Павлюченко Александра Андреевна

*Бессонова Софья Сергеевна*

*Студент (бакалавр)*

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра информационного обеспечения внешней политики, Москва, Россия

*E-mail: sofabessonova57@gmail.com*

Центры обработки данных как стратегический актив в контексте цифрового суверенитета России

В современном политическом дискурсе всё отчетливее проявляется сдвиг в понимании природы государственного суверенитета: если прежде он ассоциировался преимущественно с контролем над территорией и физическими ресурсами, то сегодня ключевым его измерением становится контроль над потоками данных и инфраструктурой их обработки. Центры обработки данных (ЦОД) в этом контексте перестают быть периферийным элементом ИТ-инфраструктуры и обретают качественно иной статус — статус стратегического национального актива, напрямую связанного с обеспечением цифрового суверенитета. Цель настоящей работы — проследить институциональную эволюцию дата-центров в Российской Федерации и выявить ключевые факторы, определяющие их трансформацию в объект первостепенного государственного значения.

Юридическим фундаментом этой трансформации выступил Федеральный закон «О безопасности критической информационной инфраструктуры» 2017 года, впервые закрепивший за ЦОД статус объектов, чья дестабилизация способна повлечь катастрофические последствия для национальной безопасности. Логическим продолжением этой линии стало Постановление Правительства РФ №1932 от 28 ноября 2025 года, утвердившее порядок ведения реестра дата-центров и окончательно легитимировавшее их особое положение в системе государственного управления.

Динамика российского рынка дата-центров подтверждает их растущую значимость. К концу 2024 года совокупная установленная мощность коммерческих площадок достигла 841,5 МВт, увеличившись на 22% по сравнению с предыдущим годом, а с учётом майнинг-овых комплексов этот показатель превысил 3,5 ГВт. Драйверами роста выступают политика импортозамещения, форсированная цифровизация государственных услуг и экспоненциально растущий спрос на вычисления для задач искусственного интеллекта. Одновременно фиксируется устойчивая тенденция географической диверсификации: инфраструктура смещается из столичных агломераций в региональные центры — Екатеринбург, Новосибирск, на Дальний Восток, что существенно повышает отказоустойчивость национальной цифровой экосистемы.

Однако стремительное развитие отрасли наталкивается на системное ограничение — дефицит энергетических мощностей. Согласно прогнозу Международного энергетического агентства, к 2030 году мировое энергопотребление дата-центров удвоится, достигнув объёмов, сопоставимых с годовым потреблением Японии. В центральных регионах России уже фиксируется острый дефицит доступных мощностей, что побудило высшее руководство страны в ноябре 2025 года поставить задачу синхронизации планов развития ЦОД с модернизацией национальной энергосистемы.

Глобальный контекст развития ЦОД определяется нарастающей фрагментацией киберпространства. Усиление национальных политик цифрового суверенитета — европейский

GDPR, американский CLOUD Act, китайская модель «суверенного интернета» — превращает инфраструктуру данных в арену острого геополитического соперничества. В этих условиях дата-центры становятся первоочередными целями в гибридных войнах: только за первое полугодие 2025 года зафиксировано более 105 тысяч кибератак на российскую критическую инфраструктуру.

Примечательно, что Россия не ограничивается оборонительной стратегией, но активно использует накопленные компетенции в строительстве ЦОД как инструмент «мягкой силы». В рамках БРИКС и СНГ продвигаются инициативы по созданию независимых оптоволоконных магистралей и возведению дата-центров «под ключ» с использованием отечественного оборудования и программных платформ. Таким образом формируется альтернативная зона технологического влияния, базирующаяся на общих стандартах безопасности и регулирования.

Резюмируя изложенное, можно констатировать, что центры обработки данных в Российской Федерации завершили трансформацию в полноценный стратегический национальный актив, развитие которого определяется сложным взаимодействием внутренних императивов (импортозамещение, цифровизация, энергообеспечение) и внешних вызовов (геотехнологическое соперничество, киберугрозы). От того, насколько успешно будут преодолены системные барьеры — прежде всего в энергетической и кадровой сферах, — зависит не только устойчивость национального цифрового суверенитета, но и роль России в формировании архитектуры глобального цифрового будущего.

### Источники и литература

- 1) Андреева А.В., Верещагин В.Ю. Что означает понятие «суверенитет» в цифровом мире? // Научно-образовательный портал «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/chto-oznachaet-ponyatie-suverenitet-v-tsifrovom-mire/viewer>
- 2) Barlow J.P. A Declaration of the Independence of Cyberspace // Electronic Frontier Foundation. 1996. 8 February. URL: <https://www.eff-org/fr/cyberspace-independence>
- 3) МЭА ждет роста потребления электроэнергии ЦОДами вдвое к 2030 году // ТАСС. 2025. 19 ноября. URL: <https://tass.ru/ekonomika/25600385>
- 4) Обзор рынка дата-центров 2025 // Альфа-Банк. 2025. URL: [https://alfabank.st/marketing/24/98/marketing/Data\\_centers\\_market\\_review\\_2025.pdf](https://alfabank.st/marketing/24/98/marketing/Data_centers_market_review_2025.pdf)
- 5) Россия продолжит строительство ЦОДов на базе АЭС, заявил Путин // РИА Новости. 2025. 19 ноября. URL: <https://ria.ru/20251119/rossija-2056116643.html>
- 6) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31. Ст. 4736.
- 7) Barney J. Firm resources and sustained competitive advantage // Journal of Management. 1991. Vol. 17, No. 1. P. 99–120.