РЕГУЛИРОВАНИЕ "ОБЛАЧНЫХ СЕРВИСОВ" КАК ИНСТРУМЕНТ МЕЖДУНАРОДНОЙ КОНКУРЕНЦИИ: ОПЫТ США И КИТАЯ

© ГРИГОРЬЕВСКИЙ В.В., 2024

ГРИГОРЬЕВСКИЙ Валентин Валентинович, аспирант отдела международно-политических проблем.
Национальный исследовательский институт мировой экономики и международных отношений им. Е.М. Примакова РАН, РФ, 117997 Москва, Профсоюзная, 23 (*v.grigoryevskiy@gmail.com*), *ORCID: 0000-0003-2684-9443*

Григорьевский В.В. Регулирование "облачных сервисов" как инструмент международной конкуренции: опыт США и Китая. *Анализ и прогноз. Журнал ИМЭМО РАН*, 2024, № 3, сс. 50-70. DOI: 10.20542/afij-2024-3-50-70 EDN: EQWMOM

DOI: 10.20542/afij-2024-3-50-70
EDN: EQWMOM
УДК: 327+004

Поступила в редакцию 09.07.2024.
После доработки18.09.2024.
Принята к публикации 01.10.2024.

Международная индустрия "облачных сервисов" (ОС) представляет собой арену глобальной экономической конкуренции и потенциально способна стать полем для политического соперничества между различными субъектами. На сегодняшний день наиболее влиятельными участниками в данной конкурентной среде остаются государства. США и Китай активно предпринимают шаги для усиления своей позиции в сфере ОС, в частности посредством различных методов регулирования. В статье рассматриваются стратегии государственного регулирования, которые классифицированы как "позитивные" и "негативные", а также как "оборонительные" и "наступательные"; приведены примеры для каждого типа. Проведен детальный анализ национальных стратегий Соединенных Штатов и Китая как концептуальных планов регулирования "облачных сервисов", заявленных в официальных документах. Детально рассмотрены документы международных межправительственных организаций и институтов глобального управления, через которые страны реализуют свои стратегии по регулированию ОС, как по отдельности, так и с их совместным участием. Перечислены общие и особенные черты политики США и КНР как в формулировании национальных стратегий, так и в принципах, декларируемых на уровне международных институтов. Подтверждена научная гипотеза о том, что регулирование ОС фактически используется как инструмент международного политического влияния. Автор определил ключевые факторы развития международной системы регулирования в сфере ОС: развитие технологической сферы ОС и трансформация мирового порядка. Также сформулировал основную сценарную ось – борьба США и Китая за доминирование в странах и регионах Глобального Юга. На основании этого автор предложил сценарный прогноз развития международного регулирования "облачных сервисов": конфронтационный (конкуренция имеет преимущественно политический характер, увеличиваются риски фрагментации интернета, происходит дивергенция технических стандартов, растет вероятность деструктивных действий, включая применение ОС в военных целях) и консенсусный (международная конвергенция во всех аспектах регулирования

ОС – техническая стандартизация, юридические нормы и экономические правила, основополагающие принципы защиты персональных данных и соблюдения национальных интересов всех стран).

Ключевые слова: киберполитика, *Kuberpolitik*, ИКТ, "облачные сервисы", международные отношения, регулирование, конкуренция, суверенитет, США, Китай.

Конфликт интересов: автор заявляет об отсутствии конфликта интересов финансового и нефинансового характера.

Финансирование: автор заявляет об отсутствии внешнего финансирования.

CLOUD SERVICES REGULATION AS A TOOL OF INTERNATIONAL COMPETITION: U.S. AND CHINA POLICIES

Received 09.07.2024. Revised 18.09.2024. Accepted 01.10.2024.

Valentin V. GRIGORYEVSKY (v.grigoryevskiy@gmail.com), ORCID 0000-0003-2684-9443,
Primakov National Research Institute of World Economy and International Relations, Russian Academy of Sciences (IMEMO), 23, Profsoyuznaya Str., Moscow 117997, Russian Federation.

The international cloud services industry represents an arena of global economic competition and has the potential to become a field for political rivalry among various actors. States remain the primary actors in this competitive landscape, with the U.S. and China actively enhancing their positions through various regulatory measures. The article examines government regulation strategies, categorising them into 'positive' and 'negative' as well as 'defensive' and 'offensive', with examples provided for each. A thorough analysis of national strategies from official U.S. and Chinese documents reveals their conceptual approaches to cloud services regulation. The documents of international intergovernmental organisations and global governance institutions through which countries implement (both individually and in their collaborative participation) their strategies for regulating cloud services were examined in detail. Commonalities and differences in the regulatory policies of the U.S. and China are highlighted, both in their national strategies and in principles articulated at the international level. The study confirms the hypothesis that cloud services regulation serves as a tool for international political influence. Key factors in the evolution of the international regulatory system for cloud services are identified, including their further technological development and shifts in the global order. The primary scenario axis is identified as the U.S.–China competition for dominance in the Global South. Based on these findings, the author presents a scenario forecast for the future of international cloud services regulation. Two potential outcomes are considered: the confrontational one leading to increased political competition, bearing risks of Internet fragmentation, divergence in technical standards, and a higher likelihood of destructive actions, including military use of cloud services; and the consensual one, resulting in international convergence on all aspects of cloud services regulation, including technical standardisation, legal norms, economic rules, fundamental principles of personal data protection and respect for national interests of all states.

***Keywords**: cyberpolitics, Kuberpolitik, ICT, cloud services, international relations, regulation, competition, sovereignty, USA, China.*

About the author: *Valentin V. GRIGORYEVSKY, Postgraduate Student, Department for International Political Problems.*

***Competing interests**: no potential competing financial or non-financial interest was reported by the author.*

***Funding:** no funding was received for conducting this study.*

***For citation*:** Grigoryevsky V.V. Cloud Services Regulation as a Tool of International Competition: U.S. and China Policies. *Analysis and Forecasting. IMEMO Journal,* 2024, no. 3, pp. 50-70. DOI: 10.20542/afij-2024-3-50-70 EDN: EQWMOM

ВВЕДЕНИЕ

"Облачные сервисы" – эффективный инструмент международного влияния, что подтверждается качественной характеристикой их технических компонентов, количественной характеристикой глобального рынка ОС, а также сопряженными возможностями и угрозами, возникающими в международной среде.

В рамках предыдущих исследований автора [1] главный акцент был сделан на возможностях использования государственного регулирования ОС в качестве инструмента международного влияния, поэтому в данной статье анализируются конкретные намерения и проявления использования этого инструмента на примере США и Китая – через национальные стратегии и деятельность в международных институтах.

Цифровое противостояние США и Китая охватывает широкий спектр ИКТ, признается исследователями как вышедшее за рамки экономической среды и в значительной степени реализуется как в политической, так и идеологической сферах. Российские американисты Н.А. Цветкова и А.Н. Сытник описывают, как киберсила Китая (сформированная за счет суверенного интернета, национальных платформ и аппаратных средств), несмотря на все экономические и политические попытки США противостоять Китаю, подрывает американское глобальное лидерство в технологической сфере [2].

Политика США и КНР в этом противостоянии классифицируется российским экспертом в области исследования науки и инноваций И.В. Данилиным как "неотехнонационализм", который сочетает различные подходы (классические протекционистские и глобальные либеральные торгово-экономические) и использует (гео)политические инструменты (от альянсов до санкций) [3].

Исследователи Немецкого института международных отношений и безопасности (Германия) М. Щульце и Д. Вольсен характеризуют технологическое превосходство как фундаментальную основу экономической и военной мощи и на примере США и Китая формулируют понятие "технополитическая сфера влияния" как средство проецирования международной силы [4].

Анализируя американские и китайские официальные стратегические документы, исследователи ИМЭМО РАН Л.В. Панкова и О.В. Гусарова определяют "облачные сервисы" как одну из критически важных зарождающихся технологий (КВЗТ), способных оказать влияние на международную безопасность и стабильность [5]. Их коллега, эксперт в области международной безопасности, Н.П. Ромашкина приводит детальный обзор эволюции регулирования ИКТ в контексте международной безопасности на уровне ООН, показывает ключевые различия в подходах США и России (Китай придерживается схожей с российской модели), а также подчеркивает важность достижения консенсуса по этой проблеме именно на уровне ООН [6]. При этом Н.П. Ромашкина делает вывод о том, что на сегодняшний день отсутствует единый международно-правовой режим, регулирующий сферу ИКТ, и ни одно государство в мире не может считать себя полностью защищенным от трансграничных информационных угроз.

Д.А. Дегтерев, М.С. Рамич и Д.А. Пискунов на примере ключевых позиционных документов США и Китая, принятых на национальном и с их участием – международном уровне, показывают, как эти страны используют регулирование киберпространства в качестве одной из форм международной власти [7]. В частности, авторы выделяют ключевые страновые отличия в моделях управления интернетом:

– США применяют многостороннюю модель управления киберпространством с широким участием негосударственных, частных и общественных организаций

(*multistakeholder*);
- Китай также применяет многостороннюю модель, но с ведущей ролью государств в рамках ООН (*multilateral*).

М.С. Рамич и Д.А. Пискунов формулируют проблему секьюритизации информационного пространства (включая "облачные сервисы"), а также определяют иерархию системы глобального регулирования, в которой США и Китай занимают позицию "создателей правил", но при этом США классифицируется как наивысший I уровень акторов (лидерство в глобальном управлении ИКТ), а Китай как II уровень (существенное влияния на глобальное управление ИКТ) [8].

Аспирант Падуанского университета (Италия) С. Фратини совместно со своими коллегами из ряда европейских вузов на основании двух ключевых критериев (средства и цели достижения цифрового суверенитета) описали четыре модели цифрового суверенитета: основанная на правах, рыночно-ориентированная, централизации и основанная на государстве [9]. 20 стран были классифицированы по этой системе, в том числе США и Китай:
- США реализует рыночно-ориентированную модель – государственное регулирование как гарант ценностей экономической политики невмешательства (*laissez-faire*) и основанные на конкуренции рыночные преимущества и инновации;
- Китай опирается на государственническую модель – размытые границы между государственным и частным секторами, концептуализация цифровых медиа как средства государственного строительства и социально-экономического роста, квазиполная самообеспеченность отечественными цифровыми провайдерами и ресурсами, масштабные инвестиции в новые технологии и желание экспортировать нормы регулирования и цифровые стандарты.

Доцент кафедры китайского права и управления в Лейденском университете (Нидерланды) Р. Кримерс исследует особенности Китая по регулированию ИКТ и на основании в том числе анализа национальных стратегических документов определяет следующие ключевые отличия от западных стран в интерпретации концепций безопасности:
- КНР определяет кибербезопасность преимущественно через информационную безопасность, а западные страны – через целостность, стабильность и функционирование информационных систем и хранящихся в них данных;
- Пекин в своей киберполитике уделяет больше внимания экономическому развитию, в то время как Вашингтон – военным, разведывательным и другим вопросам национальной безопасности [10].

Р. Кримерс объясняет это через три ключевых принципа Китая, лежащих в основе китайского определения суверенитета в киберпространстве:
- национальные правительства имеют суверенные права по защите от других национальных правительств;
- национальные правительства имеют суверенитет над всеми негосударственными субъектами, как внутри страны, так и за рубежом;
- суверенное равноправие государств в управлении интернетом (ни одно государство не должно иметь больше власти, чем другие, или стремиться к гегемонии).

Кримерс описывает ключевые цели, которых Китай стремится достичь посредством регулирования киберпространства: однозначная идентифицируемость каждого субъекта в киберсреде, прозрачность информационных потоков и возможность проведения аудита выполнения требований нормативных актов [11].

Цель настоящего исследования – провести анализ и дать прогноз фактического использования регулирования сферы "облачных сервисов" как инструмента международного влияния. Задачи исследования:
1) проанализировать официальные стратегии США и Китая в части регулирования ОС;
2) сравнить связанную с регулированием ОС деятельность США и Китая в рамках

международных межправительственных организаций, интеграционных форматов и неформальных форумов глобального управления;
3) разработать возможные прогнозы развития сферы регулирования ОС.

Статья содержит четыре раздела, сформированных исходя из поставленных автором задач исследования. В первом обоснован выбор методологии, сформулирована научная гипотеза. Во втором рассмотрены различные типы стратегий государственного регулирования, выявлена специфика государственных стратегий (как концептуальных планов) и политики США и Китая по международному влиянию в сфере "облачных сервисов", дана сравнительная характеристика реализуемых этими странами стратегий. В третьем разделе описаны международные межправительственные организации как инструмент регулирования на примере США и Китая, сопоставлена международная деятельность этих стран. В последней части представлен авторский прогноз будущего развития сферы регулирования глобальной индустрии ОС.

МЕТОДОЛОГИЯ

В контексте международного влияния важно различать возможности и намерения [1]. Страна может обладать огромным потенциалом влияния, но не реализовывать его вовне и, наоборот, 100% своих внутренних возможностей использовать при взаимодействии с другими субъектами системы или для воздействия на них [12]. Намерения такого влияния определяются конкретными планами международного воздействия (стратегии, концепции и пр.) и/или целенаправленными действиями (переговоры, санкции), которые составляют реальную мощь субъекта.

Международное влияние в сфере ИКТ формализовано автором с помощью понятия *Kuberpolitik*, которое определяет субъекты, объекты и методы влияния в этой сфере[1].

Для целей данного исследования выбран тип субъекта "государства, их союзы и коалиции, (суб)региональные интеграционные объединения", который в настоящее время все еще обладает наибольшими возможностями для реализации международного влияния. В частности, рассматриваются США и КНР как лидеры и системообразующие субъекты международной сферы ИКТ [12].

Существуют разные методы (инструменты) международного влияния: правовые, культурные, политические и экономические [13]. В рамках данного исследования "регулирование" рассматривается как совокупность политических и экономических методов. Регулирование может иметь "позитивный" и "негативный" характер и реализовываться как "оборонительными", так и "наступательными" стратегиями.

В первой части исследования была доказана научная гипотеза о том, что регулирование "облачных сервисов" предоставляет государствам возможность международного влияния [1]. В рамках второй части автор формулирует дополнительную гипотезу о том, что страны в действительности имеют намерения по использованию регулирования "облачных сервисов" в качестве инструмента международной конкуренции. В частности, правительства США и Китая используют методы государственного административного регулирования в борьбе за мировое цифровое лидерство, поскольку заинтересованы в стимулировании отечественных перспективных цифровых технологий и инновационных процессов в отдельных отраслях и в масштабе всей национальной экономики, защите и продвижении интересов сверхкрупных национальных технологических корпораций в конкурентной борьбе за цифровые рынки и соперничестве цифровых платформ.

[1] *Kuberpolitik* (от др. – греч. *κυβερ* "управлять" + нем. *politik* "политика"), или Куберполитик, комплексная киберполитика, *comprehensive cyberpolitics* – раздел политической науки, изучающий мировую политику в сфере информационно-коммуникационных технологий, в частности то, как разные типы международных субъектов, используя различные методы воздействия на разные объекты социотехнических (использующих ИКТ) и социотехнологических (разрабатывающих ИКТ) систем, могут оказывать прямое или опосредованное влияние на других международных субъектов [13].

Автор анализирует различные формы реализации государственных методов регулирования "облачных сервисов" через:

- официальные стратегии (и связанные документы), принятые на уровне различных правительственных структур;
- деятельность в рамках международных организаций и форумов регионального и глобального уровней.

Анализируемые стратегии сгруппированы по странам (США и КНР) и представлены в хронологическом порядке по дате их принятия/публикации. Все описанные международные организации и форумы разбиты на три группы по участию стран (только США, только КНР, США и КНР вместе) и перечислены в хронологическом порядке по дате их основания/формирования.

Для прогнозирования развития сферы регулирования ОС автор оперирует следующими понятиями:

- ключевые факторы развития, или движущие силы, – среди множества переменных, определяющих будущее развитие системы, выбираются те, которые имеют наибольшее влияние и в то же время наиболее независимы сами по себе и определяются в рамках конкретных сфер (социальные, технологические, экономические, политические, окружающей среды) [14];
- центральный тренд, или основная сценарная ось, – описывает такие процессы, которые с высокой степенью вероятности будут протекать при прочих равных условиях (то есть вне зависимости от вариативности описанных выше факторов) [15];
- сценарий развития – одна из множества альтернатив, сформированная комбинацией ключевых факторов в рамках центрального тренда, которая может быть также подкреплена "историей будущего", определенной через метод "изучения сценариев" [16] (при построении прогноза автор проводит аналогию с историей формирования и развития "политики нефти").

СТРАТЕГИИ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ

Анализируя методы международного влияния применительно к "облачным сервисам", можно выделить следующие векторы, которые в настоящее время реализуются в наибольшей степени:

- одни государства влияют на другие;
- государства влияют на иностранные коммерческие организации;
- государства влияют на частные лица.

Регулирование может иметь "позитивный" и "негативный" характер (и, соответственно, оказывать конструктивный или деструктивный эффект).

"Позитивное" регулирование направлено на создание благоприятных условий для развития отечественных ОС, как на национальном уровне (программы, стратегии, проекты), так и на международном (международные стандарты, ассоциации, проекты). "Негативное" предполагает реализацию правительственной политики по ограничению развития и распространения иностранных ОС – например, санкции США против катайских компаний – и/или использование отечественных технологий с целью международного влияния – к примеру, широкие полномочия США по использованию данных ОС (электронная почта, *IP*-телефония и пр.) для скрытого слежения, в том числе за иностранными гражданами и организациями.

Также можно классифицировать государственные стратегии регулирования на "оборонительные" и "наступательные". "Оборонительные" предполагают уменьшение влияния иностранных субъектов на внутреннем рынке, "наступательные" стратегии включают шаги, укрепляющие национальные возможности в части использования технологий для оказания влияния на иностранных субъектов (см. табл.).

Таблица. Матрица примеров государственного регулирования (по характеру и стратегии регулирования)

		Стратегия регулирования	
		"Оборонительная"	**"Наступательная"**
Характер регулирования	**"Позитивный"**	– стимулировать развитие отечественных ОС, конкурирующих с иностранными аналогами на внутреннем рынке (или же разработать список рекомендуемых сервисов, предоставляемых иностранными партнерами); – принять участие в формировании международного режима, который бы регулировал условия предоставления ОС с четким определением прав, обязанностей и ответственности вовлеченных сторон.	– стимулировать развитие отечественных (национальных) ОС и их активное продвижение на международном рынке; – поддерживать разведку методами промышленного шпионажа для заимствования технологий с целью сокращения технологического разрыва.
	"Негативный"	– полностью запретить использование ОС, которые предоставляются "недружественными" странами или размещаются в них (в отдельных случаях запрет может распространяться исключительно на использование ОС органами государственной власти).	– запретить использование отечественных ОС отдельным странам или компаниям (санкции и ограничительные меры); – инициировать и/или принимать активное участие в формировании международных норм и стандартов, которые бы прямо или косвенно ограничивали распространение ОС, предоставляемых отдельными странами или компаниями; – использовать ОС для скрытого слежения за иностранными гражданами и организациями; – реализовывать кибератаки, направленные против ОС конкретных стран и/или компаний.

Источник: составлено автором.

Составить максимально полную картину разрабатываемых и используемых методов регулирования отдельно взятого государства вряд ли представляется возможным, так как некоторые из этих документов могут быть либо засекречены, либо не публиковаться в открытом доступе. Тем не менее можно получить общее представление о векторах регулирования на основании публикуемых стратегий (документов) и проводимых в международной среде мероприятий, в инициативном порядке, в двустороннем или многостороннем форматах.

Стратегия США: безопасность через доминирование

Национальная киберстратегия США (*National Cyber Strategy of the USA*), подписанная в сентябре 2018 г. президентом Д. Трампом, в отличие от описанных ниже более поздних стратегий, хотя и не содержит прямого указания на "облачные сервисы", тем не менее имеет ряд утверждений, предвосхищающих увеличение внимания к этой теме в будущем. В частности:

- подчеркивается постоянная конкуренция США со стратегическими противниками – Россией, Китаем, Ираном и Северной Кореей;
- констатируется, что критическая инфраструктура, национальная оборона и повседневная жизнь американцев зависят от компьютерных и взаимосвязанных информационных технологий;
- приводятся планы по модернизации законов об электронном слежении для сбора данных и нарушения криминальной инфраструктуры;
- США декларируют намерение сохранять активную позицию международного лидера для усиления влияния и противодействия растущему спектру угроз и вызовов своим интересам в киберпространстве[2].

[2] *National Cyberstrategy 2018*. The White House. September 2018. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed 09.07.2024).

В **Национальной стратегии кибербезопасности** (*National Cyber Strategy of the USA*), подписанной 1 марта 2023 г. президентом Дж. Байденом, уделяется достаточно большое внимание теме "обычных сервисов"[3].

Так, в части установления правил регулирования кибербезопасности для защиты критической инфраструктуры администрация США планирует выявлять пробелы в полномочиях государственных ведомств для внедрения более эффективных методов кибербезопасности в индустрии "облачных вычислений" и других важных сторонних услуг, и работать с представителями индустрии, Конгрессом и регулирующими органами, чтобы закрыть такие пробелы.

В части модернизации федеральных ИКТ-систем федеральное правительство должно разработать план, в рамках которого, помимо прочего, должна быть предусмотрена замена устаревших систем более безопасными технологиями, в том числе за счет ускорения перехода к "облачным сервисам", что повысит уровень кибербезопасности.

В части постановки задач по предотвращению злоупотребления инфраструктурой США (задача 2.4) подтверждается, что злоумышленники используют в том числе "облачную" инфраструктуру страны для осуществления преступной деятельности, операций по оказанию злонамеренного влияния и шпионажа против индивидуальных жертв, предприятий, правительств и других организаций в США и за рубежом, и что федеральное правительство планирует сотрудничать с поставщиками "облачной" и другой интернет-инфраструктуры для решения этих проблем.

В части постановки задач по активизации федеральных исследований и разработок в области кибербезопасности (задача 4.2) планируется, что департаменты и агентства федерального правительства будут руководить проектами НИОКР для повышения кибербезопасности и устойчивости в таких областях, как "облачная" инфраструктура и телекоммуникации.

В части постановки задач по обеспечению будущего США "чистой" энергией (задача 4.4) делается акцент на использовании передовых "облачных" платформ управления электросетями.

Стратегия Бюро киберпространства и цифровой политики (*National Cybersecurity Strategy*) Государственного департамента США, опубликованная в июне 2023 г., называет технологии источником национальной мощи, устанавливает своей миссией "продвижение национальной и экономической безопасности США, проводя, координируя и совершенствуя внешнюю политику в области киберпространства и цифровых технологий", а также приоритизирует продвижение безопасных и надежных телекоммуникационных услуг и инфраструктуры, поощрение трансграничных потоков данных и пропаганду многосторонних подходов к управлению интернетом и цифровыми технологиями[4].

Стратегический план по кибербезопасности на период 2024–2026 гг. (*Cybersecurity Strategic Plan FY2024–2026*) Агентства по кибербезопасности и защите инфраструктуры (*Cybersecurity and Infrastructure Security Agency, CISA*) Министерства внутренней безопасности США, опубликованный в августе 2023 г., рассматривает связанные с "облачными сервисами" угрозы на уровне с другими типами важнейших угроз национальной безопасности[5]. В части постановки задач по увеличению видимости и возможности решения киберугроз и злоумышленных кампаний (задача 1.1) в плане констатируется, что на данный момент не хватает необходимой широты и глубины информации о кибервторжениях, причем проблема актуальна как для локальных ИКТ-решений, так и для "облачных". Соответственно в части постановки задач по стимулированию реализации измеримых эффективных инвестиций в кибербезопасность (задача 2.2) агентство планирует уделять особое внимание обеспечению безопасного внедрения "облачных сервисов" в организациях по всей стране.

[3] *National Cybersecurity Strategy 2023*. The White House. 01.03.2023. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed 09.07.2024).

[4] *Functional Bureau Strategy*. Bureau of Cyberspace and Digital Policy Strategy. 09.06.2023. Available at: https://www.state.gov/wp-content/uploads/2023/06/FBS_CDP_Public.pdf (accessed 09.07.2024).

[5] *CISA Cybersecurity Strategic Plan FY2024–2026*. Cybersecurity and Infrastructure Security Agency. August 2023. Available at: https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf (accessed 09.07.2024).

Киберстратегия 2023 Министерства обороны (*2023 Cyber Strategy of the Department of Defense*), засекреченный документ, краткое содержание которого было опубликовано в сентябре 2023 г., определяет киберпространство как поле боя, где главными соперниками являются Китай (который "пытается сформировать глобальную технологическую экосистему", а также "предпринимает… скрытое слежение за <иностранными> индивидами"), Россия, КНДР и Иран (все четыре страны прямо обвиняются в кибершпионаже)[6]. Несмотря на то, что основным фокусом этого документа являются военные операции, заявленные в нем планы не ограничиваются этой сферой, а также включают "проведение кампаний в киберпространстве и через него, … достигая информационного и военного преимущества" и "достижение кросс-доменных эффектов" (вероятно, подразумевая невоенные цели)[7]. В целом можно заключить, что выраженная в этом документе позиция США достаточно агрессивна, так как Соединенные Штаты допускают всего два варианта развития своей роли: либо "сдерживать и деэскалировать" угрозы, либо "господствовать" в киберпространстве[8].

Перезагрузка, предотвращение, формирование: стратегия победы Америки в экономическом соревновании с Китайской коммунистической партией (*Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*) – представленный Конгрессом США в конце 2023 г. стратегический документ, подчеркивающий высокое значение не только критической и телекоммуникационной инфраструктуры, но и непосредственно "облачных сервисов"[9].

В частности, на уровне Министерства торговли предлагается установить правило конечного использования "облачных вычислений" с целью ограничения доступа иностранных противников к разработанным на основе технологий США передовым кластерам "облачных вычислений" выше определенного порога вычислений, а также для предотвращения удаленного доступа к экспортоконтролируемым технологиям. На уровне американских компаний, занимающихся "облачными вычислениями", внедрить требования "знай своего клиента" (*know your customer, KYC*), кроме того, обязать такие компании сообщать Министерству торговли о любой иностранной вражеской компании, арендующей вычислительные мощности, превышающие определенный порог, чтобы повысить прозрачность и предотвратить предоставление американскими компаниями передовых вычислительных сервисов иностранным противникам. На уровне Экспортно-импортного банка США (*Export–Import Bank of the United States, EXIM*) в рамках его программы "Китай и трансформационный экспорт" (*China and Transformational Exports Program, CTEP*) принять больший риск потерь по кредитам в своем портфеле и расширить области трансформационного экспорта, включив в него "облачные сервисы" и инфраструктуру.

Федеральный стратегический план исследований и развития кибербезопасности (*Federal Cybersecurity Research and Development Strategic Plan*), опубликованный в декабре 2023 г., одним из своих исследовательских приоритетов определяет разработку средств по установлению доверия (*trust*) и управлению им, рассматриваемого как в широком смысле (доверие к информации в цифровом пространстве), так и в узком (внедрение политик безопасности и авторизации пользователей в ненадежных (*untrusted*) средах, например, в "публичном облаке")[10].

Стратегия Китая: безопасность через суверенитет

Национальная оборона Китая 2008 г. (*2008年中国的国防*) – официальный документ, опубликованный пресс-службой Государственного совета КНР (*国务院新闻办公室*) в январе 2009 г., широко использует понятие "информатизация" как один из методов военного

[6] *2023 Department of Defense Cyber Strategy Summary*. U.S. Department of Defense. September 2023. Available at: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (accessed 09.07.2024).

[7] Ibid.

[8] Ibid.

[9] *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*. The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. 2023. Available at: https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf (accessed 09.07.2024).

[10] *Federal Cybersecurity Research and Development Strategic Plan*. National Science and Technological Council. December 2023. Available at: https://www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf (accessed 09.07.2024).

противостояния (*informationized conflicts*, *信息化战争*). При этом речь идет не только о разработках новых и высокотехнологичных вооружений и техники, но и о ведении информационных войн[11].

Национальная стратегии безопасности киберпространства (*国家网络空间安全战略*), опубликованная в декабре 2016 г. Центральным комитетом КНР по кибербезопасности и информатизации (*中央网络安全和信息化领导小组*), подчеркивает важность, с одной стороны, развития инноваций и применения информационных технологий нового поколения (включая "облачные сервисы"), а с другой, – уважения права всех стран самостоятельно выбирать путь цифрового развития, модель управления сетью, государственную интернет-политику, а также равное участие в международном управлении киберпространством[12].

Международная стратегия сотрудничества в киберпространстве Китая, опубликованная в марте 2017 г., лишь бегло упоминает "облачные сервисы" как одну из передовых ИКТ, но делает заметный акцент на формулировании новых принципов и целей международного регулирования киберпространства:

- независимо от размера, богатства или каких-либо других характеристик государств, все они имеют равные права в создании международных порядка и правил;
- субъекты всех уровней во главе с ООН должны иметь возможность участвовать в создании многоуровневой платформы управления;
- существующие механизмы международного управления (например, Корпорация по управлению доменными именами и *IP*-адресами[13]) должны быть реформированы для обеспечения их полной независимости от отдельных правительств[14].

Национальная оборона Китая в новую эпоху (*新时代的中国国防*), опубликованная тем же ведомством в июле 2019 г., подчеркивает, что в связи с быстрым развитием современных информационных технологий, в том числе ОС, меняются формы ведения войны, эволюция приводит к информационным войнам, и "интеллектуальная война начинает обретать форму"[15].

Глобальная инициатива по безопасности данных (*Global Initiative on Data Security*), опубликованная в сентябре 2020 г. Министерством иностранных дел Китая, призывает международное сообщество воздержаться от атак на критическую информационную инфраструктуру и от использования ИКТ для массового сбора персональных данных, а ИКТ-компании – придерживаться местных законов и хранить данные в юрисдикции предоставления цифровых услуг, не преследовать незаконные интересы, пользуясь зависимостью пользователей от их продуктов[16].

Китайское международное сотрудничество развития в новую эпоху (*新时代的中国国际发展合作*), опубликованное в январе 2021 г. также пресс-службой Государственного совета КНР, подчеркивает роль Китая в формировании цифровой инфраструктуры различных регионов и в поддержании развития цифровой экономики. В частности, упоминаются следующие проекты: 37 телекоммуникационных проектов, включая телекоммуникационные сети и правительственные информационные сети; создание Национальной оптоволоконной кабельной сети в Кении, которая стимулировала

[11] Национальная оборона Китая 2008. См.: *2008年中国的国防*. Available at: https://zh.wikisource.org/w/index.php?title=2008%E5%B9%B4%E4%B8%AD%E5%9B%BD%E7%9A%84%E5%9B%BD%E9%98%B2&oldid=2393160 (accessed 26.02.2024).

[12] Национальная стратегия безопасности киберпространства. См.:《*国家网络空间安全战略*》*全文*. *中央网络安全和信息化委员会办公室*. 2016. Available at: https://www.cac.gov.cn/2016-12/27/c_1120195926.htm (accessed 09.07.2024).

[13] Международная некоммерческая организация Корпорация по управлению доменными именами и *IP*-адресами (*Internet Corporation for Assigned Names and Numbers, ICANN*), созданная 18 сентября 1998 г. при участии правительства США для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета. С октября 2016 г. имеет статус независимой международной организации.

[14] *International Strategy of Cooperation on Cyberspace*. Available at: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm (accessed 28.02.2024).

[15] Национальная оборона Китая в новую эпоху. См.: *新时代的中国国防*. Available at: https://zh.wikisource.org/w/index.php?title=%E6%96%B0%E6%97%B6%E4%BB%A3%E7%9A%84%E4%B8%AD%E5%9B%BD%E5%9B%BD%E9%98%B2&oldid=2363296%EF%BC%8E (accessed 26.02.2024).

[16] *Global Initiative on Data Security*. 08.09.2020. Available at: http://web.archive.org/web/20240529080615/https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html (accessed 29.02.2024).

электронную коммерцию, что ознаменовало скачок в развитии информационной и коммуникационной индустрии страны; создание Полицейского командного центра и правительственной "горячей линии" в Лаосе; создание Интегрированной правительственной информационной системы в Папуа – Новой Гвинее; реализация проекта электронного правительства в Бангладеш[17].

Интересно отметить, что Китай путем организации обучающих семинаров и академических программ также осуществляет активности по передаче другим странам опыта административного управления и совершенствования регулирования в различных сферах, включая сферу цифровой экономиики. Несмотря на то, что в данном документе прямо не упоминаются ОС, однозначно можно утверждать, что наличие собственной цифровой инфраструктуры открывает широкие возможности для продвижения и реализации китайских "облачных технологий", и что даже если американские цифровые гиганты будут конкурировать на рынках третьих стран с Китаем, последний все равно получит больше влияния, владея физической инфраструктурой, поверх которой такие сервисы будут предоставляться.

План развития национальной стандартизации (*国家标准化发展纲要*), известный как "Китайские стандарты 2035", опубликован в октябре 2021 г. совместно Центральным комитетом Коммунистической партии Китая и Государственным советом Китая. Он также не упоминает ОС в явном виде, но делает акцент на необходимости стандартизации технологий, которые обеспечивают развитие цифровой экономики, и предлагает стандартизировать само цифровое общество, цифровое правительство, цифровые финансы, безопасность данных и коммуникационных сетей, защиту персональных данных; предлагает рассмотреть новые типы информационной инфраструктуры, включая новые технологии передачи данных и компьютерных вычислений[18]. Похоже, что в КНР нацелились "играть вдолгую" и приняли решение подойти к достижению глобального цифрового лидерства через формирование и продвижение собственных фундаментальных стандартов в сфере ИКТ – новые низкоуровневые технологии передачи данных. За последние годы Китай значительно увеличил количество предложений в Международной организации по стандартизации (*International Organization for Standardization, ISO*) и Международной электротехнической комиссии (*International Electrotechnical Commission, IEC*). Он достиг ежегодных темпов роста новых предложений в 20%[19], а также занял лидирующие позиции как по количеству патентных заявок в сфере цифровой коммуникации, направленных в Европейское патентное ведомство (*European Patent Office, EPO*), так и по ежегодным темпам роста новых заявок, обогнав (в лице *Huawei*) шведский *Ericsson*, американский *Qualcomm* и южнокорейский *Samsung*[20].

Национальный план информатизации "14-я пятилетка" (*"十四五"国家信息化规划*), опубликованный в декабре 2021 г. Центральным комитетом по кибербезопасности и информатизации ЦК Компартии Китая (*中央网络安全和信息化领导小组*), дает детальное представление о задачах страны по развитию в сфере ИКТ с разных сторон: помимо развития самих технологий, он включает повышение компьютерной грамотности населения, совершенствование методов внедрения и государственного регулирования, развитие международного сотрудничества[21].

ОС упоминаются многократно в различных аспектах:
– социальном, как:

[17] Китайское международное сотрудничество развития в новую эпоху. См.: *新时代的中国国际发展合作*. Available at: https://zh.wikisource.org/w/index.php?title=%E6%96%B0%E6%97%B6%E4%BB%A3%E7%9A%84%E4%B8%AD%E5%9B%BD%E5%9B%BD%E9%99%85%E5%8F%91%E5%B1%95%E5%90%88%E4%BD%9C&oldid=2194584%EF%BC%8E (accessed 26.02.2024).

[18] План развития национальной стандартизации. См.: *中共中央 国务院印发《国家标准化发展纲要》*. 10.10.2021. Available at: https://www.gov.cn/zhengce/2021-10/10/content_5641727.htm (accessed 26.02.2024).

[19] *China Standards 2035 – Shaping the World of Tomorrow?* EAC International Consulting. 13.10.2021. Available at: https://eac-consulting.de/china-standards-2035/ (accessed 26.02.2024).

[20] China Files More Patents in Europe than Ever Before. *China Daily*, 06.04.2022. Available at: https://global.chinadaily.com.cn/a/202204/06/WS624ceb64a310fd2b29e55358.html (accessed 26.02.2024).

[21] Национальный план информатизации "14-я пятилетка". См.: *"十四五" 国家信息化规划*. December 2021. Available at: https://www.gov.cn/xinwen/2021-12/28/5664873/files/1760823a103e4d75ac681564fe481af4.pdf (accessed 09.07.2024).

  - новые каналы предоставления общественных услуг (образовательных и медицинских);
- внутриэкономическом/политическом, как:
  - один из целевых показателей индустриального развития по увеличению доли промышленного оборудования, использующего ОС, с 13.1% в 2020 г. до 30% в 2025 г.;
  - одна из целей по созданию национальной интегрированной системы центров "больших данных";
  - одна из целей по расширению оптимизации и модернизации традиционных отраслей путем реализации подхода "загружайте в облако, используйте данные, обогащайте интеллект";
  - один из инструментов оптимизации сетевых структур и безопасности систем электронного правительства;
  - новые бизнес-модели ("облачный туризм", "облачные потоковые сервисы" и "облачные <художественные> представления");
  - один из объектов государственного регулирования, которое должно быть адаптировано к изменениям, связанным с цифровизацией и технологическими инновациями;
- внешнеэкономическом/политическом, как:
  - одна из целей развития, в рамках которой китайские технологии должны достичь мирового уровня;
  - один из инструментов цифровизации цепочек поставок;
  - один из ключевых инфраструктурных проектов развития под названием "Умная сеть" для реализации концепции "интернет транспортных средств" (*Internet of Vehicles, IoV*);
  - один из компонентов реализации проекта "Цифрового шелкового пути";
  - одна из задач по повышению уровня исследований и разработок приоритетного программного обеспечения для достижения целей технологического прорыва в информационной сфере[22].

Общее и особенное в стратегиях США и Китая

В части формулирования стратегических планов и целей касательно "облачных сервисов" и связанных с этим методов регулирования можно выделить следующие общие характеристики между США и Китаем:

- рост внимания к теме, наблюдаемый в динамике – если в документах 2010-х годов ОС просто перечислялись как одна их передовых ИКТ, то начиная с 2020-х они выделяются в отдельный объект, по которому описывают специфические угрозы и ставят конкретные цели;
- ОС признаются одним из стимулов цифрового развития общества в целом и экономики в частности;
- ОС получают статус эффективного инструмента международного влияния: информационного, экономического, политического и военного;
- активная поддержка крупных ИКТ-компаний для их большего продвижения на международных рынках (но форма поддержки отличается – см. ниже).

Рассматривая отличительные черты США и Китая, можно выделить следующее:

- США открыто и агрессивно формулируют свою позицию в отношении "международных противников" и утверждают собственную первостепенную и исключительную роль в поддержании международного порядка и безопасности в киберпространстве, в то время как Китай настоятельно отрицает исключительное право любой страны на доминирование в данной сфере и подчеркивает необходимость выработки общих норм и правил совместно с другими государствами вне зависимости от уровня их экономического или научно-технического развития;
- США делают акцент на примате свободного потока данных и информации в международном киберпространстве, а Китай – на примате суверенитета каждой

[22] Wang Mingjie. China Files More Patents in Europe than Ever Before. *China Daily*, 06.04.2022. Available at: https://global.chinadaily.com.cn/a/202204/06/WS624ceb64a310fd2b29e55358.html (accessed 26.02.2024).

страны, который и должен определять легитимность тех или иных процессов в киберпространстве;
- США опосредованно способствуют развитию отечественных ИКТ-компаний путем минимального вмешательства в этот рынок, при этом Китай как бы формирует рынок, напрямую поддерживая и развивая крупные компании;
- США борются с влиянием КНР экономическими и политическими методами, а Китай (уже в значительной степени внутренне защищенный от влияния Соединенных Штатов на технологическом, экономическом и политическом уровнях) фокусируется на разработке и формировании нового международного технологического ландшафта, активно разрабатывая собственные стандарты и выделяя значительные государственные инвестиции на международные инфраструктурные проекты.

МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ И ИНСТИТУТЫ ГЛОБАЛЬНОГО УПРАВЛЕНИЯ

"Международные организации и институты глобального управления" – отдельный тип субъекта *Kuberpolitik*, который играет важную роль в планировании и внедрении методов международного регулирования, так как, помимо стандартизации норм взаимодействия субъектов международных отношений, он также реализует институциональную власть отдельных государств, продвигающих свои интересы.

Данный тип субъекта включает формальные организации, которые в большой степени зависят от государств, так как они либо создаются государствами-участниками (международные межправительственные организации, или ММПО), либо создаются в рамках действующего законодательства (международные неправительственные организации, или МНПО), то есть опосредованно зависят от государств. В рамках данной статьи автор рассматривает деятельность США и Китая через различные ММПО, неформальные форумы глобального управления, региональные интеграционные объединения.

На данный момент нет отдельных ММПО, созданных специально для выработки совместных мер по работе с "облачными сервисами", а ОС рассматриваются как один из типов ИКТ, через который может осуществляться влияние (политическое, военное, экономическое и т.д.). Тем не менее автор проводит анализ деятельности США и Китая в рамках существующих ММПО по формулированию и продвижению связанной с регулированием ОС повестки.

ММПО с лидирующей ролью США

Разведывательный альянс *FVEY*, также известный как **"Пять глаз"** (*Five Eyes*), созданный на базе Соглашения о радиотехнической разведывательной деятельности Великобритания–США (*UKUSA Signals Intelligence Agreement, UKUS SIGINT, UKUSA*), история которого начинается в 1940-е годы, включает США, Великобританию, Австралию, Канаду и Новую Зеландию и сотрудничает с Японией, Республикой Корея и странами – участницами НАТО. Альянс сфокусирован на деятельности в сфере сбора разведданных и обмена ими в разных областях, включая агентурную разведку. В открытом доступе нет информации о методах сбора таких данных, но косвенные признаки свидетельствуют об использовании всех потенциальных источников. Так, альянс обвиняет другие страны (в частности, Китай) в краже прав интеллектуальной собственности, в том числе через "облачные сервисы"[23].

Центр НАТО по сотрудничеству в сфере киберобороньы (*NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE*), созданный в 2008 г., рассматривает возможности ИКТ в военном аспекте, а также привлекает внимание исследователей к этой теме, организовав формат регулярной Международной конференции по киберконфликтам (*CyCon*). В рамках

[23] Gooding M. UK and Five Eyes Allies Issue Warning on Chinese 'Theft' of Intellectual Properties. *Tech Monitor*, 18.10.2023. Available at: https://techmonitor.ai/technology/cybersecurity/china-ip-theft-five-eyes (accessed 09.07.2024).

этой конференции, например, в 2020 г. рассматривались вопросы обеспечения суверенитета государственных данных в "облаке" [17], в 2022 г. – сложности, связанные с выявлением киберугроз в ОС [18], а в 2023 г. – зависимость и устойчивость цифровой цепочки поставок (включая ОС) [19].

Четырехстороннее партнерство по кибербезопасности (*Quad Cybersecurity Partnership*) – создано в рамках **Четырехстороннего диалога по безопасности** (*Quadrilateral Security Dialogue, QSD, Quad*) между Австралией, Индией, Японией и США, основанного в 2007 г. и возобновившего свою деятельность в 2017 г. Хотя партнерство не выделяет отдельно тему "облачных сервисов", но участвует в формировании принципов безопасного программного обеспечения[24], а также подчеркивает важность обеспечения безопасности и устойчивости информационных технологий и цепочек поставок цифровых продуктов и услуг[25].

"Чистая сеть" (*The Clean Network*) – инициатива США, объявленная в августе 2020 г., целью которой заявлена разработка "комплексного подхода к защите национальных активов… от агрессивного вторжения со стороны злонамеренных субъектов, таких как Коммунистическая партия Китая" и "устранение долгосрочной угрозы конфиденциальности данных, безопасности, правам человека и принципиальному сотрудничеству, исходящую для свободного мира от авторитарных злонамеренных субъектов"[26]. В декабре 2020 г. США объявили, что более 60 стран и 200 телекоммуникационных компаний присоединились к этой инициативе[27]. Также были запущены и специализированные направления инициативы, в частности:

- "Чистый провайдер" (*The Clean Carrier*), "Чистый кабель" (*The Clean Cable*) и "Чистый путь" (*The Clean Path*), призванные обеспечитесь надежную передачу данных, осуществляемую на разных этапах и посредством разных технологий (проводных или беспроводных);
- "Чистое облако" (*The Clean Cloud*) – для "предотвращения хранения и обработки наиболее конфиденциальной персональной информации граждан США и наиболее ценной интеллектуальной собственности… частных компаний <США>… в облачных системах, доступных… иностранным противникам <США> через такие компании, как *Alibaba*, *Baidu*, *China Mobile*, *China Telecom* и *Tencent*".

Декларация о доступе государственных органов к персональным данным, хранящимся субъектами частного сектора (*Declaration on Government Access to Personal Data Held by Private Sector Entities*), принятая Организацией экономического сотрудничества и развития (ОЭСР) в декабре 2022 г., признает, что продолжающаяся цифровая трансформация приводит к созданию большего количества данных, включая персональные, поскольку цифровые технологии используются во всех секторах мировой экономики. Декларация определяет следующие принципы, по которым, в случае необходимости, национальные правительства:

- имеют право получать доступ к данным вне зависимости от того, где располагаются сами данные или хранящие их компании;
- могут не информировать людей о том, что был осуществлен доступ к их данным или произошло какое-либо нарушение в отношении этих лиц;
- могут ограничивать доступ к данным, удалять или восстанавливать их[28].

Неформальный форум глобального управления **Группа семи** (***G7***) на 49-м саммите глав государств и правительств, прошедшем в Японии в мае 2023 г., в своем итоговом коммюнике

[24] *Quad Cybersecurity Partnership: Joint Principles for Secure Software*. Available at: https://www.pmc.gov.au/sites/default/files/resource/download/quad-joint-principles-secure-software.pdf (accessed 19.02.2024).

[25] *Quad Cybersecurity Partnership: Joint Principles*. Available at: https://www.mofa.go.jp/mofaj/files/100347892.pdf (accessed 19.02.2024).

[26] *The Clean Network*. United States Department of State. Available at: https://2017-2021.state.gov/the-clean-network/ (accessed 19.02.2024).

[27] Expert: Trump Rewrites the U.S. Strategy to Respond to the CCP, and Biden Is Difficult to Reverse | CCP Threats | Human Rights | China Policy. *6Park.News*, 31.01.2021. Available at: http://web.archive.org/web/20210411195357/https://6park.news/en/expert-trump-rewrites-the-u-s-strategy-to-respond-to-the-ccp-and-biden-is-difficult-to-reverse-ccp-threats-human-rights-china-policy-2.html (accessed 19.02.2024).

[28] *OECD/LEGAL/0487 Declaration on Government Access to Personal Data Held by Private Sector Entities*. Organisation for Economic Co-Operation and Development. 14.12.2022. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 (accessed 09.07.2024).

декларировала важность свободного трансграничного потока данных, информации, идей и знаний, но при этом признала проблемы, связанные с конфиденциальностью, защитой данных и прав интеллектуальной собственности, а также безопасностью "облачной" инфраструктуры. Вместе с тем были сделаны достаточно размытые заявления касательно свободного потока данных и прозрачности, потребностей государства сохранять свои законные общественные интересы, авторитарных методов использования технологий. Было заявлено о совместных планах по выработке общих и взаимодополняемых подходов и инструментов регулирования для надежной передачи данных и усиления роли технологий. Показательно, что для обозначения группы технологий используется не термин ИКТ, а ИКТС (*Information and Communications Technologies and Services, ICTS*) – информационно-коммуникационные технологии и сервисы, тем самым подчеркивается растущая роль относительно нового способа реализации цифровых продуктов, в том числе "облачных сервисов"[29].

В рамках **Партнерства по глобальной инфраструктуре и инвестициям** (*The Partnership for Global Infrastructure and Investment, PGII*) участники Группы семи взяли на себя общее обязательство продвигать государственные и частные инвестиции в инфраструктуру. В том числе с этой целью Корпорация финансирования международного развития США (*U.S. International Development Finance Corporation, DFC*) предоставляет кредит на сумму 300 млн долл. Гане на строительство крупнейшей в Африке сети взаимосвязанных средств передачи данных (дата-центров)[30]. Предполагается, что за счет расширения доступа к "облачным технологиям" будет заложена основа цифровой революции на континенте, где проживает 17% населения планеты, но на данный момент находится менее 1% общемирового числа дата-центров.

ММПО с лидерской ролью и при участии Китая

Диалог сотрудничества Азии (*Asia Cooperation Dialogue, ACD*) – международный форум, созданный в 2002 г. и включающий большинство стран Азии. В мая 2019 г. по результатам 16-й Встречи министров иностранных дел в Катаре были сделаны общие заявления об укреплении сотрудничества в целях предотвращения киберугроз, а также об усилении продвижения и защиты прав человека[31].

БРИКС (*BRICS*) – межгосударственное объединение, основанное в июне 2006 г. Бразилией, Россией, Индией и Китаем и включающее на сегодняшний день девять государств, активно продвигает позицию об управлении цифровым пространством и обеспечении международной цифровой безопасности через установление и гарантирование цифрового суверенитета стран [20]. Впервые этот принцип был озвучен в 2015 г.[32], а по итогам саммита 2017 г. сформулированы совместные планы по развитию ИКТ (и "облачных сервисов", в частности), включая создание Института будущих сетей БРИКС (*BRICS Institute of Future Networks, BIFNC*). Тогда же прозвучали заявления о намерениях по установлению международных правил обеспечения безопасности ИКТ-инфраструктуры и защиты данных, а также по совместному созданию безопасной и надежной коммуникационной сети[33].

Региональное интеграционное объединение **Ассоциация государств Юго-Восточной Азии, АСЕАН** (*Association of Southeast Asian Nations, ASEAN*), основанное в 1967 г., хотя и не включает в свой основной состав Китай, тем не менее взаимодействует с ним в различных форматах АСЕАН+ и играет важную роль в региональном форуме Восточноазиатский саммит (см. ниже). В рамках АСЕАН функционирует множество организационных форматов и групп, связанных с вопросами кибербезопасности: Конференция министров АСЕАН по

[29] *G7 Hiroshima Leaders' Communiqué*. 20.05.2023. Available at: https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/Leaders_Communique_01_en.pdf?v20231006 (accessed 19.02.2024).

[30] *Factsheet on the G7 Partnership for Global Infrastructure and Investment*. Available at: https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/session1_01_en01.pdf (accessed 19.02.2024).

[31] *Doha Declaration, 16th Ministerial Meeting of the Asia Cooperation Dialogue 'Partners in Progress'*. 01.05.2019. Available at: http://acd-dialogue.org/ministerial-meeting/16th/Doha-Declaration-Adopted.pdf (accessed 09.07.2024).

[32] *Communique of BRICS Ministers of Communications on the Outcomes of the Meeting on 'Expansion of Cooperation in the Field of Communications and ICTs'*. 23.10.2015. Available at: http://en.brics2015.ru/load/637860 (accessed 09.07.2024).

[33] *BRICS Summit Xiamen Declaration*. 04.09.2017. Available at: https://brics2023.gov.za/wp-content/uploads/2023/07/170904-xiamen.pdf (accessed 09.07.2024).

кибербезопасности (*ASEAN Ministerial Conference on Cybersecurity*), Межсессионное совещание Регионального форума АСЕАН по безопасности и использованию ИКТ (*ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of ICT*), Заседание рабочей группы министров обороны АСЕАН по кибербезопасности (*ASEAN Defence Ministers Working Group Meeting on Cyber Security*), Программа киберпотенциала АСЕАН (*ASEAN Cyber Capacity Programme*)[34].

Шанхайская организация сотрудничества, ШОС (*Shanghai Cooperation Organization, SCO*) – международная организация, созданная в июне 2001 г. Китаем, Россией, Казахстаном, Таджикистаном, Кыргызстаном и Узбекистаном, к которой позже присоединились Индия, Пакистан и Иран – своими главными задачами ставит укрепление стабильности и безопасности, развитие экономического сотрудничества, энергетического партнерства, научного и культурного взаимодействия. Деятельность ШОС также связана и со сферой ИКТ. Так, в мае 2023 г. состоялся Форум по развитию и сотрудничеству в области цифровых технологий Китай–ШОС (*China – Shanghai Cooperation Organization Digital Technology Cooperation and Development Forum*), в рамках которого было отобрано 37 проектов и подготовлен "Сборник кейсов цифрового сотрудничества Китая и стран ШОС (2023 г.)"[35], включающий, например, проект по созданию Инновационного центра "облачных вычислений" Ланканг–Меконг[36]. В ноябре 2023 г. на встрече Группы экспертов ШОС по международной информационной безопасности обсуждались вопросы формирования международно-правового режима регулирования информационного пространства и возможности разработки договора о борьбе с использованием ИКТ в преступных целях[37].

"Цифровой шелковый путь" (*数字丝绸之路*) – проект Китая, инициированный в мае 2017 г. в рамках Организации международного сотрудничества Шелковый путь (*一带一路*)[38], является, вероятно, одним из главных инструментов реализации стратегии Китая по занятию им лидирующих позиций в глобальной сфере ИКТ. В рамках этого проекта еще раз подчеркивается роль Китая в решении следующих задач:

- поддержание цифрового развития мировой экономики;
- сокращение глобального цифрового разрыва;
- развитие глобального управления в сфере управления данными и цифровыми процессами;
- формирование, обучение и развитие "цифровых талантов"[39].

ММПО с совместным участием США и Китая

Организация Объединенных Наций, ООН (*United Nations, UN*), созданная в 1945 г. – универсальная международная межправительственная организация со 193 странами-участницами на сегодняшний день, вероятно, в наименьшей степени является той международной площадкой, через которую США и Китай могут высокоэффективно продвигать свою повестку в сфере "облачных сервисов" (по сравнению с другими вышеперечисленными организациями и диалоговыми платформами). Тем не менее их деятельность ведется и по этому направлению. Актуальна тема согласования Всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*), проект

[34] *East Asia Summit Leaders' Statement on Deepening Cooperation in the Security of ICT and of the Digital Economy*. Available at: https://asean.org/wp-content/uploads/2018/11/EAS-Leaders%E2%80%99-Statement-on-Deepening-Cooperation-in-the-Security-of-ICT-a....pdf (accessed 09.07.2024).

[35] Ruijie Networks Was Invited to Participate in the China-SCO Digital Technology Cooperation and Development Forum. *Ruijie Networks*, 31.05.2023. Available at: https://vn.ruijienetworks.com/about/news/scobdc (accessed 16.09.2024).

[36] Цяйняо был выбран в качестве примера сотрудничества в цифровой сфере между Китаем и странами ШОС. См.: *菜鸟入选中国–上合组织国家数字领域合作案例*. 12.06.2023. Available at: http://web.archive.org/web/20231129112657/http://it.enorth.com.cn/system/2023/06/12/054009753.shtml (accessed 29.02.2024).

[37] *О заседании Группы экспертов ШОС по международной информационной безопасности*. Министерство иностранных дел Российской Федерации. 21.11.2023. Available at: https://www.mid.ru/ru/foreign_policy/rso/1916398/ (accessed 29.02.2024).

[38] Full Text of President Xi's Speech at Opening of Belt and Road Forum. *Xinhua*, 14.05.2017. Available at: http://www.xinhuanet.com/english/2017-05/14/c_136282982.htm (accessed 27.02.2024).

[39] Цифровой шелковый путь ускоряет модернизацию мира. См.: *数字丝绸之路加速世界现代化 - 中国一带一路网*. 30.11.2023. Available at: https://www.yidaiyilu.gov.cn/p/0RRKAALU.html (accessed 28.02.2024).

которой Российская Федерация подала в Генеральную Ассамблею ООН в 2017 г. Этот проект не содержит прямого указания на ОС, так как ИКТ рассматривается в целом как инструмент киберпреступлений[40]. Представители (правительства и общественные организации) США, Великобритании, ЕС и отдельных стран Латинской Америки и Азии высказывают опасение, что принятие документа в текущей редакции может дать законные основания отдельным странам криминализировать онлайн-контент и ограничивать свободу слова, преследовать журналистов, активистов и политическую оппозицию [21]. Иран заявляет, что предложенный проект не является договором о правах человека, и следует использовать подход, аналогичный Конвенции ООН против коррупции, – то есть не включать ссылки на права человека[41]. Россия предлагала криминализировать 23 вида киберпреступлений, и проект Конвенции был поддержан Китаем в его изначальной редакции, однако в последней редакции (на момент подготовки статьи) осталось 11 видов преступлений[42].

Восточноазиатский саммит (*East Asia Summit, EAS*), созданный в 2005 г., изначально включал Китай, а США (и Россия) присоединились к неформальному форуму лидеров 16 государств Восточной и Юго-Восточной Азии, который организует ежегодную встречу в верхах, в 2011 г.[43] В октябре 2018 г. было опубликовано "Заявление лидеров Восточноазиатского саммита по углублению сотрудничества в области безопасности информационно-коммуникационных технологий и цифровой экономики" с указанием на использование результатов работы экспертных групп АСЕАН, а также сделано заявление о необходимости создания открытой, безопасной, стабильной, доступной и мирной среды ИКТ[44]. По итогам 18-й встречи, прошедшей в сентябре 2023 г. в Индонезии было сделано заявление, в котором, помимо прочего, подчеркивалась важность разработки "более ощутимых" проектов связи, а также практически слово в слово повторялось заявление 2018 г. о "создании открытой, безопасной… среды ИКТ"[45].

Азиатско-Тихоокеанское экономическое сотрудничество, **АТЭС** (*Asia-Pacific Economic Cooperation, APEC*), форум открытого регионализма, созданный в 1989 г. и включающий на сегодняшний день 21 страну, уделяет особое внимание теме регулирования ОС. В ноябре 2017 г. Специальная руководящая группа по интернет-экономике (*Ad Hoc Steering Group on Internet Economy*) опубликовала "Дорожную карту АТЭС по интернету и цифровой экономике" (*APEC Internet and Digital Economy Roadmap*), в которой одним из ключевых направлений устанавливается содействие согласованности и сотрудничеству подходов к регулированию интернета и цифровой экономики при соблюдении внутреннего законодательства государств[46]. В августе 2023 г. Рабочая группа АТЭС по телекоммуникациям и информации (*APEC Telecommunications and Information Working Group, TELWG*) опубликовала "Рекомендации по облачной трансформации в АТЭС" (*Recommendations for Cloud Transformation in APEC*). Рекомендации, в частности, советуют странам-участницам четко определить роли и обязанности организаций, предоставляющих ОС (например, контролеры данных и обработчики данных), и руководящие принципы обеспечения конфиденциальности данных; а также применять правила регулирования, которые соответствуют своему назначению,

[40] *Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях*. ООН. 29.06.2021. Available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (accessed 09.07.2024).

[41] *A Dream Deferred or a Near Miss? UN Committee Postpones Decision on Cybercrime Convention*. Global Initiative Against Transnational Organized Crime. Available at: https://globalinitiative.net/analysis/un-committee-postpones-decision-cybercrime-convention/ (accessed 19.02.2024).

[42] Черненко Е. Под статью подвели не все. Россия недовольна проектом Конвенции ООН по борьбе с киберпреступностью. *Коммерсантъ*, 12.01.2024. Available at: https://www.kommersant.ru/doc/6452715 (accessed 09.07.2024).

[43] Восточноазиатский саммит является площадкой для диалога глав государств и правительств стран региона по широкому кругу политических и экономических вопросов, представляющих общий интерес. Встречи в таком формате проводятся ежегодно в привязке к мероприятиям АСЕАН на высшем уровне. Собственного секретариата у форума нет, его функции выполняет Секретариат АСЕАН. Все решения на саммитах принимаются консенсусом.

[44] *East Asia Summit Leaders' Statement on Deepening Cooperation in the Security of ICT and of the Digital Economy*. Available at: https://asean.org/wp-content/uploads/2018/11/EAS-Leaders%E2%80%99-Statement-on-Deepening-Cooperation-in-the-Security-of-ICT-a....pdf (accessed 09.07.2024).

[45] *Chairman's Statement of the 18th East Asia Summit*. ASEAN. 07.09.2023. Available at: https://www.mofa.go.jp/files/100551492.pdf (accessed 09.07.2024).

[46] *APEC Internet and Digital Economy Roadmap*. APEC. 24.10.2017. Available at: https://www.apec.org/docs/default-source/Groups/ECSG/17_csom_006.pdf (accessed 09.07.2024).

прозрачны, контролируемы и основаны на доказательствах[47].

Группа двадцати (***G20***), созданная в 1999 г. и включающая 19 стран-участниц, на 18 саммите, прошедшем в Индии в сентябре 2023 г., несмотря на наличие отдельного трека "Технологическая трансформация и цифровая общественная инфраструктура", ограничивается только общими заявлениями о важности данной темы. Тем не менее в ее декларациях прослеживается некий тренд, общий с описанными выше заявлениями, который таким образом хорошо резюмирует актуальную повестку (и неявное противоречие): "Мы признаем важность надежного свободного трансграничного потока данных, соблюдая при этом применимые правовые рамки"[48].

Общее и особенное в международной деятельности США и КНР

В части формирования и реализации международной институциональной силы США и Китай также имеют как общие, так и особенные черты. Общие характеристики деятельности двух стран можно подытожить одним пунктом: активное участие как в существующих международных организациях и форумах, так и создание новых, где многократно подчеркивается важность двух больших и взаимосвязанных тем – влияния ИКТ (и в частности, "облачных сервисов") на международные отношения и проблемы международного регулирования этой сферы.

Однако рассматриваемые страны сильно отличаются в плане наполнения своей повестки международного сотрудничества.

Во-первых, США бóльшую часть своего внимания и усилий уделяют именно военной сфере (киберугрозы, кибератаки, кибершпионаж, кибербезопасность, военное киберпланирование и т.д.), в то время как Китай действует по всему фронту вопросов, затрагиваемых передовым развитием ИКТ (экономический, военно-политический, культурный и нормативно-правовой).

Во-вторых, Вашингтон продвигает "либеральный" подход (свободный поток данных и информации) к международному экономическому киберсотрудничеству как единый "стандарт", к которому должны стремиться все страны, а Пекин ставит под вопрос универсальность таких "правил", критикуя их неполноту и неоднозначную трактовку, и активно выступает за создание новых правил, учитывающих законные интересы всех участников.

В-третьих, Соединенные Штаты в значительной степени опираются на частные компании и общественные организации (продвигая "свободу" как главное мерило), в то время как Китай главным образом обращается к национальным правительствам (апеллируя к "суверенитету").

В-четвертых, США, уже обладая глобальным доминированием в сфере ОС, пытаются сохранить свою позицию, а КНР продвигает собственные стандарты на международном уровне и широко реализует крупные инфраструктурные ИКТ-проекты, тем самым добиваясь для себя лидерства как в пространственном измерении, так и технологических сферах.

В-пятых, США больше сотрудничают со странами, которые близки им культурно, экономически и политически (Канада, Великобритания, государства ЕС, Австралия), а Китай – с очень разными странами (БРИКС). В этой связи у КНР возникает потенциально больший риск разногласий со своими международными партнерами, но при этом и растет шанс выработать действительно универсальные подходы в глобальном масштабе.

[47] *TELWG Recommendations for Cloud Transformation in APEC*. APEC. 15.08.2023. Available at: https://mddb.apec.org//Documents/2023/SCE/SCE3/23_sce3_006.pdf (accessed 09.07.2024).

[48] *G20 New Delhi Leaders' Declaration*. New Delhi, 9–10 September 2023. Available at: http://www.g20.utoronto.ca/2023/G20-New-Delhi-Leaders-Declaration.pdf (accessed 19.02.2024).

ПРОГНОЗ РАЗВИТИЯ СФЕРЫ РЕГУЛИРОВАНИЯ "ОБЛАЧНЫХ СЕРВИСОВ"

Анализируемую систему сложно прогнозировать, так как она является многоуровневой и многофакторной, от чего в значительной степени зависит ее изменение в будущем. Автор описывает эти факторы и уровни, дает изолированный прогноз для каждого из них, определяет ключевой тренд и на этом основании представляет вероятные сценарии развития.

Ключевые факторы развития международной системы регулирования в сфере ОС.

1. Развитие технологии "облачных сервисов"

Развитие ОС как технология и цифровой продукт (ИКТ-решение) с высокой степенью вероятности принципиально не поменяется: будут появляться новые методы передачи данных, оптимизированные технологии обработки и хранения данных, приниматься новые стандарты, но концептуальная модель удаленного выполнения программ и хранения данных не изменится. Тем не менее высоковероятно, что биполярная технологическая конкуренция будет сохраняться.

Также высоковероятно, что тенденция развития ОС как инструмента цифровизации социально-экономических процессов продолжится, и все больше таких процессов будут оцифрованы как раз с использованием ОС.

Высоковероятно, что ОС как военно-политический инструмент будут еще шире и активнее использоваться для информационных кампаний, шпионажа, военного воздействия и политического принуждения, что вызвано вышеупомянутым принципом их функционирования (удаленное выполнение программ и доступ к ним через сеть).

С высокой степенью вероятности развитие новых методов регулирования будет происходить параллельно с развитием способов проведения кибератак (в широком смысле).

2. Трансформация мирового порядка

Высоковероятно, что США и Китай будут оставаться глобальными лидерами и центрами международной гравитации во всех сферах (технологической, экономической, политической, военной). Конфликтность между ними будет расти, а уровень противостояния США и Китая – повышаться. Наряду с этим будет усиливаться стремление и других стран к увеличению их роли и влияния на форумах глобального управления. Вероятно, текущая система функционирования ООН как универсальной международной площадки достижения международного консенсуса будет все менее эффективно справляться со своей задачей.

Центральный тренд определяет процессы, которые с высокой долей вероятности будут протекать при прочих равных условиях (то есть вне зависимости от вариативности описанных выше факторов). Автор делает предположение, что один из наиболее существенных ресурсов будущего развития США и Китая – это Глобальный Юг, а борьба за доминирование в этом регионе станет центральным трендом анализируемой системы. Вне зависимости от реализации конкретного сценария США и Китай будут уделять большое внимание развитию крупных проектов информационной инфраструктуры, продвижению своих ИКТ-компаний и "поддержанию кибербезопасности" на Глобальном Юге.

Вероятные сценарии развития, по мнению автора, главным образом определяются (среди всех вышеперечисленных факторов) возможностью достижения глобального консенсуса в целом и будущим ООН как международной площадки для его достижения, в частности.

Сценарий "А. Консенсус не достигается" (продолжение текущей ситуации), при которой конкуренция имеет преимущественно политический характер, увеличиваются риски фрагментации интернета, происходит дивергенция технических стандартов, растет вероятность деструктивных действий, включая применение "облачных сервисов" в военных целях.

Сценарий "Б. Консенсус достигается" (как длительный процесс). В таком случае мы сможем наблюдать международную конвергенцию во всех аспектах, касающихся регулирования ОС – техническая стандартизация, юридические нормы и экономические правила, основополагающие принципы защиты персональных данных и соблюдения национальных интересов всех стран. При этом сценарии конкуренция за Глобальный Юг между США и Китаем будет иметь преимущественно экономический характер, а количество потенциальных взаимных деструктивных действий в киберпространстве будет значительно снижаться.

Учитывая прогнозы роста рынка ОС в сравнении с рынком сырой нефти (первый обгонит второй в 2032 г. [1]), интересно провести аналогию "политики облачных сервисов" с "политикой нефти". До нефтяного кризиса 1973 г. мировая торговля нефти имела больше экономический характер, чем политический. Первый мировой нефтяной кризис привел к формированию понятия "нефтяное оружие", а после кризиса большинство стран мира стали развивать свою политику в части обеспечения энергетической безопасности. Конечно, ОС довольно сильно отличаются от нефти по своей природе, но есть и много общих характеристик, и ключевая из них – влияние если не на все, то на большинство отраслей и сфер жизнедеятельности (когда от успешного развития и внедрения новых технологий зависит эффективность и скорость развития экономики и общества). Конечно, важно учитывать и ключевое отличие "облачных сервисов" от нефти – первые не являются ограниченным ресурсом (хотя могут быть временно ограниченным по причине технологического отставания), не являются ресурсом материальным (хотя и основаны на физической инфраструктуре), и недостаток такого ресурса может быть восполнен со временем (в том числе за счет кибершпионажа). Поэтому, по мнению автора, "борьба" в этой сфере будет вестись именно на скорость. Тем не менее мир пока не стал свидетелем ни "цифрового кризиса", ни полного "цифрового занавеса", а пик регулирования, вероятно, еще впереди.

СПИСОК ЛИТЕРАТУРЫ / *REFERENCES*

1. Григорьевский В.В. Регулирование "облачных сервисов" как инструмент международной конкуренции: определение предметного поля. *Анализ и прогноз. Журнал ИМЭМО РАН*, 2024, № 2, сс. 41-56. [Grigoryevsky V.V. Regulating Cloud Services as a Tool of International Competition: Defining the Domain. *Analysis and Forecasting. Journal of IMEMO*, 2024, no. 2, pp. 41-56. (In Russ.)] DOI: 10.20542/afij-2024-2-41-56
2. Цветкова Н., Сытник А. Цифровое противостояние США и КНР: экономическое и политическое измерения. *Мировая экономика и международные отношения*, 2023, т. 67, № 11, сс. 15-23. [Tsvetkova N., Sytnik A. Digital Confrontation Between USA and China: Economic and Political Dimensions. *World Economy and International Relations*, 2023, vol. 67, no. 11, pp. 15-23. (In Russ.)] DOI: 10.20542/0131-2227-2023-67-11-15-23
3. Данилин И.В. Американо-китайская технологическая война через призму технонационализма. *Пути к миру и безопасности*, 2021, № 1(60), сс. 29-43. [Danilin I.V. The U.S.–China Technological War Through the Prism of Techno-Nationalism. *Pathways to Peace and Security*, 2021, no. 1(60), pp. 29-43. (In Russ.)] DOI: 10.20542/2307-1494-2021-1-29-43
4. Schulze M., Voelsen D. Digital Spheres of Influence. Lippert B., Perthes V., eds. *Strategic Rivalry Between United States and China*. Berlin, Stiftung Wissenschaft und Politik, 2020, pp. 30-34. DOI: 10.18449/2020RP04
5. Панкова Л.В., Гусарова О.В. Перспективные технологии стратегического уровня. Арбатов А.Г., Богданов К.В., Гусарова О.В., Евтодьева М.Г., отв. ред. *Международная безопасность: новый миропорядок и технологическая революция*. Москва, Весь Мир, 2023, сс. 162-178. [Pankova L.V., Gusarova O.V. Promising Strategic Technologies. Arbatov A.G., Bogdanov K.V., Gusarova O.V., Evtodieva M.G., eds. *International Security: The New World Order and Technology Revolution*. Moscow, Ves' mir, 2023, pp. 162-178. (In Russ.)]
6. Romashkina N.P. Information and Communication Technology and International Security. Romashkina N.P., Markov A.S., Stefanovich D.V., eds. *Information Technologies and International Security*. Moscow, IMEMO, 2023, pp. 12-33. DOI: 10.20542/978-5-9535-0613-7
7. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: "новая биполярность" в "сетевом обществе". *Вестник международных организаций*, 2021, т. 16, № 23, сс. 7-33. [Degterev D.A., Ramich M.S., Piskunov D.A. U.S. & China Approaches to Global Internet Governance: 'New Bipolarity' in Terms of 'The Network Society'. *International Organisations Research Journal*, 2021, vol. 16, no. 3, pp. 7-33. (In Russ.)] DOI: 10.17323/1996-7845-2021-03-01
8. Рамич М.С., Пискунов Д.А. Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов. *Вестник РУДН. Международные отношения*, 2022, № 22(2), сс. 238-255. [Ramich M.S., Piskunov D.A. The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes. *Vestnik RUDN. International Relations*, 2022, vol. 22, no. 2, pp. 238-255. (In Russ.)] DOI: 10.22363/2313-0660-2022-22-2-238-255
9. Fratini S., Hine E., Novelli C., Roberts H., Floridi L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *SSRN Electronic Journal*, January 2024, pp. 1-30. DOI: 10.2139/ssrn.4816020

10. Creemers R. China's Conception of Cyber Sovereignty. Broeders D., Berg B.V.D., eds. *Governing Cyberspace: Behavior, Power and Diplomacy. Digital Technologies and Global Politics*. Lanham, Rowman & Littlefield, 2020, pp. 107-142. DOI: 10.2139/ssrn.3532421
11. Creemers R. China's Cybersecurity Regime: Securing the Smart State. *SSRN Electronic Journal*, March 2022, pp. 1-38. DOI: 10.2139/ssrn.4070682
12. Григорьевский В.В., Дегтерев Д.А., Пискунов Д.А., Прохоренко И.Л. Международная политэкономия ИКТ-индустрии. *Мировая экономика и международные отношения*, 2023, т. 67, № 3, сс. 5-19. [Grigoryevsky V.V., Degterev D.A., Piskunov D.A., Prokhorenko I.L. International Political Economy of ICT Industry. *World Economy and International Relations*, 2023, vol. 67, no. 3, pp. 5-19. (In Russ.)] DOI: 10.20542/0131-2227-2023-67-3-5-19
13. Григорьевский В.В. Kuberpolitik – власть в цифровую эру. *Вестник Санкт-Петербургского университета. Международные отношения*, 2024, № 3, в печати. [Grigoryevsky V. Kuberpolitik – Power in the Digital Age. *Vestnik Sankt-Peterburgskogo universiteta. Mezhdunarodnye otnoshenija*, 2024, no. 3, in press. (In Russ.)]
14. Schwartz P. *The Art of the Long View: Planning for the Future in an Uncertain World*. New York, London, Toronto, Sydney, Auskland, Crown, 2012. 288 p.
15. Ringland G. *Scenario Planning*. United Kingdom, Action Publishing Technology Limited, 2014. 492 p.
16. Fahey L., Randall R.M. *Learning from the Future: Competitive Foresight Scenarios*. Germany, Wiley, 1998. 446 p.
17. Kushwaha N., Roguski P., Watson B.W. Up in the Air: Ensuring Government Data Sovereignty in the Cloud. Jančárková T., Lindström L., Signoretti M., Tolga I., Visky G., eds. *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*. Tallinn, NATO CCDCOE Publications, 2020, pp. 43-62. Available at: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed 10.09.2024).
18. Sukumar A.M. 'Responsibility to Detect?': Autonomous Threat Detection and Its Implications for Due Diligence in Cyberspace. Jančárková T., Visky G., Winther I., eds. *14th International Conference on Cyber Conflict. Keep Moving*. Tallinn, NATO CCDCOE Publications, 2022, pp. 173-188. Available at: https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf (accessed 10.09.2024).
19. Gjesvik L., Bryhni H., Schia N.N., Khanyari A.L., Arouna A. Digital Supply Chain Dependency and Resilience. Jančárková T., Giovannelli D., Podiņš K., Winther I., eds. *15th International Conference on Cyber Conflict. Meeting Reality*. Tallinn, NATO CCDCOE Publications, 2023, pp. 141-160. Available at: https://ccdcoe.org/uploads/2024/05/CyCon_2023_book_print.pdf (accessed 10.09.2024).
20. Игнатов А., Зиновьева Е. *"Цифровой суверенитет" в повестке объединения БРИКС*. Российский совет по международным делам. 24.01.2024. [Ignatov A., Zinovieva E. *BRICS Agenda for Digital Sovereignty*. Russian International Affairs Council. 24.01.2024. (In Russ.)] Available at: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/ (accessed 29.02.2024).
21. Wilkinson I. *What Is the UN Cybercrime Treaty and Why Does It Matter?* The Royal Institute of International Affairs (Chatham House)*. 04.08.2023. Available at: http://web.archive.org/web/20240803233333/https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter (accessed 19.02.2024).

* Деятельность организации признана Минюстом РФ нежелательной на территории Российской Федерации.