

УДК 34

## КИБЕРБЕЗОПАСНОСТЬ И «ЦИФРОВОЙ СУВЕРЕНИТЕТ»: ОПЫТ КИТАЯ И ГЛОБАЛЬНЫЕ ПЕРСПЕКТИВЫ

**Гришко Степан Викторович**

Студент магистратуры,

Российская академия народного хозяйства и государственной службы

при Президенте РФ, город Москва

В статье рассматривается подход Китая к обеспечению кибербезопасности и формированию цифрового суверенитета в контексте глобальной цифровой трансформации. Анализируются ключевые законодательные акты и политические инициативы Китая, направленные на защиту национальных интересов в киберпространстве. Автор отмечает, что внедрение киберсуверенитета в Китае происходит через построение «Великого китайского файрвола» – системы фильтрации и цензуры, блокирующей доступ к иностранным веб-сайтам, социальным сетям и приложениям, которые правительство считает нежелательными. Оценивается влияние китайской модели киберуправления на развивающиеся страны и ее противоречия с западными подходами, основанными на принципах открытого интернета и свободы информации.

**Ключевые слова:** кибербезопасность, цифровой суверенитет, Китай, киберпространство, информационная безопасность, киберуправление, цифровая экономика, правовое регулирование, международные отношения, Цифровой Шелковый путь, цензура, интернет, развивающиеся страны.

\*\*\*\*\*

В современном мире вопрос обеспечения безопасности (в том числе кибербезопасности, цифровой безопасности) приобретает все большее значение в связи с растущим влиянием компьютерных систем и Интернета на все сферы жизни, развитием беспроводных сетей, систем искусственного интеллекта. При очевидных преимуществах цифровых технологий их повсеместное внедрение может стать причиной серьезных проблем, связанных с информационной безопасностью. Уязвимость данных, утечка конфиденциальной информации и дезинформации, направленной на манипулирование общественным мнением и подрыв доверия к институтам власти, а также киберпреступность в целом – все это требует внедрение комплексных стратегий, сочетающих в себе технологические решения, законодательные инициативы и просветительскую работу среди населения. В данном контексте важно обратиться к опыту Китая, который на пути правовой регламентации вопросов цифровой безопасности достиг определенных успехов.

Очевидно, что Китай стремится к созданию «цифрового суверенитета», где государство выполняет ключевую роль в защите национальных интересов в киберпространстве. Принятие ряда нормативно-правовых актов свидетельствует о стратегическом приоритете, отдаваемом китайским руководством обеспечению контроля над цифровым пространством. Среди них – Закон о кибербезопасности Китайской Народной Республики (中华人民共和国网络安全法), Закон Китайской Народной Республики о защите персональных данных (中华人民共和国个人信息保护法), Закон о безопасности данных Китайской Народной Республики (中华人民共和国数据安全法), а также положения и правила, касающиеся сферы регулирования цифровых платформ [1, с. 159].

Помимо нормативно-правового регулирования, Китай активно развивает собственную технологическую инфраструктуру, стремясь к технологической независимости в ключевых областях, таких как полупроводники, программное обеспечение и искусственный интеллект. Инвестиции в развитие отечественных технологий направлены на снижение зависимости от зарубежных поставщиков и укрепление позиций китайских компаний на мировом рынке. Реализация концепции «цифрового суверенитета» также предполагает активное участие государства в управлении цифровыми платформами и контроле над контентом, что выражается в жесткой цензуре информации и ограничении доступа к запрещенным веб-сайтам и приложениям, блокировке популярных западных платформ, таких как Google, Facebook и Twitter [6, с. 146].

В отличие от китайского подхода, где доминирует централизованное управление киберпространством, в западных странах акцент делается на децентрализованную модель, предполагающую активное участие различных частных лиц и организаций в развитии и формировании цифровой среды. Китайское правительство рассматривает эту модель как потенциальную угрозу своему государственному суверенитету и контролю над информационным пространством, опасаясь, что неконтролируемое распространение информации и свобода выражения мнений в интернете могут подорвать стабильность и политическую систему страны. В связи с этим Китай стремится к созданию суверенного киберпространства, огражденного от влияния западных идеологий и ценностей.

В своем исследовании М. А. Егорова отмечает, что «подход Китая к киберуправлению привлекателен для ряда развивающихся стран. Некоторые страны, не входящие в западный блок, предпочитают Интернет, основанный на «незападных» стандартах и ценностях. В частности, развивающиеся страны расценивают Интернет как способ колонизации со стороны западных стран. Ведь именно с помощью информационно-коммуникационных технологий на рынок могут зайти цифровые гиганты, внося свои коррективы в экономическую жизнь страны» [3, с.17]. В этой связи, концепция «киберсуверенитета», продвигаемая Китаем, находит все больше сторонников среди государств, опасющихся цифровой зависимости от западных технологий и стремящихся к большей автономии в киберпространстве [5, с. 254]. Однако, подобный курс на «цифровой суверенитет» порождает ряд вызовов и противоречий со стороны западных стран, которые утверждают, что китайская модель киберсуверенитета ограничивает свободу слова и доступ к информации, а также создает барьеры для развития глобальной цифровой экономики. В ответ Китай парирует обвинения, заявляя о вмешательстве во внутренние дела и подчеркивает, что его политика направлена на защиту национальной безопасности, акцентируя внимание на том, что суверенитет в цифровой сфере ничем не отличается от суверенитета в физическом мире и является необходимым условием для независимого развития страны.

Таким образом, следует предполагать, что внутренняя стабильность для Китая – это не просто вопрос политического спокойствия, но и фундаментальная основа для экономического роста и социального развития. Коммунистическая партия Китая рассматривает любой потенциальный источник нестабильности, будь то политическое инакомыслие, социальные волнения или экономические потрясения, как прямую угрозу своему правлению и, следовательно, стабильности всей страны. Стремление к цифровому суверенитету, несмотря на все вызовы, вероятно, будет оставаться одним из ключевых приоритетов Китая в ближайшие годы. Это обусловлено стратегическими амбициями страны, опасениями касательно национальной безопасности и желанием играть более весомую роль в глобальной цифровой экономике. Вопрос лишь в том, какие методы и подходы будут использоваться для достижения этой цели, и какое влияние это окажет на будущее глобальной цифровой экосистемы.

---

**Список использованных источников**

---

1. Гун Нань. «Защита персональных данных в Китае: законодательство в цифровую эпоху» // Вестник Санкт-Петербургского университета. – 2023. – №1. – С. 159–172.
2. 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. – № 3 (16). – С. 7–33.
3. Егорова М.А. Китайская концепция киберсуверенитета и ее значение для правового регулирования искусственного интеллекта и обеспечения информационно-психологической безопасности в условиях защиты конкуренции // Предпринимательское право. – 2024. – № 3. – С. 17–26.
4. Ковригин Д.Э. Границы государственного суверенитета национального сегмента киберпространства // Власть. – 2023. – № 1. – С. 124–129.
5. Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. – 2021. – № 2 (23). – С. 254–264.
6. Сахаров А.Г., Шелепов А.В. Политика Китайской Народной Республики в сфере регулирования цифровых платформ // Вестник международных организаций. – 2024. – № 2. – С. 145–160.
7. Янькова А.Д. Архитектура концепции киберсуверенитета КНР (по материалам докладов Всемирной интернет-конференции «Киберсуверенитет: теория и практика») // Проблемы Дальнего Востока. – 2023. – № 4. – С. 1–14.

---

**CYBERSECURITY AND DIGITAL SOVEREIGNTY:  
CHINA'S EXPERIENCE AND GLOBAL PROSPECTS**

---

**Grishko S.V.**

This article examines China's approach to cybersecurity and digital sovereignty in the context of global digital transformation. It analyzes key Chinese laws and policy initiatives aimed at protecting national interests in cyberspace. The author notes that cyber sovereignty in China is being implemented through the construction of the "Great Firewall" – a filtering and censorship system blocking access to foreign websites, social media, and applications deemed undesirable by the government. The article also assesses the impact of China's cyber governance model on developing countries and its contradictions with Western approaches based on the principles of an open internet and freedom of information.

**Keywords:** Cybersecurity, digital sovereignty, China, cyberspace, information security, cyber governance, digital economy, legal regulation, international relations, Digital Silk Road, censorship, internet, developing countries.