

Роль высокотехнологичных ТНК в обеспечении национальной безопасности КНР

Научный руководитель – Воронкова Людмила

Чэнь Цзыхао

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет глобальных процессов, Направление геополитики и дипломатии, Москва, Россия

E-mail: hao5813263@gmail.com

В последние годы страны всего мира уделяют все больше внимания вопросам национальной безопасности, в том числе в рамках функционирования общей системы государственного управления. В процессе обеспечения национальной безопасности государства все более важную роль играют высокотехнологичные транснациональные компании - ТНК. Огромное влияние этих корпораций на сферу национальной безопасности такой крупной страны как КНР вынуждает ее правительство уделять особое внимание вопросам сотрудничества с ТНК.

Автор приходит к выводу, что высокотехнологичные транснациональные компании КНР, обладая мощным научно-исследовательским и технологическим потенциалом, распространяют свое технологическое господство как внутри страны происхождения, так и за рубежом, обеспечивая при этом национальную безопасность Китая.

С тех пор как общая концепция национальной безопасности КНР стала рассматриваться с идеологической и теоретической точки зрения, ее принципы постоянно трансформировались и совершенствовались. Принципы национальной безопасности с китайской спецификой основаны на исторических и культурных традициях, особенностях социально-политической системы Китая, но с учетом успешного мирового опыта.

Сущность национальной безопасности - это целый комплекс проблем, стоящих перед обществом, и решать их надо, опираясь на исторический опыт как своей страны, так и других государств [4].

В современных условиях понятие безопасности заметно расширилось. С развитием современных коммуникационных и сетевых технологий информационная безопасность от простой безопасности связи и безопасности сигналов перешла в компьютерную безопасность. В информационную эпоху информационная безопасность быстро распространилась через военную область на все аспекты общественной жизни [1].

В настоящее время государства входят в новый технологический цикл и появляются новые технологические вызовы, например, кибервызовы, связанные с кибербезопасностью, угроза терроризма в технологической среде. Киберпространство представляет собой искусственную виртуальную среду, с помощью которой соединены устройства, расположенные в различных государствах, и его структура может меняться [6]. Кроме того, именно киберпространство расширило возможности влияния негосударственных акторов на мировую политику, что создало новые вызовы для национальной безопасности стран мира [7].

В отличие от крупных компаний США, которые стремятся к международной экспансии и гегемонии, преследуя при этом собственные цели, крупные ТНК Китая в сфере высоких технологий стремятся поддерживать глобальную безопасность и строить сообщество с общим будущим для человечества [5]. Поскольку высокотехнологичные компании КНР

быстро стали доминирующими производственными и технологическими компаниями в мире, влияние Китая на процессы по обеспечению глобальной безопасности также резко возросло, что вызвало повышенную озабоченность в Соединенных Штатах и создало новое поле битвы для жесткой конкуренции двух стран в технической области [2].

Вызовы для системы безопасности страны в данный момент имеют комплексный характер, они могут представлять угрозу стабильности государственному устройству, внутренней жизни государства, в связи с чем правительство КНР усилило надзор и управление приложениями. Так, в статье 35 Закона о кибербезопасности КНР прямо указано, что если высокотехнологичные ТНК критически важной информационной инфраструктуры приобретают сетевые продукты и услуги, которые могут повлиять на национальную безопасность, они должны пройти проверку Национальной администрации киберпространства Китая [3].

Соответствующие компетентные органы КНР также сформулировали ряд ограничений для работы приложений. В КНР стоит отметить такие крупные китайские высокотехнологичные компании как Huawei, ZTE, Alibaba, Inspur, Aमेg и др., которые оказывают влияние на систему национальной безопасности. Данные высокотехнологичные компании ввели соответствующие стандарты кибербезопасности, которые охватывают безопасность программного обеспечения, безопасность оборудования, безопасность услуг, безопасность процесса разработки и т. д. Среди них технический обзор в основном относится к анализу рисков безопасности, основанном на аудите исходного кода, тестировании на проникновение и других технологиях.

Таким образом, транснациональные корпорации как действующие субъекты, обладающие значительным влиянием в сфере международной торговли и международных инвестиций, особенно высокотехнологичные ТНК, играют ключевую роль в обеспечении национальной безопасности КНР. Очевидно, что государственное регулирование транснациональных корпораций в КНР будет продолжаться, способствуя защите национальных интересов и обеспечению национальной безопасности. В современных условиях ведущим предприятиям высокотехнологичных отраслей Китая необходимо перейти к конкурентным отношениям с экономически развитыми странами, в том числе представителями ТНК, и развивать взаимовыгодное сотрудничество со всем миром, постепенно избавляясь от зависимости от зарубежных технологий.

Источники и литература

- 1) Ли Мэнган, Исследования по вопросам национальной информационной безопасности, Пекин: Издательство литературы по общественным наукам, 2012: 21 // [U+674E] [U+5B5F] [U+521A] . [U+56FD] [U+5BB6] [U+4FE1] [U+606F] [U+5B89] [U+5168] [U+95B8]
- 2) «Разработка новых технологических стандартов стала игрой между США и Китаем» Еще одно поле битвы Разработка новых технологических стандартов стала еще одним ключевым полем битвы в игре между США и Китаем [U+FF09] [U+300A] [U+65B0] [U+5174] [U+6280] [U+672F] [U+6807] [U+51C6] [U+5236] [U+51C6] [U+5F00] [U+53D1] [U+65B0] [U+6280] [U+672F] [U+6807] [U+51C6] [U+6210] [U+4E3A] [U+7F81] [s://www.voachinese.com.translate.google/a/china-tech-standards/6488171.html?_x_tr_sl=aut](https://www.voachinese.com.translate.google/a/china-tech-standards/6488171.html?_x_tr_sl=aut)
- 3) Сердюк А. В., Бреслер М. Г., Сулейманов А. Р. Специфика регулирования it-индустрии в Китае: история и современность // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. – 2021. – №. 4 (38). – С. 53-62.

- 4) Цзя Цинго. Размышления о характеристиках национальной безопасности и принципах ее управления. // Журнал Международные исследования в области безопасности. 2022. Т.40. № 1. С. 4- 25. [U+8D3E] [U+5E86] [U+56FD]. [U+5BF9] [U+56FD] [U+5BB6] [U+5B89] [U+5168] [U+7279] [U+70B9] [U+4E0E] [U+6CBV] [U+7400] // [U+300A] [U+56FD] [U+9645] [U+5B89] [U+5168] [U+7814] [U+7A76] [U+300B]. 2022. Т.40. № 1. С. 4-25.
- 5) Юань Пэн. Стратегическое мышление на пути национальной безопасности с китайской спецификой // Исследования национальной безопасности. 2022. № 1. С.7-23. [U+8881] [U+9E4F]. [U+5173] [U+4E8E] [U+4E2D] [U+56FD] [U+7279] [U+8272] [U+56FD] [U+5BB6] [U+5B89] [U+5168] // [U+300A] [U+56FD] [U+5BB6] [U+5B89] [U+5168] [U+7814] [U+7A76] [U+300B] 2022 [U+5E74]
- 6) Ebert H., Maurer T. Contested Cyberspace and Rising Powers // Third World Quarterly. 2013. Vol. 34. Iss. 6. P. 1054-1074.
- 7) Nye J.S. Jr. Nuclear Lessons for Cyber Security // Strategic Studies Quarterly. 2011. Vol. 5. Iss. 4. P. 9-20.