Отзыв официального оппонента
на диссертационную работу Цуканова Леонида Вячеславовича
на тему «Сотрудничество монархий Персидского залива в области кибербезопасности: особенности, проблемы, тенденции», представленную к защите на соискание ученой степени кандидата политических наук по специальности 5.5.4 - международные отношения. глобальные и региональные исследования

Представленная к оппонированию диссертация посвящена, несомненно, важной и весьма актуальной проблеме политики государств ССАГЗ в сфере кибербезопасности. Несмотря на то, что нарастающая значимость процессов цифровизации в мировой политике вообще и в регионе Ближнего Востока, в частности, никаких сомнений не вызывает, а сама активная деятельность государств Персидского залива в цифровой сфере привлекает все большее внимание, нельзя сказать, что в научном плане эти вопросы часто становятся предметом серьезного изучения. Справедливости ради, за исключением автора диссертации и его научного руководителя, не помню, чтобы еще кто-то из российских ближневосточников (не считая нескольких исламоведов, занимающихся весьма специфическими аспектами вопросов кибербезопасности) серьезно занимался этой темой.

Таким образом, ни актуальность, ни научная новизна работы никаких сомнений не вызывают.

Сама работа производит прекрасное впечатление – она хорошо написана, фундирована, логична, приведенный в ней анализ интересен, вообще, она отличается одновременно и свежестью, и серьезностью взгляда.

Во Введении очень хорошо описан раздел «степень научной разработанности», он демонстрирует глубокое знание автором историографии рассматриваемой проблемы, а также его знакомство с широким кругом литературы по смежным с непосредственно изучаемой проблематикой вопросам. Библиография к диссертации насчитывает более 300 наименований, что также говорит о серьезной проработке темы.

Заявленная цель исследования – «выявление основных направлений и особенностей международного сотрудничества монархий Залива в сфере

кибербезопасности» – сформулирована весьма четко, что, к сожалению, не всегда бывает даже в хороших работах. Формулировка задач, объекта и предмета исследования вопросов не вызывают.

Вполне достойно описана методология исследования. Ее общие параметры приводятся во Введении к работе, а более частные рассматриваются в первой главе.

Источниковая база достаточна для исследования темы, хотя обзор источников во Введении мог бы быть и более подробным и включать в себя их критический анализ, а не только перечисление по группам.

Прекрасно показана научная новизна исследования.

Наконец, что касается общих вводных разделов, нет никаких сомнений и в высокой степени апробированности исследования – за время его подготовки автор зарекомендовал себя как талантливого и активного специалиста на самых разных академических и аналитических площадках.

Первая глава диссертации носит, в целом, вводный характер. Она посвящена обзору концептуальных подходов к исследованию международной информационной безопасности. В ее первом параграфе автор рассматривает вопрос о кибербезопасности как предмете политического анализа. При этом он довольно подробно освещает различные теоретические, концептуальные, терминологические подходы к вопросам кибербезопасности, информационной безопасности, киберугроз и т.п., разрабатываемые различными государствами, международными организациями и экспертными сообществами, в том числе и с учетом их политических интересов. Появление этого параграфа в структуре работы видится вполне естественным, а знакомство автора с многообразными теоретическими спорами по вопросам кибербезопасности демонстрирует его глубокое знание теоретических аспектов проблемы. Вместе с тем, параграф оставляет впечатление некоторой избыточности – не всегда понятно, насколько изложенный в нем материал необходим для адекватного решения тех научных задач, что были поставлены во Введении. Впрочем, грех избыточности здесь едва ли существенен – понятно, что диссертанту хотелось поделиться с

читателем всем тем, что он знает о теоретических вопросах, чтобы не нести эту ношу в одиночестве, разделяя ее лишь с научным руководителем.

Во втором параграфе первой главы Л.В. Цуканов вновь обращается к методологическим основам исследования. Здесь он более подробно, нежели во введении, рассматривает различные теории неореализма и их применимость к исследованию международного взаимодействия в киберсфере на Ближнем Востоке. Отдельно он касается возможности применения конструктивистских подходов, выделяя среди них теорию «сетевого общества». Автору удалось удачно экстраполировать теоретические подходы, в принципе, направленные скорее на изучение традиционных угроз безопасности, на цифровую сферу. Несколько неясным, при этом, остается то, почему была избрана именно неореалистическая парадигма анализа. Содержащееся здесь утверждение, будто она обладает наиболее эффективным методологическим инструментарием, никак не доказывается, поскольку сравнений с другими подходами не проводится. Более того, исходя из текста, складывается впечатление, что подходы конструктивистов могут быть и более эффективными. Впрочем, выбор методологии – дело автора, и выбор этот вовсе не обязательно должен доказываться.

Вторая глава исследования – на мой субъективный взгляд самая интересная – посвящена трендам развития национальных систем кибербезопасности монархий Залива. В первом ее параграфе рассматриваются те конкретные вызовы и угрозы, с которыми сталкиваются эти страны в условиях цифровизации. Автор, в сущности, ограничивает здесь свой анализ рассмотрением непосредственных киберугроз с учетом высокой степени международной напряженности и множества региональных конфликтных ситуаций, в которые вовлечены изучаемые страны. Описание этих угроз, их перечисление, конкретные данные по деятельности государств региона в сфере укрепления кибербезопасности и наращивания наступательного потенциала с использованием цифровых технологий читать весьма интересно. Здесь представлен и хорошо проанализирован богатый источниковый материал,

содержится много интересной эмпирической информации, а предлагаемый анализ весьма разумен и, кажется, точен.

Далее Л.В. Цуканов обращается к вопросу об уровне готовности государств ССАГЗ к отражению киберугроз, который он определяет по методологии, разработанной экспертами ООН в рамках международного научно-исследовательского проекта «Глобальный индекс кибербезопасности». Такой подход возможен, но, конечно, нуждается в обосновании.

Очень интересен раздел, посвященный запросу на коллективные меры в обеспечении киберугроз. Выделенные автором стимулы к наращиванию коллективных действий на этом направлении не просто хорошо обоснованы, но и демонстрируют высокий профессионализм диссертанта в области аналитики.

Третья глава исследования сконцентрирована на основных направлениях международного сотрудничества стран ССАГЗ в кибербезопасности. Ее первый раздел, посвященный региональным площадкам взаимодействия, к которым автор, помимо ССАГЗ и ЛАГ, относит почему-то и ОИС, в целом серьезных возражений не вызывает. Общий вывод автора, состоящий в том, что «декларируемый монархиями Залива курс на развитие коллективной системы кибербезопасности в рамках ССАГЗ еще далек от реализации его на практике» (с. 137), конечно, может относиться не только к рассматриваемой сфере взаимодействия, но и едва ли не к любой другой. Вместе с тем, интересное наблюдение касается новой роли ЛАГ как ключевой площадки взаимодействия, на которой «формируется общая для всех арабских стран повестка кибербезопасности» (с. 138). Возможно, если автор прав, то нам стоит обратить большее внимание на динамику развития ЛАГ, которая последние годы обычно описывается исключительно в пессимистических тонах.

Рассматривая военное сотрудничество в сфере кибербезопасности, автор собрал, вероятно, максимально возможные данные, доступные по открытым источникам. Общие выводы, как и в других разделах исследования, вопросов не вызывают. Тем не менее, можно было бы указать на наличие внутреннего противоречия между стремлением стран региона к укреплению стратегической

автономии во всех сферах, включая технологическую, и в то же время в существовании запроса (особенно продвигаемого внешними акторами) на интенсификацию регионального сотрудничества в военной сфере, включая кибербезопасность. Понятно, что эти цели требуют подчас прямо противоположенных линий поведения.

Далее диссертант предлагает обзор деятельности внерегиональных акторов в формировании безопасной цифровой среды в аравийских монархиях. Обзорный характер этого параграфа не позволяет говорить о недостаточной проработанности некоторых аспектов затронутой проблематики. Конечно, если бы речь шла о серьезном анализе этой деятельности, то нужно было бы посмотреть и ее нормативно-правовую базу в каждом из государств, ее цели, как политические, так и военно-политические и экономические и т.д., и т.п. Однако подобный подход потребовал бы написания еще одной (или не одной) диссертации, и потому диссертант вполне правомерно ограничился кратким обзором с вполне логичными выводами.

В заключительном параграфе диссертации Л.В. Цуканов прибегает к SWOT анализу перспектив и рисков развития кооперации в киберсфере, после чего предлагает три сценария дальнейшего развития ситуации. Анализ проведен прекрасно, что же касается сценариев, то они вполне правомерны, хотя оценка их вероятности довольно произвольна, а сам их характер носит настолько общий характер, что не может быть подвергнут существенной критике. Опять-таки, если бы речь шла о серьезном прогнозировании, то требовалось бы более подробно проработать вопросы, затронутые в предыдущем разделе.

Выводы по работе отвечают поставленным цели и задачам. Они обоснованы и интересны.

Работа сопровождается весьма интересными и полезными приложениями, составленными автором.

При всех несомненных достоинствах представленного текста, относительно него могут быть сделаны некоторые критические замечания, по большей части, впрочем, носящие дискуссионный характер.

Так, спорным кажется встречающиеся на с. 4 утверждения: «Необходимость адаптироваться к цифровым реалиям стала одной и главных причин запуска стратегических программ экономической диверсификации «Видение» и, как следствие, форсированного строительства национальных систем киберзащиты» и: «Сегодня сектор кибербезопасности обеспечивает аравийские монархии… эффективными инструментами продвижения к технологическому суверенитету».

При всем уважении к сфере цифровизации, стратегические проекты развития государств Залива все же запущены были не из-за ее развития, а из-за необходимости стран адаптироваться к новым социально-экономическим условиям (урбанизация, рост населения, модернизация обществ, ожидаемое сокращение углеводородных ресурсов и т.д.). Вообще, в работе много раз «Видения» определяются как стратегические документы, направленные на диверсификацию экономик. Однако, это не совсем так – экономические аспекты этих документов, конечно, существенны, но цели их принятия носят более фундаментальный характер – они направлены (в случае с КСА и ОАЭ) на переустройство обществ или (в случае с Оманом) на «защиту оманской личности» от негативных внешних влияний.

Кроме того, фигурирующее в приведенной цитате понятие «технологического суверенитета» до сих пор не вполне концептуализировано, а, учитывая зависимость НТР стран Залива от внешних акторов, их стремление к такому суверенитету вовсе неочевидно, тем более что тут же говорится о глубокой вовлеченности изучаемых стран в международные научно-технологические связи.

Далее. Ссылаясь на Е.С. Мелкумян автор пишет: «Масштабные преобразования ожидаемо оказали заметное влияние на трансформацию внешнеполитических приоритетов аравийских монархий, что нашло отражение

в форсированном расширении связей с передовыми технологическими державами мира, прежде всего США, КНР, Республикой Корея и др.». Мне представляется ставить трансформацию внешнеполитических приоритетов монархий в зависимость от задач диверсификации экономик – это существенное упрощение. Полагаю, что как внешняя политика со всеми ее изменениями, так и задачи развития монархий подчиняются общей логике укрепления собственной безопасности. В то же время возникает вопрос, насколько существенна эта трансформация внешнеполитических связей? Со всеми упомянутыми в цитате государствами отношения развивались и ранее. Тем более сомнительно здесь упоминание партнеров стран ССАГЗ именно как технологических держав – научно-технологическая зависимость от передовых в этой сфере государств и без того была характерна для стран ССАГЗ еще до разработки всяких «Видений».

Перечисляя киберугрозы во второй главе, возможно, стоило бы упомянуть и косвенные вызовы, связанные с быстрой цифровизацией. Среди них – трансформация социальных структур и возникновение новых социальных и политических сообществ, консолидирующихся на цифровых платформах. Кстати, характерно, что согласно данным в параграфе 2.3 сами власти стран ССАГЗ такого рода вызовы учитывают в своей нормативно-правовой базе.

Представляется, что, если автор продолжит разработку темы исследования, ему стоило бы уделить несколько большее внимание изучению нормативно-правовой базы и институциональному дизайну деятельности государств в сфере кибербезопасности. В частности, верно отмечая недостатки ее жесткого «вертикального» регулирования, автор не задается вопросах о его причинах.

Кроме того, во второй главе было бы уместно более четко определить расхождения государств ССАГЗ в политике в цифровой сфере, тем более учитывая избранный неореалистический методологический подход к исследованию.

При рассмотрении деятельности ССАГЗ автор отмечает множество ослабляющих эту организацию противоречий. Однако, как мне представляется,

было бы верно продемонстрировать сначала базовые расхождения между членами ССАГЗ по наиболее важным для них вопросам, и только потом переходить к исследованию роли вопросов цифровизации в этой общей повестке дня.

Как можно видеть по характеру сделанных замечаний, все они носят частный характер и, по большей части, означают разные взгляды автора диссертации и его оппонента на какие-то отдельные аспекты регионального развития. Общего впечатления о работе, разумеется, они никак не портят.

Диссертационная работа «Сотрудничество монархий Персидского залива в области кибербезопасности: особенности, проблемы, тенденции» соответствует требованиям п.9 «Положения о присуждении ученых степеней в УрФУ», а ее автор – Цуканов Леонид Вячеславович – заслуживает присуждения ученой степени кандидата политических наук по специальности 5.5.4 - международные отношения, глобальные и региональные исследования.

Официальный оппонент:

Доктор политических наук, заместитель директора ФГБУН Институт востоковедения РАН по научной работе, заведующий Центром арабских и исламских исследований ИВ РАН

Кузнецов Василий Александрович

Адрес: Россия, Москва, ул. Рождественка, 12/1, тел. +79163431003, cais@ivran.ru

13 июня 2024 г.