Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра международных отношений
и внешней политики России

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТРАТЕГИЙ КНР И США В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 442 группы
направления 41.03.05 «Международные отношения»
Института истории и международных отношений

Сейрановой Софьи Норайровны

Научный руководитель
кандидат исторических наук, доцент _____ Лапенко М.В.
подпись, дата

Зав. кафедрой
доктор исторических наук, профессор _____ Голуб Ю.Г.
подпись, дата

Саратов 2018

Введение. Актуальность данной темы обусловлена тем, что в настоящее время международные отношения приобретают качественно новый характер из-за развития ИКТ и поэтому государства начинают проводить активную политику в киберпространстве. Информационные технологии дали положительный толчок к развитию стран, с их помощью происходит цифровизация экономики, которая помогает в принципе менять всю модель экономических отношений и выводить ее на более высокий уровень, культурное взаимодействие усиливается благодаря постоянному, беспрерывному информационному обмену между странами, отмечается что развитие ИКТ является движущей силой такого важного процесса как глобализация. Однако, на ряду с положительными тенденциями развития киберпространства, существуют угрозы, которые связаны с ним, в первую очередь это кибератаки, кибершпионаж, террористы также активно используют киберсреду для вербовки и пропаганды. При анализе современной мировой политической обстановки весьма актуальным с точки зрения того как мировые державы реагируют на новые вызовы является исследование подходов КНР и США к вопросу обеспечения кибербезопасности. И это, обуславливается ролью и технологическим потенциалом данных государств на международной арене.

Цель исследования – охарактеризовать влияние киберугрозы на международную и национальную безопасность.

Данная цель конкретизировалась в следующих задачах:

- исследовать «информационные» и «кибервойны» как теоретический концпет в политической науке

- проанализировать хактивизм и кибертерроризм в контексте международной стабильности и безопасности

- изучить какую угрозу Китайской Народной Республики представляют киберугрозы

- проанализировать публикации секретных правительственных документов в киберпространстве в контексте национальной безопасности Соединенных Штатов Америки

- сравнить и проанализировать подходы КНР и США к обеспечению кибербезопасности

Разработанность темы в научной литературе. Важную роль при написании бакалаврской работы сыграли научные труды западных ученых, базирующих свои концепции на основе геополитики и политического анализа международных отношений. Г.Киссинджера[1], Э. Тоффлера[2], С. Хантингтона[3], Зб. Бжезинского[4], Ф.Махлупа[5]. В их трудах можно проследить как начало развиваться информационное общество и как государства начали использовать киберпространство в реализации своих целей. Также о том как используются новейшие технологии в реализации внешнеполитических целей написано в книге «Гибридные войны в хаотизирующемся мире XXI века», написанная под редакцией П.А. Цыганкова[6].

Важную роль при написании бакалаврской работы сыграла монография сотрудника Департамента информации и печати МИД России, кандидата политических наук А.А. Чернова «Становление глобального информационного общества: проблемы и перспективы»[7]. О действия Китайской Народной Республики в киберпространстве пишут такие исследователи как Г.Р. Ибрагимова[8], Е.В. Евдокимов[9], в их трудах можно

---

[1] Киссинджер Г. Дипломатия. – М., 1997.
[2] Тоффлер Э. Третья волна. – М., 1999.
[3] Хантингтон С. Столкновение цивилизаций. – М., 2003.
[4] Бжезинский Зб. Великая шахматная доска. Господство Америки и его геостратегические императивы. – М., 1998.
[5] Махлуп Ф. Производство и распространение знаний в США. - М.: Прогресс, 1966. – 280 с.
[6] «Гибридные войны» в хаотизирующемся мире XXI века // Под ред. П.А. Цыганкова. – М.: Издательство Московского университета, 2015. – 384 с. (Библиотека факультета политологии МГУ)
[7] Чернов А.А. Становление глобального информационного общества: проблемы и перспективы – Монография// М.: Дашков, 2003. - 232 с.
[8] Ибрагимова Г.Р. Стратегия КНР в области управления Интернетом и обеспечения информационной безопасности // Индекс безопасности. – 2013. – № 1. – URL: http://www.pircenter.org/media/content/files/10/13559074100.pdf
[9] Евдокимов Е.В. Политика Китая в глобальном информационном пространстве // Международные процессы. – 2011. – № 1 (25). – URL: http://www.intertrends.ru/twenty-fifth/009.htm

проследить как развивалась стратегия информационной войны КНР и как Пекин подходит к вопросу обеспечения кибербезопасности. Также о развитии интернета в Китае пишет Инкстер Н.[1]. В свою очередь С.В. Старкин[2], М.Картер[3] пишут о кибербезопасности в США, в своих работах они отмечают какие институты создает Вашингтон для того, чтобы обеспечить кибербезопасность.

Источниковая база исследования. Особую ценность при анализе киберстратегий представили: Стратегия национальной безопасности США[4], Белые книги КНР[5], посвященные основным внешне- и внутриполитическим вопросам страны, а также стратегические документы обеих стран по проблеме обеспечения кибербезопасности: Руководящие принципы по безопасности информационных систем и сетей[6], Всеобъемлющая межамериканская стратегия кибербезопасности: многоаспектный и комплексный подход к созданию кибербезопасности[7], Конвенция о киберпреступности Совета Европы[8], Обзор политики киберпространства США: обеспечение надежной и устойчивой инфраструктуры информации и коммуникаций[9], Закон о кибербезопасности в Китае 2017[10] и др.

---

[1] Inkster N. Evolution of the Chinese Internet: Freedom and Control. – CAN: University of Lethbridge, 2016. – 33 p.

[2] Старкин С.В. Аналитические институты разведывательного сообщества США: концептуальные основы, механизмы и технологии деятельности в условиях глобализации: автореф. дис. ... д-ра полит. наук. – Н.Новгород, 2011. – 20 с.

[3] Carter M. Cyber Security. – USA: Amazon Digital Services LLC, 2016. – 10 p.

[4] The 2015 National Security Strategy (February 2015) // The White House. – URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

[5] China's Military Strategy: The State Council Information Office of the People's Republic of China (May 2015). – URL: http://eng.mod.gov.cn/Database/WhitePapers/index.htm

[6] OECD Guidelines for the Security of Information Systems and Networks // OECD. – URL: http://www.oecd.org/sti/ieconomy/15582260.pdf

[7] A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity // OAS. – URL: http://www.oas.org/juridico/english/cyb_pry_strategy.pdf

[8] Convention on Cybercrime of the Council of Europe 2001 // Council of Europe . – URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[9] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (July 2009) // The White House. – URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final.pdf

Бакалаврская работа состоит из двух глав, каждая из которых включает три параграфа.

Глава 1. Влияние киберугроз на международную безопасность и национальную безопасность отдельных стран.

Глава 2. Киберугрозы в контексте национальной безопасности Китайской Народной Республики и Соединенных Штатов Америки.

Основное содержание работы. В параграфе 1.1 «Информационные и кибервойны как инструмент деструктивного влияние в современной политике» говорится о том, что в настоящее время на смену традиционным войнам из-за развития ИКТ пришли кибервойны. Также говорится о том, что информационные войны это далеко не новое явление, но на сегодняшний день, по мнению многих экспертов, информационная безопасность является одной из самых неразвитых сфер безопасности в современном мире и поэтому, безусловно, нужно изучать данную область для того, чтобы представлялось возможным предугадывать действия государств в глобальном информационном пространстве. Нельзя игнорировать тот факт, что в настоящее время ведутся настоящие кибервойны за господство в информационном поле, что безусловно требует пристального внимания к данной сфере общества, т.к. уже сейчас многие эксперты предполагают, что Третья мировая война может развернуться именно в киберпространстве, данный факт не может не волновать. Кроме того, описывается восточная модель подхода к информационной безопасности и западная.

В параграфе 1.2. «Хактивизм и кибертероризм как новые вызовы международной стабильности и безопасности» объясняется и рассматривается хактивим как концепт в политической науке. Существуют группировки хактивистов, на сегодняшний момент их насчитывается более 100. Одной из них является Anonymous, которая в 2009 г. стала известна широкой общественности благодаря операции «Чанология», основой которой является протест против опасных действий Церкви сайентологии, проект до сих продолжается. Но в первую очередь, интересует их

деятельность в политической сфере, а она, безусловно, есть. Стоит отметить, что до группировки Anonymous политически мотивированный хакинг представлял собой спорадическую, крайне непоследовательную деятельность. Хактивисты используют незаконно цифровые данные для получения политической выгоды, часто они мотивируют это тем что борются за гражданские права, однако, просто занимаются мошенничеством. В параграфе также также говорится о том, что террористы активно используют киберпространство для вербовки и пропаганды. Также публикуются видеоролики, где террористы казнят невинных людей, жестоко обращаются с детьми, женщинами, всё это оказывает огромное давление на массовое сознание. Также террористы активно вербуют людей из разных стран в социальных сетях и оказывают сильное давление на государства. Так, в прошлом году группировка «Киберджихад» взломала аккаунты военного руководства Соединенных Штатов, была обнародована даже переписка президента. Развернулась настоящая кибервойна.

Отмечается, что многие государства уже на данный момент понимают, какой урон международной и национальной безопасности может нанести использование каким-либо государством Интернет-пространства для дестабилизации обстановки в другом государстве, такое информационное воздействие влечет за собой сбой электронных систем управления страной. Таким образом, можно нарушить такие важные системы, как энергетическая (атомная), транспортная и многие другие.

В параграфе 1.3. «Публикации секретных правительственных документ как удар по международному имиджу государства» говорится о том. Как недавние публикации Интернет-ресурса WikiLeaks нанесли серьезный ущерб имиджу США, а также обнародование секретных материалов бывшего сотрудника АНБ Эдварда Сноудена. Отмечается, что огромные потоки информации, которые льются на нас со всех сторон, формируют наше мнение и, безусловно, могут манипулировать нашим сознанием. Конечно, многие государства, понимая это, пытаются использовать

данный факт, чтобы повысить свой престиж на международной арене и в глазах мировой общественности, пытаются контролировать средства массовой информации, чтобы последние не смогли подорвать их авторитет. Но это не всегда получается. Существует множество новостных некоммерческих организаций, которые стремятся показать миру правдивую реальность. Наиболее ярким примером является WikiLeaks – проект, созданный в 2006 г. австралийским интернет-журналистом и телеведущим Джулианом Ассанжем. Ресурс специализируются на публикации секретных правительственных документов, его основная цель – донести до мировой общественности ранее скрытую информацию и новости. Конечно, говоря об утечке секретных документов, упоминается Эдвард Сноуден, технический ассистент, бывший сотрудник ЦРУ и Агентства национальной безопасности США. Опубликованные им документы разоблачают незаконную деятельность в глобальном информационном пространстве, показывают, что АНБ прослушивает почти всех мировых лидеров. Данный факт не просто наносит урон по национальной безопасности США, но и ставит под сомнение авторитет Вашингтона на международной арене.

Параграф 2.1. «Киберугрозы как серьезный вызов национальной безопасности КНР», говорится о том, что Китайская Народная Республика подходит к вопросу обеспечения информационной безопасности, со свойственной ей спецификой, которая значительно отличается от западной. По мнению аналитиков, в принципе, китайская теория информационной войны должна соответствовать китайской культуре, философии, военной стратегии. Государственный совет КНР считает, что Интернет является важной инфраструктурой государства и поэтому его нужно держать под контролем. Любое посягательство на этот внутренний сегмент принимается как угроза национальной безопасности. Для того, чтобы эффективно реализовывать меры по обеспечению информационной безопасности

правительство передало функции оборонительных и наступательных действий в киберпространстве Третьему и Четвертому штабу Национальной освободительной армии Китая (НОАК). Четвертое управление Генерального Штаба НОАК предназначено для информационного противоборства и ведения кибервойны. Его отличие от Третьего в том, что его действия имеют, в первую очередь, наступательный характер. На его базе также функционируют научно-исследовательские институты. Так, в 2011 г. была создана база, которая обеспечивает безопасность информации НОАК. Стоит отметить, что помимо данных ведомств вопросами кибербезопасности также занимается МОБ (Министерство общественной безопасности), Департамент безопасности средств связи и коммуникации. Но главную роль в обеспечении кибербезопасноти все же играет 11-е бюро МГБ (Министерства государственной безопасности).

Также в параграфе отмечается, что Пекин активно занимается кибербезопасностью и в рамках международных организаций, таких как БРИКС, АСЕАН.

Параграф 2.2. «Информационные стратегии и кибербезопасность США» - анализируются концепции информационных войн в США, приводятся примеры их реализаций. Говорится о том, что наиболее активное использование ИКТ для реализации внешнеполитических задач началось в США. В Госдепартаменте, ЦРУ и ряде других структур были созданы специальные отделы, которые должны были работать с иностранной Интернет-аудиторией для распространение нужной информации. У Вашингтона также есть своя стратегия ведения информационной войны, примером того как американцы на практике реализовывают эту стратегию могут служить события во Вьетнаме, разрабатывая психологические операции, американские психологи учли менталитет вьетнамских партизан и основной упор в пропаганде делался на психологические и социальные аспекты, а не на политику. Для морального истощения скрывающихся в джунглях вьетконговцев было организовано непрерывное вещание

пропаганды с вертолётов. При этом активно применялось эмоциональное воздействие: трансляция воплей ужаса, женского и детского плача, буддистской погребальной музыки и прочие звуковые эффекты. С развитием IT-технологий, Интернет-пространство также стало важной сферой и внутренней, и внешней политики США. Но важно сказать о том, что изначально в США сформировался подход двойных стандартов в отношении вопросов информационной войны и кибербезопасности, определявший четкий водораздел между внутренней и внешней политикой. Так, внутри страны принимались различные меры по укреплению информационной безопасности, противодействию информационному криминалу и кибертерроризму, активно велись разработки новейших информационных технологий для военного сектора, разрабатывались сценарии информационных войн и операций. При этом на международной арене США долгое время не признавали наличия комплекса угроз информационной безопасности, включавшей в себя военную составляющую. Позиция США в этой сфере сводилась к тому, что угрозы целостности и работоспособности национальной и глобальной информационной инфраструктуры в подавляющем большинстве случаев исходят от неправомерных действий в киберпространстве, а отнюдь не от военных действий одних государств против других

Параграф 2.3. «Киберстратегии КНР и США: современное состояние и тенденции развития», анализируются и сравниваются подходы двух стран к обеспечению кибербезопасности. В настоящий момент, на международной политической арене есть два полюсных подхода к вопросу обеспечения кибербезопасности и в принципе к определению информационного общества: восточный и западный. Ярким представителем восточного подхода является КНР, а западного США. Для восточного подхода, как уже ранее отмечалось в работе, характерен философский компонент, приверженность традициям, а западные специалисты в данных вопросах больше опираются на прагматичность и инновационность. Говорится о том, что китайская военная

наука в век информатизации заметно претерпела изменения, в основном это касается переоценки способов и методов эффективности ведения войны. В целом, китайская теория информационной войны находится под сильным влиянием древнего военного искусства Китая. Руководство Поднебесной пытается применить 36 стратагем войны к методам информационной войны. Целями китайских специалистов в области информационной войны становятся источники, каналы передачи и получатели информации , объекты командования, управления, связи, компьютеров и разведки, а также средства радиоэлектронной борьбы. Первыми объектами нападения, по мнению экспертов, могут стать компьютерные системы, объединяющие политические, экономические и военные объекты страны, а также общество в целом; кроме того, КНР может стремиться к поражению механизмов принятия решений для нарушения координации действий противника. Это требует разрушения когнитивных и информационных систем[1]. Подобная стратегия подразумевает, что в будущем войну будут вести не только военные, но и гражданские специалисты. Американская же концепция информационной войны, в первую очередь, основывается не на исторических фактах, хотя и они играют важную роль, а на новых идеях и инновационных технологиях. Также важно отметить, что китайская военная наука выделяет элементы информационной войны, которые заметно отличаются от классификаций, принятых в США. Это касается форм, сущности, особенностей, принципов, типов, циклов и уровней информационного противоборства. Однако, существуют и общие тенденции, которые в дальнейшем могут послужить точкой опоры для совместного сотрудничества, уже сейчас ведутся переговоры по заключению соглашения между США и КНР в области кибербезопасности

Заключение. По результатам проведенного исследования можно сделать некоторые выводы.

[1] Ибрагимова Г.Р. Стратегия КНР в области управления Интернетом и обеспечения информационной безопасности // Индекс безопасности. – 2013. – № 1. – URL: http://www.pircenter.org/media/content/files/10/13559074100.pdf

Итак, проанализировав влияние информационной революции на национальную безопасность государств, можно выделить несколько аспектов. Во-первых, посредством ИКТ государства реализуют ряд важных функций: взаимодействие на уровне всех слоев населения, а не только политических элит; использование новых коммуникационных возможностей; формирование положительного имиджа государства на международной арене. Во-вторых, информационная безопасность по-прежнему остается одной из самых неразвитых сфер безопасности, и это можно проследить на примере того, как достоянием общественности становятся секретные документы правительств. В-третьих, очевидно, что неконтролируемое использование ИКТ может нанести серьезный ущерб международной безопасности и стабильности, а также национальной безопасности отдельных государств.

Сравнительный анализ киберстратегий КНР и США показал разность подходов этих стран. В основу китайской стратегии заложены принципы древней китайской философии и военной стратегии, данный факт конечно отличает подход Поднебесной к кибербезопасности от западных держав. Китайское Интернет-пространство представляет собой сложную, многоуровневую систему, которая тщательно фильтрует информацию и отслеживает ту информацию, которая может дискредитировать власть в глазах общественности. В свою очередь Вашингтон имеет печальный опыт в обеспечении информационной безопасности, особенно после обнародования секретных данных Интернет-ресурсом WikiLeaks и бывшим сотрудником АНБ Эдвардом Сноуденом. Обе страны создают подразделения, которые занимаются кибербезопасностью. Так, еще в 2011 году правительство Китая создало 11-е бюро Министерства государственной безопасности, основная цель которого – обеспечение кибербезопасности, также в 2016 году была опубликована Стратегия кибербезопасности КНР, в которой также уделяется важное место вопросу обеспечения информационной безопасности, говорится о том, что должен быть осуществлен контроль за состоянием

киберпространства, государство должно быть готово к киберугрозам. Что касается современного состояния кибербезопасности США, то в начале мая 2018 года Киберкомандование США, входящее в Пентагон, получило нового главу и новые полномочия, что свидетельствует о растущем значении цифровых войн. При этом подразделение кибербезопасности Пентагона получило новый статус независимой «командной единицы» и таким образом впервые встало на одну доску с девятью другими боевыми подразделениями США. Это изменение свидетельствует, что «кибератаки признаны полноценными боевыми действиями». В заключении отмечается, что обе страны понимают важность обеспечения кибербезопасности как внутри государств, так и на международном уровне и поэтому готовы к конкретным решениям обеспечения кибербезопасности как в формате международных организаций и партнерских блоков, так и на двусторонней основе. Уже сейчас ведутся переговоры по заключению соглашения между США и КНР в области кибербезопасности. Это говорит о том, что государства понимают важность многостороннего обеспечения кибербезопасности в современных политических реалиях.