САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

САРДАРОВА Валерия Анатольевна

Выпускная квалификационная работа

**Вопросы кибербезопасности в американо-китайском взаимодействии**

**Cybersecurity in the US-China Interaction**

Направление 41.03.05 – «Международные отношения»,

Основная образовательная программа бакалавриата «Международные отношения»

Научный руководитель:

д.п.н., доцент кафедры американских исследований

ЛЕКСЮТИНА Я.В.

Рецензент:
к.п.н., доцент кафедры мировой политики

БОЛГОВ Р.В

Санкт-Петербург

2018

ОГЛАВЛЕНИЕ

**Введение**.........................................................................................................................................3

1. **Кибербезопасность: понятие и институциональный аспект обеспечения**
	1. Понятийно-категориальный аппарат кибербезопасности...................................12
	2. Институциональный аспект обеспечения кибербезопасности в США и КНР...........................................................................................................................16
2. **Нормативно-правовые базы США и КНР, регулирующие деятельность в киберпространстве**
	1. Правовые основы обеспечения кибербезопасности США.................................30
	2. Правовые основы обеспечения кибербезопасности КНР...................................42
3. **Противостояние и сотрудничество США и КНР в сфере кибербезопасности**
	1. Кибербезопасность как проблема в американо-китайских отношениях...........52
	2. Попытки гармонизации интересов США и Китая в области обеспечения кибербезопасности..................................................................................................63

**Заключение**.................................................................................................................................72

**Список источников и литературы**.........................................................................................74

**Введение**

**Актуальность темы**

В современных условиях развития общества и технологий невозможно отрицать тот факт, что роль информационной среды неуклонно возрастает. Киберпространство – это новый канал для создания и распространения всевозможной информации, оно стало новым двигателем роста экономики, новой платформой социального управления, новым способом международного сотрудничества, к тому же и совершенно новой областью государственного суверенитета. Однако киберпространство предоставляет нам не только ресурсы, возможности, но и затрагивает ряд вопросов. Кибербезопасность современного государства оказывает прямое влияние на все составляющие его политики. Председатель КНР Си Цзиньпин отметил, что в наши дни национальная безопасность невозможна без её кибербезопасности, а модернизация страны невозможна без её информатизации[[1]](#footnote-1).

С растущей ролью информатизации в международной политике, растут и риски, связанные с желаниями различных и государственных, и негосударственных акторов, нарушить стабильность или вовсе разрушить информационные структуры других государств. Стремительное развитие информационных технологий, которое мы можем наблюдать на сегодняшний день, приводит к тому, что огромные суммы денег, затраченные на оборону, могут не оправдать себя, если будет достаточно запустить программу, способную нарушить работу всего оборонного комплекса страны.

При наличии подобных рисков формирование собственного подхода к обеспечению кибербезопасности на сегодняшний день представляется необходимым для любого государства. Таким образом, развитие нового типа противостояния, как информационная борьба, переход гонки в технических вооружениях в киберпространство также обуславливают актуальность исследования отношений государств в области кибербезопасности.

Одним из ключевых факторов, влияющих на ход развития отношений в данной области, является отсутствие у Пекина и Вашингтона единого взгляда на формирование международных норм регулирования киберпространства, а также отсутствие общего определения «кибербезопасности». Эскалация китайско-американских споров в вопросах кибербезопасности стимулирует рост напряженности в киберпространстве в целом и провоцирует дальнейшее втягивание в гонку кибервооружений всего мирового сообщества. От кооперации или соперничества США и Китая в данной сфере также зависит киберполитика государств, обладающих не столь значительными возможностями в киберпространстве.

В силу данных причин необходимо обратить внимание на американский и китайский подходы к формированию политики в области кибербезопасности, ведь именно США и КНР считаются одними из наиболее влиятельных акторов мировой политики, а их взаимодействие в вопросах кибербезопасности и стабильность формирующейся ими системы взаимоотношений имеют глобальное значение.

**Объект исследование –** кибербезопасность в современных международных отношениях.

**Предметом исследования** является проблематика кибербезопасности в американо-китайских отношениях.

**Хронологические рамки исследования** охватывают период с 1990-х гг. до 2018 года. Выбор нижней границы исследования обусловлен тем, что именно в данный период времени началось формирование информационной инфраструктуры и становление национальных подходов ряда стран, в частности США и КНР, к кибербезопасности и к использованию информационных технологий в качестве средства реализации национальных интересов.

**Цель работы -** определить содержание противоречий и выявить потенциал сотрудничества американо-китайских отношений в сфере кибербезопасности.

Для реализации цели необходимо решить **задачи:**

1. Дать понятие кибербезопасности и рассмотреть различные подходы экспертных групп к его определению;
2. Раскрыть институциональный аспект обеспечения кибербезопасности в США и КНР, проанализировать ход его развития;
3. На основе комплексного анализа официальных документов выявить особенности нормативно-правовых баз, регулирующих деятельность в киберпространстве США и КНР;
4. Определить имеющиеся проблемы американо-китайских отношений в киберпространстве и охарактеризовать основные события, повлиявшие на формирование данных проблем;
5. Выявить существующие линии сотрудничества между США и КНР в области кибербезопасности, проанализировать их и определить возможный потенциал их развития.

**Методологическая основа исследования.**

Методология исследования обусловленасостоянием изученности данной темы и основана на междисциплинарном подходе.Метод сравнительного анализа был применен к нормативно-правовой базе США и КНР в сфере кибербезопасности и позволил выявить особенности обеспечения кибербезопасности в исследуемых странах, обозначить их общие интересы. Исторический и системный методы применялись при анализе развития институционального аспекта обеспечения кибербезопасности в Китае и США.Хронологический метод был использован при рассмотрении событий, повлиявших на развитие систем обеспечения кибербезопасности в исследуемых странах, в их последовательности и временной протяженности.

**Анализ источниковой базы исследования:** в работе были использованы различные по характеру документы и материалы. В первую очередь источниковая база представлена официальными документами США и КНР, в которые входят совместные соглашения между Китаем и Соединенными Штатами, определяющие различные аспекты двусторонних отношений, в том числе имеющие ключевое значение при формировании взаимодействия в киберпространстве и в области кибербезопасности (напр. документы c результатами проведения совместных диалогов по вопросам кибербезопасности[[2]](#footnote-2)). Также в группу официальных документов входят нормативно-правовые акты. Анализ текстов законодательных актов позволяет обозначить позиции сторон по многим вопросам, в том числе по вопросам в сфере кибербезопасности (напр. Стратегия действий в киберпространстве США[[3]](#footnote-3), международные стратегии для киберпространства США[[4]](#footnote-4) и КНР[[5]](#footnote-5), закон о кибербезопасности КНР[[6]](#footnote-6)). Важную часть источников составляют заявления, комментарии, речи, выступления председателей КНР, президентов США и других высокопоставленных лиц (напр. речь Ху Цзиньтао на Национальной научно-технической конференции в КНР[[7]](#footnote-7), выступление Барака Обамы и Си Цзиньпина на совместной пресс-конференции[[8]](#footnote-8)). Подобные материалы выявляют официальную позицию высших лиц государства по определенным вопросам, касающихся кибербезопасности стран, разнообразным событиям международной жизни. Также в источниковой базе необходимо выделить статистические данные, которые были необходимы при анализе количества и последствий кибер атак между исследуемыми США и КНР, при наглядном сравнении различных показателей сферы кибербезопасности (напр. статистика о средней годовой стоимости кибератак для компаний в отдельных странах[[9]](#footnote-9), данные о ежедневных DDoS атаках по всему миру[[10]](#footnote-10)). Также в ходе исследования в качестве официальных источников применялись материалы некоторых информационных агентств, как, например, Синьхуа, ввиду специфики средств массовой информации Китая. Таким образом, наличие широкой исследовательской базы позволяет рассмотреть кибербезопасность в американо-китайском взаимодействии с разных сторон, выявить и рассмотреть её особенности.

**Степень научной разработанности:**

Тематика двусторонних отношений между такими крупными державами Азиатско-Тихоокеанского региона, как КНР и США, проблемы и перспективы их развития в сфере кибербезопасности, являются актуальными темами исследования на сегодняшний день и представлены в работах специалистов из многих стран, но наибольшее количество исследований данных отношений ведется в США и КНР, так как они непосредственно вовлечены в них.

Прежде всего необходимо отметить вклад в исследования американо-китайских отношений в целом, их различных аспектов Е. Бажановым[[11]](#footnote-11), С. Трушем[[12]](#footnote-12), А. Парканским[[13]](#footnote-13), О. Тимофеевым[[14]](#footnote-14), А. Давыдовым[[15]](#footnote-15), Я. Лексютиной[[16]](#footnote-16). Среди множества американских ученых, занимающихся изучением американо-китайских отношений, их динамикой, а также отдельными вопросами, можно выделить таких известных политологов, как Дж. Най[[17]](#footnote-17), Г. Хардинг[[18]](#footnote-18), Д. Лэмптон[[19]](#footnote-19), а также Р. Саттер[[20]](#footnote-20). Среди китайских исследователей можно выделить Тан Цзиньюй[[21]](#footnote-21) и Минсина Пэя[[22]](#footnote-22). В целом, наблюдается высокая интенсивность научно-исследовательских разработок проблематики американо-китайских отношений.

Тематика кибербезопасности и киберпространства также исследуется множеством экспертов. Среди отечественных исследователей можно выделить С. Старкина[[23]](#footnote-23), занимающегося вопросами обеспечения безопасности, проблемами военно-технического сотрудничества и трансферта технологий, М. Безкоровайного[[24]](#footnote-24), исследующего аспект кибербезопасности в современном мире, Г. Ибрагимову[[25]](#footnote-25), исследующую глобальную безопасность и национальные, международные киберстратегии, автора исследования о стратегии КНР в киберпространстве, Е. Разумова[[26]](#footnote-26), автора исследования о политике КНР по обеспечению кибербезопасности. Также стоит выделить Панцерева К., Виноградову С., Васильеву Н, Болгова Р., авторов учебника «Информационное общество и международные отношения»[[27]](#footnote-27), в котором были предложены подходы к определению информационной безопасности, а также рассмотрены основные структуры, регулирующие киберпространство. Отдельно из авторов учебного пособия стоит выделить работу Болгова Р. [[28]](#footnote-28), где были рассмотрены информационные технологии в военных стратегиях стран, в том числе США и КНР, а также отдельное исследование[[29]](#footnote-29) об информационных технологиях в модернизации вооруженных сил КНР. Среди западных экспертов в области кибербезопасности можно выделить Д. Стэйнберга[[30]](#footnote-30), автора нескольких книг об обеспечении безопасности в современном киберпространстве, Д. Линдсэй[[31]](#footnote-31), изучающего влияние технологий на глобальную безопасность, особенно кибербезопасность и безопасность военных инноваций, а также систему кибербезопасности КНР. Также стоит выделить А. Сигала[[32]](#footnote-32), автора 3-х монографий о развитии цифровых технологий и кибербезопасности, в том числе в Китае, Д. Вентре[[33]](#footnote-33), автора работ, посвященных проблематике обеспечения кибербезопасности КНР, именно в его трудах прослеживаются попытки теоретического обоснования функционирования гос аппарата КНР в киберпространстве, и М. Хатауэй[[34]](#footnote-34), ведущего эксперта в вопросах кибербезопасности и политики киберпространства, основного автора Обзора политики в области киберпространства для Барака Обамы, а также главного руководителя Общей национальной инициативы по кибербезопасности при президентстве Дж. Буша-мл. С китайской стороны можно выделить Хао Ели[[35]](#footnote-35), старшего советника Китайской международной стратегической ассоциации, принимающей участие во многих диалогах между КНР и США, РФ по вопросам кибербезопасности, а также автора трудов на темы развития киберпространства и обеспечения национальной кибербезопасности.

 Отдельно необходимо выделить группу исследований, направленную на изучение вопроса кибербезопасности в американо-китайских отношениях, а также влиянии данной проблематики на двусторонние отношения. Например, А. Петухова и И. Комарова, исследовавших переход соперничества США и КНР в киберпространство[[36]](#footnote-36), Г. Юрченко[[37]](#footnote-37), К. Антипова[[38]](#footnote-38) и А. Булавина[[39]](#footnote-39), занимающихся исследованием американо-китайских отношений в киберпространстве, но при этом стоит отметить, что во многих исследованиях при описании китайской системы кибербезопасности в источниковой базе указаны в основном наработки американских ученых. Среди американских исследователей можно выделить М. Свэйна[[40]](#footnote-40), эксперта в американо-китайских отношениях и отношениях в области безопасности Китая и стран Восточной Азии в частности, а также М. Салмайера[[41]](#footnote-41), директора проекта по кибербезопасности и противодействию киберпреступности в Центре Белфера. Китайские эксперты также уделяют внимание вопросу кибербезопасности в американо-китайских отношениях, так, например можно отметить труды известного китайского эксперта, тесно связанного с китайской администрацией в сфере киберпространства, а также директора Исследовательского центра управления киберпространством в Университете Фудань, Шень И[[42]](#footnote-42), касающиеся взаимодействия США и КНР в киберпространстве. Следует сказать о попытках Ган Чэня и Вэнь Чиньлима проследить возможности сотрудничества США и Китая в киберпространстве[[43]](#footnote-43), а также работы Фан Биньсина[[44]](#footnote-44), Ван Гуйфана[[45]](#footnote-45), в которых, однако, прослеживаются заметные соответствия с официальной позицией китайского правительства при осуществлении сравнительного анализа подходов США и Китая к обеспечению кибербезопасности.

В целом, подводя итог анализу научной разработанности данной проблематики, можно отметить, что исследования, в которых была бы представлена целостная картина развития американо-китайских отношений в сфере кибербезопасности и их взаимодействия в современных условиях с учетом исторического развития, как в США, КНР, так и России, не осуществлялись, однако в связи с растущей актуальностью данного вопроса, с ростом количества экспертных групп, предполагается, что количество исследований будет также увеличиваться.

**Структура работы**: работа состоит из введения, трёх глав, заключения, списка источников и литературы. В первой главе рассмотрены различные понятия кибербезопасности, охарактеризованы основные подходы к определению понятия, институциональный аспект обеспечения кибербезопасности в мире, в США и КНР. Во второй главе проанализированы нормативно-правовые базы США и КНР, регулирующие их деятельность в киберпространстве, рассмотрен хронологический ход их развития. Третья глава повествует о кибербезопасности как проблеме в американо-китайских отношениях, а также посвящена взаимодействию США и КНР в вопросах обеспечения кибербезопасности.

1. КИБЕРБЕЗОПАСНОСТЬ: ПОНЯТИЯ И ИНСТИТУЦИОНАЛЬНЫЙ АСПЕКТ ОБЕСПЕЧЕНИЯ
	1. Понятийно-категориальный аппарат кибербезопасности

Становление такого понятия, как кибербезопасность, было результатом возникновения угроз национальной безопасности ряда стран и зародившейся киберпреступности. Первое компьютерное преступление было зафиксировано в США более 50 лет назад, в 1966 году, но вопрос о компьютерной безопасности возник на повестке дня около 30 лет назад. Инцидент 1988 года[[46]](#footnote-46), когда было зафиксировано проникновение студента Корнельского университета в компьютерные системы американской разведки и министерства обороны, их отключение, привел к созданию компьютерной группы быстрого реагирования при университете Карнеги Меллон, предназначенной для регистрации крупных «взломов» компьютерных сетей и оказания помощи в устранении последствий от атак, проделанных киберпреступниками. Именно это и стало первыми мерами противодействия киберпреступности.

На сегодняшний день понятие кибербезопасности многогранно, поэтому достаточно трудно формализуемо, существует множество различных представлений и взглядов. Наличие правильной формулировки понятия кибербезопасности является крайне важным для точного определения главных целей работы различных структур и последующей защиты киберпространства от угроз.

В учебном издании «Информационное общество и международные отношения» авторы выделяют два подхода к информационной безопасности, условно называемые «реалистическим» и «либеральным»[[47]](#footnote-47). «Реалистический» подход и его признаки включают в себя контроль над распространением информации и технологий, разработку средств ведения кибервойны, мониторинг уровня кибербезопасности потенциальных противников, увеличение уровня безопасности информационных систем внутри страны. Концепция «либерального» подхода предполагает принятие международных соглашений по проблемам кибербезопасности, построение отношений государств в киберпространстве на основе взаимного доверия.

Говоря о различных представлениях о кибербезопасности, необходимо рассмотреть и официальные формулировки. Например, в концепции стратегии кибербезопасности РФ приведено следующее понятие: «Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями»[[48]](#footnote-48). Есть основание считать данное определение несколько некорректным, поскольку в нём делается упор исключительно на угрозах.

На сайте securitylab.ru, информационном портале о событиях в области кибербезопасности, единственном ресурсе в русскоязычном Интернете, который оперативно публикует полную информацию обо всех выявленных в мире кибер уязвимостях, представлено понятие кибербезопасности как набора средств, стратегий, принципов обеспечения безопасности, гарантий предоставляемой безопасности, действий и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей[[49]](#footnote-49). Представленное определение кибербезопасности подразумевает достижение и сохранение свойств безопасности у ресурсов организаций или пользователей, их направленность против потенциальных киберугроз.

В изданном в 2016 году Законе о кибербезопасности КНР даётся определение кибербезопасности, как всеобъемлющей дисциплины, включающей в себя информатику, сетевые технологии, коммуникационные технологии, криптографию. Уточняется, что дисциплина направлена на защиту от случайного или злонамеренного повреждения, изменения или утечки данных[[50]](#footnote-50).

В обзоре политики в сфере кибербезопасности США Белого Дома представлено определение, где кибербезопасностью называют деятельность или процесс, способность или состояние, в соответствии с которыми все информационные и коммуникационные системы и содержащаяся в них информация, защищены от несанкционированного доступа, ущерба, использования, модификации. Также кибербезопасностью называют стратегии, политики и стандарты безопасности и функционирования систем в киберпространстве, охватывающие спектр мер по сокращению возможных угроз и своевременной политике реагирования на возможные инциденты[[51]](#footnote-51).

Рассмотренные официальные формулировки понятия кибербезопасности очень разнятся, они преследуют несхожие цели и предполагают потенциальные угрозы разного рода. Всё это подчеркивает существование различных подходов к определению кибербезопасности. Анализируя формулировки исследуемых США и КНР, можно сделать вывод, что именно «реалистический» подход к определению кибербезопасности и его признаки отражают политику обеспечения кибербезопасности Соединенных Штатов и Китая, при этом концепция «либерального» подхода также имеет место, так как обе страны всё чаще идут на диалог и соглашаются с нарастающей ролью киберпространства и необходимостью создания общего регулирующего органа.

Говоря об обеспечении кибербезопасности, необходимо учитывать достаточно важный её аспект – взаимосвязи между участниками, т.е. пользователями, которая может привести к синергетическому эффекту. Необходимы тщательные исследования свойств киберпространства, динамики его развития, методов управления этой динамикой. Крайне сложно, практически невозможно построить действительно эффективную систему кибербезопасности без её системного анализа, поэтому представляется целесообразным включить в комплекс исследований в области кибербезопасности такие направления, как: выработка единой терминологии кибербезопасности и киберпространства; разработка системы показателей функционирования киберпространства, а также его защиты от потенциальных угроз; разработка моделей киберпространства и факторов, влияющих на его функционирование; создание специальных методов обеспечения устойчивости киберпространства при воздействии угроз; создание интеллектуальных методов обеспечения кибербезопасности, таких, как метод ситуационного анализа состояния информационной безопасности, новые методы криптографической защиты, интеллектуальные методы выявления проникновений в системы, методы интеллектуальной идентификации пользователей при атаке[[52]](#footnote-52).

Питер Сингер, эксперт в области кибербезопасности фонда «New America Foundation» и один из авторов книги о кибериндустрии «Кибербезопасность и кибервойна: что должен знать каждый», во время презентации своей книги на Talks at Google отметил, что «несмотря на все надежды, связанные с информационными технологиями, несмотря на наступление нового цифрового века, мы живём во времена кибернебезопасности»[[53]](#footnote-53). С наступлением 21-го века всё чаще межгосударственные отношения и политические противостояния находят продолжение в интернете именно в различных видах атак, эксперты выделяют вандализм (использование интернета для порчи web-страниц), пропаганду (массовую рассылку пропагандистского характера), шпионаж (взлом и в дальнейшем получение доступа к частным страницам или серверам с целью сбора секретной информации/ее замены на фальшивую), DDoS-атаки на компьютерные системы и серверы (вмешательство в работу оборудования, атаки на узлы инфраструктуры) и т.д. Всё это – составляющие кибервойн[[54]](#footnote-54). Кибервойной называют противостояние в сети Интернет, направленное на выведение из строя наиболее важных компьютерных систем страны-противника (прежде всего системы гос органов, военных структур), а так же систем её критических отраслей инфраструктуры[[55]](#footnote-55).

Считается, что такие важные правительственные компьютерные системы, как, например, система управления ядерным оружием, обычно не подсоединены к другим системам и используют совершенно отдельные интернет – сети, однако достаточно часто хакеры обнаруживают в государственных внутренних сетях точки соприкосновения с интернетом, благодаря которым все эти сети могут быть заражены вредоносным ПО. Несмотря на наличие подобных рисков, интернет - относительно регулируемая, контролируемая среда, поэтому любая аномальная активность может быть сначала отслежена, а затем в максимально возможные кратчайшие сроки взята под контроль и впоследствии изолирована. Государства, выделяющиеся амбициями в кибервоенной сфере, всегда стараются максимально адаптировать вредоносное программное обеспечение для конкретных систем, так как взлом данных сетей может иметь решающую роль при военном конфликте. Однако при рассмотрении варианта войны, в которой стороны вынуждены постоянно отвечать на инновации друг друга, становится ясно, что кибервойна может стать еще одной гранью любого конфликта - порой важнейшей.

Таким образом, определение кибербезопасности как набора средств, стратегий, принципов обеспечения безопасности, гарантий предоставляемой безопасности, действий и технологий, которые используются для защиты киберсреды, а также реалистический подход к определению кибербезопасности, являются наиболее точными и соответствующими современным реалиям. Процесс обеспечения кибербезопасности включает в себя множество аспектов, внимание которым так или иначе уделяется во всех официальных формулировках кибербезопасности, а рассмотренные различные виды противостояний в киберпространстве только подтверждают острую необходимость в осуществлении кибербезопасности и создании соответствующих институтов, регулирующих киберпространство.

1.2 Институциональный аспект обеспечения кибербезопасности

Проблемы обеспечения кибербезопасности по мере их возникновения стали предметом обсуждения высшего руководства не только самых крупных держав. Перед возрастающей угрозой, которую киберпространство представляет для всего мира и всех стран без исключения, мировое сообщество начало предпринимать попытки выработки единых стратегий и единых стандартов к обеспечению информационной безопасности. На сегодняшний день в мире существует ряд организаций и международных структур, занимающихся вопросами кибербезопасности и регулирования киберпространства, а также предпринимающих попытки организовать сотрудничество в сфере обеспечения кибербезопасности между как можно большим количеством стран-участниц, в том числе США и КНР.

Еще в 2002 году резолюцией A/RES/57/239 Генеральной Ассамблеи ООН[[56]](#footnote-56) были приняты 9 взаимодополняющих элементов для создания глобальной культуры кибербезопасности, которые включают в себя: осведомленность о необходимости безопасности информационных сетей; ответственность за безопасность информационных сетей; реагирование на инциденты, затрагивающие безопасность сетей; этику, то есть учитывание законных интересов других; демократию, чтобы безопасность обеспечивалась соответствуя ценностям демократического общества; оценку рисков, позволяющую выявить угрозы и факторы уязвимости; проектирование и внедрение средств обеспечения безопасности, рассматривая соображения о кибербезопасности в качестве важнейшего элемента всей системы; управление обеспечением безопасности, опираясь на динамичную оценку рисков; переоценку вопросов безопасности информационных систем и сетей и вносить надлежащие изменения. Данная резолюция была одним из первых документов, признающим возникающие угрозы киберпространства и необходимость в обеспечении кибербезопасности как имеющихся, так и планируемых создаваться систем.

Одной из главных международных организаций, определяющей рекомендации в области телекоммуникаций, радио, а также киберпространства, является Международный Союз Электросвязи (МСЭ)[[57]](#footnote-57). Основанный в 1865 году[[58]](#footnote-58), МСЭ играет важную роль в области информационной безопасности и стандартизации в различных сферах деятельности уже более 150 лет.

В связи с необходимостью создания глобальной основы, которая могла бы предоставить международные принципы, соответствующие уровню деятельности хакеров, а также позволяющей странам быстро координировать деятельность в киберпространстве на региональном и глобальном уровнях, в 2008 году группа экспертов высокого уровня, включающая в себя специалистов в области кибербезопасности, представляющих самый широкий спектр областей: администрации Государств – Членов МСЭ, региональные и международные организации, а также научно-исследовательские и академические учреждения, представили Глобальную программу кибербезопасности МСЭ[[59]](#footnote-59). Данная программа была основана на таких принципах, как международное сотрудничество, правовые меры, организационные структуры, создание потенциала, технические и процедурные меры[[60]](#footnote-60). Конечной целью программы было определено «достижение значительного прогресса в отношении согласованных целей в борьбе с киберпреступностью и повышение уровня доверия и безопасности в информационном обществе»[[61]](#footnote-61). В рамках деятельности по созданию глобальной системы обороны МСЭ в том же 2008 году подписал Меморандум о взаимопонимании с созданным в мае 2008 года Международным многосторонним партнерством против киберугроз – ИМПАКТ[[62]](#footnote-62). В качестве первого в мире всестороннего альянса против киберугроз, поддерживаемого ООН, ИМПАКТ объединил правительства, академические организации и экспертов кибербезопасности с целью повышения способности глобального сообщества решать проблемы, связанные c информационной безопасностью. Именно ИМПАКТ стал оперативной базой для реализации Глобальной программы кибербезопасности, принятой МСЭ.

Помимо разработки Глобальной программы кибербезопасности, МСЭ в 2013 году впервые представил исследование по Глобальному индексу кибербезопасности[[63]](#footnote-63). Цель данного исследования заключалась в измерении приверженности Государств – Членов МСЭ кибербезопасности по 5 главным критериям, а именно: наличию правовых систем и структур, занимающихся вопросами кибербезопасности и киберпреступлений; техническим возможностям в области кибербезопасности; существованию институтов координации политики и стратегий развития кибербезопасности на государственном уровне; наличию научно-исследовательских, образовательных и подготовительных программ, а также сертифицированных специалистов и госучреждений, способствующих наращиванию потенциала в сфере информационной безопасности; наличию партнерств, механизмов сотрудничества и систем обмена информацией. Обнародованный рейтинг был принят во внимание всем мировым сообществом и позволил оценить, насколько серьезно каждая из стран относится к вопросу кибербезопасности. С тех пор МСЭ успели издать еще два исследования по данному рейтингу, последнее из которых было опубликовано в 2017 году[[64]](#footnote-64). По результатам данного исследования 2 место (после Сингапура) принадлежит США, а КНР только на 32 месте, что показывает значительное отставание Китая, однако при этом предоставляет возможности для их сотрудничества в рамках МСЭ с целью развития и совершенствования оцениваемых критериев.

Необходимо также отметить Глобальный центр кибербезопасности, о создании которого было объявлено[[65]](#footnote-65) 24 января 2018 года в Давосе на Всемирном экономическом форуме. Центр будет в Женеве и будет работать как автономная организация под покровительством Всемирного экономического форума[[66]](#footnote-66). Цель центра - “учреждение первой международной платформы для правительств, компаний, специалистов и правоохранительных органов, предназначенной для сотрудничества по преодолению проблем кибербезопасности”[[67]](#footnote-67). Центр уже получил поддержку британской телекоммуникационной компании BT Group, американской компании по разработке и исследованию беспроводных систем связи Qualcomm, российского Сбербанка, Интерпола, а также других известных компаний и правоохранительных организаций, что показывает растущий интерес к участию в проектах подобного рода не только представителей администраций стран, но и крупных организаций, в том числе международных, их заинтересованность в исследуемой проблеме, а также готовность к сотрудничеству.

О необходимости решить проблему, как защитить данные, национальные системы, использующие эти данные, от киберпреступности, первыми задумались США. Именно в период администрации Клинтона в 1995 году был инициирован старт работы над государственной стратегией в области кибербезопасности, в результате чего киберугрозы стали считаться угрозой национальной безопасности страны.

После террористических атак 11 сентября 2001 года, которые продемонстрировали явную уязвимость США, начало происходить развитие реальных механизмов кибербезопасности. Например, в 2003 году по решению правительства был создан Департамент национальной безопасности (Министерство внутренней безопасности)[[68]](#footnote-68), который стал главным центром регулирования мер безопасности в киберпространстве. Целью создания департамента была консолидация всех исполнительных органов, имеющих отношение к безопасности страны, в единую правительственную организацию, что было самой масштабной реформой структуры федерального правительства США со времени создания Департамента обороны в 1947 году. С созданием нового министерства Джордж Буш увеличил финансирование сферы внутренней безопасности США в 3 раза, в результате чего бюджет Департамента в 2005 году составил более 40 млрд. долл. В том же году администрация разработала Национальную стратегию по обеспечению кибербезопасности[[69]](#footnote-69), которая определяла ведущие программы, направленные прежде всего на обеспечение национальной безопасности, такие, как, предотвращение вероятных кибератак и уменьшение на тот момент уже существующей уязвимости критической инфраструктуры.

Вопрос кибербезопасности продолжал оставаться важной проблемой, которой уделялось достаточно внимания администрацией США. Важным шагом стало принятие Комплексной инициативы по национальной кибербезопасности[[70]](#footnote-70) в 2008 году, которая стала основой для последующей разработки политики страны в киберпространстве. В доктрине, помимо целей в области кибербезопасности, также были назначены ведомства, ответственные за исполнение доктрины, ими стали Министерство внутренней безопасности, Управление администрирования и бюджета и Агентство национальной безопасности.

В 2009 году с приходом Барака Обамы была принята «Комплексная национальная инициатива по кибербезопасности», в которой были представлены 12 новых инициатив по кибербезопасности страны[[71]](#footnote-71), фундаментальной целью которых было исполнении мер по защите гражданских свобод, что являлось и продолжает являться главной целью кибербезопасности США.

Таким образом, система кибербезопасности США была построена на взаимодействии структур, которые выполняют функции противовесов, не позволяя другим получить монопольное положение. Можно выделить три больших уровня, первый из которых занимают национальные учреждения: Министерство обороны, которое занимается кибербезопасностью с акцентом на цели и задания армии, ему подчиняется Агентство Национальной Безопасности; **Министерство Внутренней Безопасности -** глобальный орган внутренней безопасности США**, в состав которого входит Национальное управление кибербезопасности США**; **Министерство Юстиции, занимающееся расследованием преступлений в киберпространстве внутри страны.**

Второй уровень кибербезопасности состоит из центров, подчиненных министерствам, таких, как Национальная совместная группа по расследованию киберпреступлений, Национальный операционный центр по угрозам, Кибернетическое командование ВС США, Ресурсный центр кибербезопасности, Центр защиты от киберпреступлений, Разведывательное сообщество, Компьютерная команда экстренной готовности. Задачи и цели данных структур совершенно разные, однако их деятельность направлена не только на локализацию последствий атак, но и на организацию превентивных мер. По глобальному рейтингу кибербезопасности, представленному в докладе МСЭ[[72]](#footnote-72), США имеют наивысшие показатели сразу по нескольким критериям, в большей степени благодаря налаженной работе существующих структур данного уровня. Также эксперты МСЭ выделяют отдельные факторы, позволяющие координировать сферу кибербезопасности между всеми штатами, именно поэтому в последнем докладе был особо выделен Ресурсный Центр Кибербезопасности[[73]](#footnote-73), созданный национальной ассоциацией губернаторов США.

Третий уровень киберзащиты США составляют различные региональные, локальные структуры, которые работают под патронатом выше названных органов[[74]](#footnote-74).

Построенная таким образом система кибербезопасности США подтвердила свои возможности и жизнеспособность и существует уже на протяжении многих лет. Дифференциация структур позволяет каждой функционировать автономно и решать свои задачи, соблюдая общую стратегию.

Правительство продолжает поиск и формирование новых групп экспертов по кибервойнам и кибербезопасности в целом. На пленарном заседании сената в апреле 2016 года Майкл Роджерс, директор Агентства Национальной Безопасности и командующий Кибернетическим командованием США, сообщил об установлении партнерства между представителями Командования и лучшими специалистами Кремниевой долины, специализирующимися в киберпространстве[[75]](#footnote-75).

Вскоре после этого на пост президента Соединённых Штатов Америки пришел Дональд Трамп, который еще до избрания часто говорил о том, на каком низком уровне, по его мнению, находилась кибербезопасность страны, о том, что ею «управляли люди, которые не знают, что делают»[[76]](#footnote-76), обещал большие изменения. Крупных изменений не произошло, но несколько указов выпущено всё же было. 11 мая 2017 года был подписан указ, направленный на укрепление кибербезопасности федерального правительства и защиту критической инфраструктуры страны от кибератак[[77]](#footnote-77).  Указ был подписан на фоне распространившихся в американском обществе дискуссий по поводу вероятного вмешательства России в президентскую кампанию 2016 года. В то же время, советник президента США по внутренней безопасности Том Боссерт заявил на брифинге, что указ Трампа  связан не с действиями России, а с потребностями США[[78]](#footnote-78). По его словам, документ направлен на давно назревшие потребности политики в киберпространстве, и напомнил, что Россия — не единственный противник США в интернете. А в декабре 2017 году Палата представителей США приняла законопроект по созданию агентства кибербезопасности и безопасности инфраструктуры[[79]](#footnote-79). Ожидается, что агентство существенно повлияет на уже существующую структуру системы киберзащиты США.

Говоря об институциональном аспекте обеспечения кибербезопасности в Китае, прежде всего стоит выделить такой фактор, как убеждения руководства страны относительно государственного суверенитета, которые, очевидно, напрямую влияют на уровень открытости и свободы интернета в КНР, а концентрация всей власти в одних руках еще больше повышает значение данного фактора для политического курса, в том числе и в информационном пространстве.

Руководство Китая не относит неограниченный доступ к информации к неотъемлемым правам человека, не считает это основой построения стабильности в обществе, как полагают в США. При формировании политики в области кибербезопасности Пекин уделяет немалое внимание продолжающей возрастать роли Интернета, потенциальным угрозам, которые он содержит, а также вероятности захвата важной информации через киберпространство, отсюда возникает необходимость государства в контроле Интернета.

Однако, несмотря на существующие опасения, руководство страны в последнее время всё чаще говорит о том, что развитие кибербезопасности -– одна из первостепенных задач для Китая, и Китай будет становиться всё более открытым[[80]](#footnote-80), о чем председатель КНР Си Цзиньпин также заявил 9 апреля 2018 года на Азиатском Экономическом форуме[[81]](#footnote-81). Также Си Цзиньпин в своих выступлениях не раз подчеркивал, что кибербезопасность – одно из главных условий развития, а развитие в свою очередь – гарантия безопасности. Он отмечал, что «кибербезопасность прежде всего ради общества, кибербезопасность опирается на общество, кибербезопасность – общая ответственность всего общества, она требует совместного участия и государственных организаций, и простых пользователей сети, чтобы совместно строить эффективные линии защиты информационной безопасности всей страны»[[82]](#footnote-82). Департаментам всех уровней провинций партия настоятельно рекомендовала тщательно изучить и впоследствии реализовать дух выступлений Генерального секретаря Си Цзиньпина, чтобы постоянно совершенствовать «чувство безотлагательности» и ответственности за работу по кибербезопасности.

Основные усилия руководства Китая при построении системы национальной безопасности страны направлены на построение прочной военизированной системы. Практически все структуры КНР, занимающиеся вопросом кибербезопасности, работают под началом военных. Интеграцию гражданских и военных служб, основополагающую роль КПК, можно назвать спецификой китайской системы кибербезопасности.

Несмотря на то, что с самого начала формирования и затем в течение долгого времени существовало формальное разделение правительства на гражданский и военный сектор, вся полнота власти все равно принадлежала и принадлежит председателю КНР. Наибольшее влияние на регулирование государственных информационных процессов с момента образования КНР и до реформы 2016 года имело руководство Народно-освободительной армии Китая (НОАК), поэтому вооружённые силы имели преимущество над гражданскими структурами, так как в полномочия военных входило проведение любых операций, в том числе шпионаж (например, политический, экономический, промышленный). Среди всех преобразований китайских вооруженных сил стоит выделить модернизацию, происходившую во второй половине 1990-х годов, в результате которой НОАК и войска резерва вместе с войсками народной вооруженной полиции (НВП) и народным ополчением составили "триединую систему" вооруженных сил Китая, в задачи которой также входило и отслеживание потенциальных угроз в информационной среде.

Началом работы конкретно над построением системы кибербезопасности в Китае можно считать 2001 год, когда Коммунистическая партия Китая осознала возрастающую значимость информационной безопасности и приняла решение о начале разработки возможностей Китая по ведению борьбы в киберпространстве. Тогда же в 2001 году появилась первая руководящая группа по государственной информатизации, возглавляемая премьером Госсовета КНР, Чжу Фунцзи[[83]](#footnote-83). Под ответственность данной группы попало развитие национальной инфраструктуры информационных технологий, и её информатизация. Подразделение руководящей группы по государственной информатизации – координационная группа по обеспечению государственной сетевой и информационной безопасности, несло ответственность за управление политикой безопасности. Руководящая группа по государственной информатизации и Канцелярия Государственного совета по информатизации были напрямую ответственные за осуществление политики в киберпространстве, однако просуществовали только до 2014 года.

Также необходимо выделить две структуры при Генеральном Штабе КНР – Третье и Четвертое управление, которые долгое время являлись направляющими в построении всей системы кибербезопасности Китая[[84]](#footnote-84). Так, Третье управлениезанималось киберразведкой и являлось основным подразделением, отвечающим за безопасность НОАК. Под контролем Третьего управления находилось несколько организаций, таких, как, например, Центр оценки информационной безопасности и сертификации НОАК, Информационная канцелярия НОАК[[85]](#footnote-85). Четвертое управление, также известное как департамент радиоэлектронных контрмер, было нацелено на организацию наступательных действий в киберпространстве, превентивных действий, целевых атак, а также разработке других подобных мероприятий. Операционные подразделения Четвертого управления НОАК были отражены в структурах-коллегах, существовавших на национальном уровне для служб и воплощенных в групповых армиях для военных регионов. В качестве основного структурного подразделения НОАК, занимающегося кибершпионажем, можно отметить UNIT № 61398, которое с 2006 года базируется в Шанхае[[86]](#footnote-86). В 2013 году численность подразделения оценивалась в 2000 человек[[87]](#footnote-87).

На сегодняшний день в государственном аппарате Китайской Народной Республики по обеспечению кибербезопасности особую роль играют Военный совет ЦК КПК и Военный совет при Госсовете КНР. В структуру Госсовета КНР входят профильные министерства, такие, как Министерство индустрии и информационных технологий, Министерство науки и технологий КНР, а также Министерство государственной безопасности, которое выдает лицензии, занимается грантами и финансированием академических программ, сертификацией коммерческих продуктов[[88]](#footnote-88). Данные министерства могут быть задействованы в разработке защитных мер в информационном пространстве. Также существуют ведущие малые группы, специализирующиеся на важных стратегических вопросах, в том числе вопросах национальной безопасности и вопросах внешнеполитического направления. К ним относятся Ведущая малая группа по вопросам национальной безопасности, Ведущая малая группа по проблемам Тайваня и Центральная малая рабочая группа по внешней политике[[89]](#footnote-89).

С 2013 года в сфере вооружённых сил КНР начались структурные изменения, связанные с реформой НОАК, проводимой новым политическим руководством страны. Так, вместо Генерального штаба НОАК главенствующей единицей стал Объединённый штаб, напрямую подчиняющийся Центральному военному совету при ЦК КПК[[90]](#footnote-90). В ходе продолжавшейся реформы НОАК стало известно о создании войск стратегической поддержки (в некоторых источниках «Силы стратегической поддержки»). Об их составе, численности, структуре, целях и задачах было известно крайне мало, а официальные лица в своих высказываниях на данную тему ограничивались лишь общими словами. Китайские и иностранные военные аналитики сходятся во мнении, что тремя основными направлениями, по которым действуют ВСП (ССП), являются космическое, электронное и киберпространство[[91]](#footnote-91). Настоящая деятельность ВСП НОАК засекречена до сих пор. Решение китайского правительства объединить 4 или 5 военных ведомств в единую структуру, которая выступает сегодня на одном уровне с флотом и ВВС страны, говорит о том, что Пекин очень серьезно относится к возможности ведения некинетических войн, что соответсвует планам Китая в рамках 13-й пятилетки стать мощной кибердержавой[[92]](#footnote-92). Объявленная Си Цзиньпином 11 января 2016 года реформа органов управления НОАК, являющаяся продолжением реформы 2013-го года, была названа беспрецедентной по своему радикализму за все время существования КНР.

За два года до объявления реформы органов управления НОАК руководство страны преобразовало ведущую группу по государственной информатизации и Государственную координационную группу по сетевой и информационной безопасности в Центральную ведущую группу по кибербезопасности и информатизации[[93]](#footnote-93), возглавляемую генеральным секретарем партии Си Цзиньпином[[94]](#footnote-94). Целью преобразованной группы было объявлено развитие информационных систем и поддержка IT-индустрии в стране[[95]](#footnote-95). Стоит отметить, что в данную группу входят премьер-министр Ли Кэцян и член Постоянного комитета Политбюро Лю Юньшань с 19 другими должностными лицами из Политбюро или на уровне министерств. Примечательно, что 10 из 11 членов Политбюро также входят в новую руководящую группу Си Цзиньпина по всестороннему углублению реформ. Это указывает на то, что руководство Китая рассматривает кибербезопасность как важный аспект укрепления авторитета КПК и современного Китая в целом. Китай твердо придерживается курса проведения военных реформ, которые включают в себя реорганизацию, усовершенствованные планы учебной подготовки, новые виды вооружений – все так или иначе связанное с актуальными на сегодняшний день информационными технологиями. Генерал Хао Ели[[96]](#footnote-96), вице-президент китайского института инноваций и стратегии развития, бывший замдиректор Четвертого управления НОАК считает, что «формирование правил для киберпространства в действительности представляет собой процесс игры в шахматы между великими державами»[[97]](#footnote-97).

По словам некоторых китайских военных экспертов, проводимые реформы НОАК, рассчитанные на период до 2049 года, будут уделять всё большее внимание информатизации[[98]](#footnote-98). Главной целью всех проводимых сейчас реформ является создание информатизированных вооруженных сил, способных оперативно действовать в военных конфликтах с применением новых информационных технологий. Информатизация и компьютеризация вооруженных сил, которые проводятся в рамках модернизации НОАК, нацелены на усиление боевых возможностей прежде всего за счет улучшения взаимодействия всех видов войск во время проведения совместных операций.

Правительство финансирует всё большее количество различного рода программ, так как руководство страны не скрывает и даже открыто говорит о проблеме нехватки специалистов по кибербезопасности. Таким образом, в 50 китайских университетах финансируются программы, направленные на поддержку исследований в области организации кибератак, их проведении, а также киберобороны. Поддерживаются исследования, связанные с проведением информационной войны[[99]](#footnote-99). 15 августа 2017 года министерство образования объявило, что в Китае за 10 лет (2017-2027 годах) планируется построить 4-6 всемирно известных школ кибербезопасности[[100]](#footnote-100). Первый Инновационный центр военно-гражданского слияния в области кибербезопасности для преодоления угроз безопасности со стороны киберпространства был создан в Пекине уже в конце 2017 года[[101]](#footnote-101).

Из-за значительного роста количества скоординированных атак в киберпространстве, как на правительственные, так и на частные сети, показывающего интенсифицированное внимания к Интернету, как средству для атак в попытках достичь политических, социальных целей, руководства стран становятся просто вынуждены заботиться об ужесточении мер безопасности. И в США, и в КНР, система обеспечения кибербезопасности начала формироваться еще в 90-е годы.

Начиная с тех времен и по сегодняшний день, киберугрозы, создаваемые киберпреступниками, террористами и военными ведомствами других государств, для США обозначены как приоритетные направления национальной безопасности. Формируемая система кибербезопасности из трёх больших уровней имеет цель в достижении информационного превосходства, создании системы обмена данными о киберугрозах и разработке новых технических программ кибербезопасности.

Китайская система кибербезопасности отличается интеграцией военных и гражданских структур. С приходом Си Цзиньпина к власти и начавшимися реформами НОАК, Китай все еще находится в переходном периоде формирования полноценной инфраструктуры обеспечения кибербезопасности и организует всё новые программы, нацеленные на развитие кибербезопасности страны.

И США, и КНР признают нехватку специалистов в области кибербезопасности, продолжают формировать институты для её обеспечения. Всё это представляет собой не только область, где возможно развитие сотрудничества, но и сферу, где могут возникнуть противоречия ввиду различных взглядов на регулирование интернета в стране.

# 2. НОРМАТИВНО-ПРАВОВЫЕ БАЗЫ США И КНР, РЕГУЛИРУЮЩИЕ ДЕЯТЕЛЬНОСТЬ В КИБЕРПРОСТРАНСТВЕ И ОБЕСПЕЧИВАЮЩИЕ НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

# 2.1. Правовые основы обеспечения кибербезопасности США

На сегодняшний день кибербезопасность рассматривается, как проблема государственной важности, которая затрагивает все слои общества. Государственные программы в киберпространстве и их политика кибербезопасности являются средствами усиления национальной безопасности и надежности информационных систем государства. Для того, чтобы выявить противоречия США и КНР в проводимой ими политике, определить потенциальные сферы для сотрудничества, необходимо проанализировать документы, законопроекты, инициативы и государственные стратегии, повлиявшие на ход развития и становление современной версии стратегии стран в киберпространстве.

Первые основы американской военной стратегии кибербезопасности были заложены в 1990-е годы. В период администрации Билла Клинтона в 1995 году была обнародована Стратегия национальной безопасности[[102]](#footnote-102), где была поставлена задача: путем наступательных и оборонительных информационных операций добиться информационного превосходства. Директива Президента № 63 «О защите критической инфраструктуры»[[103]](#footnote-103), подписанная президентом США в 1998 году, получила развитие и была кодифицирована в виде «Национальной стратегии безопасности киберпространства»[[104]](#footnote-104) . Также Директива Президента №63 была кодифицирована в виде Директивы Президента в области национальной безопасности №7 «Об определении, приоритизации и защите критически важных элементов инфраструктуры»[[105]](#footnote-105), причем в обоих документах особый приоритет имело создание программы по минимизации угроз в киберпространстве.

Вскоре после произошедших террористических атак 11 сентября 2001 года, которые выявили уязвимость национальной безопасности, администрация Джорджа Буша интенсифицировала работу по направлению развития конкретных механизмов обеспечения кибербезопасности. Так, в 2003 году была разработана Национальная стратегия по обеспечению безопасности киберпространства[[106]](#footnote-106), в которой администрация Буша определила основные программы, направленные на обеспечение национальной кибербезопасности, предотвращение кибератак и уменьшение уязвимости критической инфраструктуры. В стратегии также подчеркивалась значимость достижения превосходства благодаря наступательным и оборонительным информационным операциям. Министерством обороны были выделены три случая их применения: в мирное время, в период кризиса и во время конфликта, что показывает уже тогда возникшие намерения руководства страны усилить свои силы в киберсреде, чтобы быть готовыми и к информационной обороне.

Стратегия 2003 года получила своё продолжение уже в 2008 году, когда была принята Комплексная инициатива по национальной кибербезопасности[[107]](#footnote-107). Данной инициативой была заложена основа для последующей разработки киберполитики страны, она подтвердила, что в будущем киберугрозы потребуют еще больших усилий от правительства по внедрению своих технических, а также организационных возможностей для более действенных решений современных угроз и уязвимостей.

Необходимо отметить, что несмотря на то, что кибербезопасность США начала развиваться еще в 90-е годы и продолжила своё развитие в 2000-е, именно с приходом администрации Барака Обамы начался принципиально новый этап развития в направлении кибербезопасности. Президент Обама изначально определил кибербезопасность как одну из самых серьезных проблем в безопасности страны, при этом затрагивающую экономическую сферу. Вскоре после вступления Барака Обамы в должность, им было поручено провести рассмотрение федеральных мер по защите американской информационной инфраструктуры. В этом же году группа экспертов предоставила “Обзор политики в киберпространстве”[[108]](#footnote-108). В обзоре экспертами были предложены варианты дальнейших шагов, которые будут направлены на внутреннюю трансформацию системы кибербезопасности США. Приняв к сведению рекомендации экспертов и оценив положение страны, администрацией Обамы была сформулирована новая Комплексная национальная инициатива по обеспечению кибербезопасности, в которую включили 12 основных положений, среди которых были: создание Федеральной корпоративной сети как единой корпоративной сети с тем, чтобы сформировать общий подход к безопасности; координация и перенаправление научных исследований и разработок (Научно-исследовательские и опытно-конструкторские работы (НИОКР); подключение киберцентров с целью повышения ситуационной осведомленности; разработка и внедрение государственного плана контр-киберразведки; развитие кибер образования; определение и развитие стратегии и программы киберсдерживания; определение роли федерального правительства в расширении кибербезопасности критической инфраструктуры и др.[[109]](#footnote-109)

Двумя годами позже, в мае 2011 года, Белый дом представил миру Международную стратегию в киберпространстве[[110]](#footnote-110), в которой была отмечена необходимость военного сдерживания и противостояния, создания мирного и стабильного глобального киберпространства благодаря межгосударственному сотрудничеству. В документе выделялось признание и приспособление возрастающей военной потребности в надежных и безопасных сетях. Кроме того, американцами была признана важность и необходимость расширения существующих военных союзов для противостояния потенциальным угрозам в киберпространстве. Среди приоритетных направлений стратегии следует отметить повышение безопасности, надежности и устойчивости, что включает в себя развитие сотрудничества в сфере кибербезопасности, в частности, норм поведения государств в рамках двусторонних соглашений и различных многосторонних организаций. Также рассматриваются вопросы глобального управления Интернетом, нацеленные на дальнейшее продвижение открытости и инноваций в Интернете, а также проблемы свободы в Интернете, а именно - поддержка гражданского общества в обеспечении надежных платформ с возможностью свободного самовыражения. Представленная Международная стратегия показала открытость американской администрации к сотрудничеству с другими странами, а также в очередной раз подчеркнула, каких принципов они сами придерживаются.

Позднее, в июле 2011 года, также в период администрации Обамы, была принята Стратегия действий Министерства обороны в Киберпространстве[[111]](#footnote-111), что было первым документом, определяющим политику Министерства обороны в киберпространстве. В содержании данной Стратегии Министерство обороны опиралось на безопасность и надежность нового киберпространства, которое должно защищать основные свободы всех граждан, неприкосновенность их частной жизни, а также полностью свободные потоки информации, которые необходимы для своевременной связи при осуществлении военных миссий. Таким образом, в Cтратегии действий Министерства обороны в Киберпространстве были определены пять стратегических инициатив:

1. Министерство обороны рассматривает киберпространство как оперативную среду для организации, подготовки и оснащения операций с тем, чтобы извлечь преимущества потенциала киберпространства;

Данная инициатива отражает необходимость управление рисками в киберпространстве посредством увеличения квалификации, ситуационной осведомленности и созданием действительно безопасной сетевой среды.

1. Министерство применяет новую операционную концепцию защиты сети и систем ведомства;

Система предупреждения, которая распространяется на обеспечение кибербезопасности, а также передачу данных области кибербезопасности пользователям и администраторам, могла бы помочь решить проблему с большим количеством уязвимых мест в системе Министерства обороны США.

1. Минобороны сотрудничает с другими правительственными ведомствами и учреждениями и частным сектором, чтобы сформировать общегосударственную стратегию кибербезопасности;

В данной инициативе говорится о сотрудничестве Министерства с Департаментом национальной безопасности, а также другими ведомственными партнерами и частным сектором, для обмена идеями, для развития новых возможностей и коллективной поддержки при противостоянии современным вызовам киберпространства.

1. Министерство обороны выстраивает надежные взаимоотношения с союзниками США и международными партнерами по укреплению коллективной кибербезопасности;

В рамках данной инициативы делается упор на развитие международной осведомленности и возможности предупреждения, которая будет способна улучшить коллективную систему сдерживания. Так как международное сотрудничество в киберпространстве продолжает развиваться, министерство нацелено продвигать тесное сотрудничество в киберпространстве со своими союзниками, прежде всего путем разработки общей системы оповещения, а также проведения совместных учебных мероприятий.

1. Министерство обороны усиливает национальную изобретательность посредством квалифицированной рабочей силы и быстрого технологического развития.

Поддержка венным ведомством ученых, всевозможных академических и экономических ресурсов, с целью формирования группы кадров для работы в киберпространстве. Также в рамках данной инициативы планировалось внедрение инноваций в деятельность в киберпространстве, взаимодействие с представителями Кремниевой долины и других инновационных центров[[112]](#footnote-112).

Одной из главных проблем кибербезопасности, волновавших США, оставался коммерческий шпионаж со стороны Китая, однако издававшиеся указы не способствовали улучшению ситуации. И несмотря на отсутствие большого успеха в установлении норм, направленных против шпионажа, США удалось достичь признания возможности применения международного права к деятельности в киберпространстве[[113]](#footnote-113) и того, что защита прав человека должна осуществляться также и в Интернете. Для содействия принятию продвигаемых норм правительство США следовало реформировать свою разведывательную деятельность так, чтобы прежде всего она сама была более согласована с нормами открытости Интернета, которые США пытались установить, поощрять инициативы других стран в продвижении норм, возможно, даже когда это противоречит интересам США.

Вообще может показаться достаточно странным, что АНБ и официальные лица Пентагона предлагали применять такие мягкие инструменты, как нормы, а не выступали сторонниками строгих военных правил для контроля киберпространства, но можно выделить несколько причин, по которым стратегия с продвижением норм являлась лучшим вариантом: во-первых, США были очень уязвимы для кибератак и очень страдали от этой проблемы, которую было трудно решить, используя обычные инструменты военного управления. Во-вторых, достаточно сложно обеспечить безопасность, когда не всегда возможно определить источник нападения и даже время атаки. Наконец, соблюдение любых строгих правил сложно обеспечить, тем более в киберпространстве, где атакуют программным обеспечением, что по своей сути является нематериальным оружием[[114]](#footnote-114).

При этом важно отметить, что и нормы, несмотря на их мягкость, могут иметь важные последствия. Так, например, нормы в отношении применения ядерного оружия, установившиеся с 1950-х годов, сделали использование такого оружия практически немыслимым в обычных обстоятельствах. Нормы в киберпространстве также со временем могли бы привести к тому, что некоторые виды кибератак считались бы нормативно неуместными. Нормы могли бы послужить примером для любой заинтересованной страны и способствовать общемировому пониманию идей безопасности и их совместной работе[[115]](#footnote-115).

Киберстратегия США продолжала развиваться, и следующим важным шагом в её развитии стало принятие в 2012 году Национальной Стратегии обмена и защиты информации[[116]](#footnote-116). Данный документ определил три основных принципа политики США в вопросе информационной безопасности: информация как национальное достояние; обмен и защита информации, что требовало разделения общих рисков; принятие лучших решений, благодаря информации. Объяснить принятие новой стратегии можно тем, что американское киберпространство продолжало подвергаться множеству атак, администрация пыталась найти новые, иногда даже инновационные способы защиты информационных сетей и структур.

Итогом всех предыдущих стратегий можно назвать обнародованную в ночь на 24 апреля 2015 года Министерством обороны США обновленную стратегию кибербезопасности страны[[117]](#footnote-117), в которой снова было установлено стремление сдерживать любые кибератаки и максимально защищать Соединенные Штаты от любого противника и преступника, который пытается нанести вред интересам страны. В стратегии присутствовали и впервые выделенные потенциальные враги в киберпространстве, определив три группы угроз:

* Отдельные государства (Китай, Россия, Иран и Северная Корея)

К 2015 году Россией и Китаем достигнуты большие результаты в разработке кибер возможностей. Кража интеллектуальной собственности Китаем в пользу китайских компаний подрывала конкурентоспособность США. Российские хакеры отличались скрытностью, их не всегда получалось раскрыть. Северокорейские и иранские взломщики обладали меньшими возможностями, но, по мнению американских экспертов, испытывали явную враждебность к США и их интересам.

* Негосударственные акторы (Исламское государство)

Негосударственные акторы, такие, как Исламское государство, используют киберпространство для вербовки боевиков и распространения террористической пропаганды, что является логичным объяснением внесения Соединенными Штатами их в список врагов.

* Киберпреступники.

В сети множество киберпреступников, не относящих себя в какому-либо государству и действующих с прежде всего личными целями. Всё чаще поведение преступников в сети делает более сложным определение источника угрозы, вероятность ошибки продолжает увеличиваться.

Таким образом, для снижения указанных и других потенциальных рисков, а также повышения национальной безопасности США, в данной стратегия определялись такие стратегические цели и задачи, как:

* Создание и поддержание необходимых средств управления киберпространством;

В данном пункте говорится о подготовке новых кибернетических сил улучшенной профессиональной подготовки.

* Защита информационной сети и данных министерства обороны, снижение рисков миссий министерства обороны;

В рамках этой цели Министерство обороны намеревалось проводить всевозможные учения по работе в киберпространстве, особенно на случай, если на данные и сети Минобороны будут совершены атаки.

* Готовность защитить страну и жизненно-важные интересы США от подрывных или разрушительных кибератак;

В данном пункте подчеркивалась важность работы Министерства обороны с межведомственными партнерами, частным сектором, а также государствами-партнерами. Также предусматривается важность продолжения развития возможностей разведки для прогнозирования потенциальных угроз, проведение ежегодных обзоров возможностей Минобороны защитить страну.

* Создание и поддержка приемлемых кибер возможностей и плана по их использованию, чтобы контролировать эскалацию конфликтов и определять конфликтную среду на всех этапах её возникновения;

В случае нарастания напряженности у президента должен быть широкий диапазон возможностей управления сложившейся ситуацией, также Министерство обороны должно быть в состоянии использовать кибернетические операции. Это подразумевает ускорение интеграции кибер разработок в реальные планы.

* Создание и поддержка мощных международных альянсов и партнерств по сдерживанию общих угроз и повышению международной безопасности и стабильности.

Так как выполнение всех вышеперечисленных целей требует сотрудничества с зарубежными союзниками и партнерами, данной задачей Минобороны подтверждает, что им необходимо выстроить партнерский потенциал в области кибербезопасности. Для этого им необходимо установить, а где-то укрепить партнерство в ключевых для себя регионах: Европа, Азиатско-Тихоокеанский регион, а также Ближний Восток. Установка партнерства с перечисленными регионами включает в себя работу с союзниками по НАТО, создание нового стратегического партнерства в АТР, поддержка устойчивости сетей и систем союзников в Северо-Восточной Азии и Ближнем Востоке.

Помимо этого, очень важно отметить предусмотренное в стратегии усиление кибер-диалога США по укреплению стратегической стабильности с Китаем, несмотря на то, что Китай был причислен к врагам. Причиной этому является то, что переговоры с КНР могли помочь добиться большего взаимопонимания и прозрачности военной доктрины, политики, роли и миссии каждого государства в киберпространстве. Целью кибер-диалога также являлось снижение рисков недопонимания, которые могли бы способствовать эскалации напряженности и нестабильности.

Как гласит пресс-релиз Пентагона, опубликованная стратегия представляет собой «дополнение к существующей стратегии 2011 года», но по факту новая стратегия является более детальным и расширенным планом, текст стратегии по объему вдвое превосходит существовавший документ четырехлетней давности. Со времени опубликования стратегии 2011 года произошло много громких скандалов, как скандал вокруг программы PRISM и других разоблачений Эдварда Сноудена, обрушение серверов Sony северокорейскими «взломщиками», многочисленные проникновения китайских и российских хакеров во внутренние сети американских компаний и ведомств. Стратегия 2011 года была уже устаревшей и нуждалась в обновлении. Это косвенно подтверждается и в тексте документа 2015 года: «С момента разработки первой киберстратегии в 2011 году Пентагон достиг заметного прогресса в налаживании системы безопасности, разработке планов и работе с партнерами. В киберпространстве условия меняются особенно быстро. Мы должны быть динамичными, гибкими и расторопными, предупреждать угрозы, чувствовать возможности, развивать партнерства»[[118]](#footnote-118).

В день обнародования стратегии, министр обороны США, Эштон Картер, на своем выступлении выделил одну из миссий Пентагона, вокруг которых планировалось строить доктрину кибербезопасности в следующие пять лет (по плану следующее обновление документа должно выйти не позднее 2020 года) - это прежде всего защита собственной информационной сети. Минобороны открыто признало, что пока не способно защитить каждый «уголок» интернета от всех атак, поэтому перед ними стояла первоочередная задача в выделении и защите наиболее важных сегментов сети Пентагона[[119]](#footnote-119). Работа с корпорациями так же, как и партнерство с зарубежными союзниками  - важный элемент защиты национальных интересов США, уже второго приоритета Пентагона. Вдобавок среди представленных стратегических целей Пентагона была выделена систематизация существующей системы кибербезопасности, то есть привлечение квалифицированных кадров из рядов гражданских, предоставление возможности создания карьеры.

Изучив основные цели киберстратегии 2015 года, можно сделать вывод, что Министерство обороны признало свои уязвимости в киберпространстве, признало масштаб существующих киберугроз, который требует действий со стороны как государства, так и частного сектора. Сравнивая стратегию 2015 года с первоначальной стратегией 2011 года, также необходимо отметить, что оба документа содержат в себе пять «стратегических инициатив», большинство из которых повторяются. За период разработки новой стратегии в вопросе защиты сетей Пентагона акцент сместился с  базового поддержания безопасности на общее укрепление кибербезопасности, поддержание наиболее важных частей системы. Пункты, посвященные инновациям в интернет-отрасли, найму новых специалистов и сотрудничеству с международными и американскими структурами, подверглись слабым изменениям и в общем остались схожими.

Последним изданным документом, затрагивающим вопрос кибербезопасности США, является опубликованная 19 декабря 2017 года администрацией уже Дональда Трампа Стратегия национальной безопасности[[120]](#footnote-120), где Китай представлен в качестве одного из соперников США, но уже отмечено, что Китай стремится изменить глобальную расстановку сил в собственных интересах, а это может создать угрозу Соединенным Штатам. МИД Китая незамедлительно отреагировал и в ответ на данное обвинение заявил, что Вашингтону следует отказаться от устаревших концепций[[121]](#footnote-121). В тексте стратегии отмечается, что США будут добиваться равного и справедливого использования всеми государствами "общих пространств", а именно - космоса, мирового океана, воздушного пространства и, конечно, киберпространства. США намерены опираться на своих союзников, в первую очередь - стран НАТО. В то же время в НАТО было заявлено, что альянс планирует значительное увеличение расходов на разработку мер по кибербезопасности, для противостояния России, Китаю и Северной Корее[[122]](#footnote-122).

По мнению некоторых экспертов, стратегия национальной безопасности 2017 года в некотором смысле является возвращением к так называемой доктрине Буша, главный принцип которой был – «мир с позиции силы». У Обамы была позиция, связанная с применением инструментов мягкой силы. Трамп же снова делает упор на «мир через силу» (Peace through strength)[[123]](#footnote-123).

В тексте стратегии применительно к Интернету был приведен тезис о необходимости «ограниченной, но важной роли правительства в обеспечении соблюдения законности», заявлено, что США против «закрытых меркантилистских торговых блоков», а передача любых американских технологий, в рамках глобализации, квалифицируется как «принудительная». Важно отметить, что сам термин «глобализация» в стратегии не фигурирует, но подчеркивается «ложность предположения последних двух десятилетий о том, что вовлечение соперников и включение их в международные институты и глобальную торговлю превратит их в благонамеренных акторов и заслуживающих доверия партнёров»[[124]](#footnote-124).

Американский эксперт, Майкл Салмейер, считает, что новая стратегия представляет собой более тщательное рассмотрение кибербезопасности, как теперь уже основной проблемы национальной безопасности, однако Салмейер отмечает, что «новая Стратегия выходит за пределы установленных в ней целей и при этом уделяет слишком мало внимания вопросу сдерживания и обмена информацией»[[125]](#footnote-125).

В Стратегии национальной безопасности 2017 года представлены четыре основных направления действий: защита американского народа, родины и американского образа жизни; способствование американскому процветанию; сохранение мира через силу; увеличение американского влияния. Аспект кибербезопасности имеет место во всех четырёх представленных направлениях, но особенно представлен в первых трех.

В первом направлении рассматриваются взгляды администрации на то, как деятельность киберпространства будет способствовать усилиям США по уничтожению террористов. Интернет – одно из террористических убежищ, в документе четко указано, что в США существует необходимость решать проблему «темного» интернета. Также в данном направлении представлен отдельный раздел о транснациональных преступных организациях, которые, по мнению администрации США, могут быть использованы государственными противниками «для проведения неприемлемых кибер-вторжений, саботажа, кражи и политической подрывной деятельности»[[126]](#footnote-126).

Второе направление, озаглавленное как «Способствование американскому процветанию», содержит уже вполне предсказуемые слова о хищении Китаем американской интеллектуальной собственности. Действия Китая охарактеризованы как «экономическая война с кибер-поддержкой». Стоит отметить, что в самой стратегии отсутствует какой-либо новый принцип о том, как преобладать в войнах такого типа.

В третьем направлении «Сохранение мира через силу» присутствуют достаточно жесткие высказывания о деятельности России в киберпространстве. В документе подтверждается, что Россия продолжает наращивать инвестиции в свой набор новых военных возможностей, в том числе в «дестабилизирующие кибер-способности».

Все действия и намерения, описанные в стратегии, подтвердили, что вектор развития национальной безопасности остается прежним, однако подход к обеспечению безопасности, действительно, меняется.

Через месяц после публикации «Стратегии национальной безопасности», 19 января 2018 года, Министерство обороны США опубликовало новую версию «Национальной оборонной стратегии». Документ также определяет цели и задачи Пентагона, главные принципы военного планирования, снова уделяет большое внимание сдерживанию России и Китая. В тексте Стратегии Министерства обороны настаивается на модернизации американских ВС и увеличении расходов на системы вооружений. Изменение оборонной стратегии в принципе логично следует за появлением новой «Стратегии национальной безопасности» США, обнародованной в декабре, и дополняет общую картину обороны США.

Необходимо обозначить, что на предстоящие изменения в политике США, осуществляемой в киберпространстве, указывают не только недавно представленные стратегии. На сайте Министерства внутренней безопасности США указано, что в 2019 году Соединённые Штаты планируют выделить около $1 млрд на обеспечение кибербезопасности страны, а также $319 млн для защиты критически важной инфраструктуры[[127]](#footnote-127). Для сравнения еще в бюджете 2017 года сумма, выделяемая на кибербезопасность страны, в сумме была около $700 млн[[128]](#footnote-128).

В целом, исходя из проанализированных документов и приказов, мы можем сделать вывод, что американская стратегия кибербезопасности постепенно расширялась с момента принятия первого документа в начале 1990-х годов. Разработка концепции информационных операций оказала большое влияние на дальнейшую эволюцию мер безопасности. Позже, в период администрации Буша, продолжали появляться новые официальные документы, дополняющие уже формирующуюся стратегию безопасности страны в информационном пространстве. Основное развитие стратегия получила во время президентства Обамы: она была дополнена новыми сферами деятельности, приобрела большое число задач, включив взаимодействие с другими федеральными ведомствами. В период администрации Обамы в США появилась национальная стратегия информационной безопасности, которая не только нацелена на укрепление национального сегмента информационных систем, но и содержит в себе стратегию действий на международном уровне. Сегодня политика Соединенных Штатов в кибербезопасности основывается на таких приоритетах, как, защита критической инфраструктуры, повышение безопасности всех федеральных сетей, улучшение системы отчетности и реагирования на киберугрозы. Наконец, Соединенные Штаты подчеркивают важность дальнейшего развития своей кибер политики: они уделяют внимание подготовке высококвалифицированных сотрудников, осуществляют исследования, разработки и всё больше прибегают к использованию инноваций частного сектора. Таким образом, мы можем сделать вывод, что национальная кибербезопасность в относительно короткое время стала одним из основных направлений национальной политики США.

# 2.2. Правовые основы обеспечения кибербезопасности КНР

Для КНР существует ряд угроз, влияющих на формирование единой политики в области кибербезопасности, в том числе угрозы, связанные с растущей ролью интернета. Стремительному развитию интернета в Китае способствовал взятый КПК в 1995–1996 годах курс на развитие китайской науки и техники, который включал и разработки в области интернета, при этом растущая популярность интернета поставила перед руководством партии двойственную задачу: руководству страны было необходимо сохранить тотальный контроль во всей стране, при этом власти понимали, что Китаю необходимы внедрение ИКТ, экономическая модернизация, разрешение вопросов социальной жизни граждан. Руководство осознавало, что решение этих задач во многом зависит от уровня проникновения информационных технологий, в том числе интернета, во все сферы жизни страны, но абсолютно свободное функционирование интернета в Китае означало бы проникновение идей, вероятно, нацеленных в том числе и на дискредитацию политического строя государства, а КПК это не устраивало. События на площади Тяньаньмэнь в 1989 году сделали руководство страны весьма чувствительным к современным технологиям, вследствие чего руководство страны долгое время не могло определиться, какую позицию занять по отношению к развивающемуся интернету.

Необходимость контроля прежде всего над информационным и новостным пространствами была отмечена председателем «третьего поколения» руководителей Китая Цзян Цзэминем. Для решения поставленной задачи, началась довольно жёсткая политика по отношению к средствам массовой информации, после чего в 1996 году Партия дала согласие на развитие сети интернет в стране, в планы развития науки и техники Китая были включены информационные технологии[[129]](#footnote-129). Формирующаяся стратегия Китая по внедрению и развитию интернета в стране отличалась от западного подхода. «Интернет — это орудие работы, а не средство времяпрепровождения» — высказывание, которое в полной мере показывает позицию власти к использованию новых технологий в сфере коммуникаций.

Формирование отношения правительства к интернету и контролю над ним, безусловно, влияло и на становление кибербезопасности страны. Таким образом, не менее важным элементом обеспечения информационной безопасности в Китае сразу же было признано регулирование всего, что касалось шифрования. Одна из первых директив вышла еще в 1999 году[[130]](#footnote-130). Она регламентировала работу с программными обеспечениями: производство и продажа продуктов шифрования в коммерческом секторе были возможны только с имеющимся разрешением государственных органов и только в соответствии с установленными ими правилами. Так, криптостойкость никакого из продуктов не могла превышать уровень, утвержденный государством. Только спустя время власти разъяснили, что эти правила применяются исключительно к продуктам, где шифрование является основной функцией, то есть продуктам, потенциально связанным с государственными сетями и национальной безопасностью.

В 2000 году Всекитайское собрание народных представителей (ВСНП) предприняло попытку определить классификацию вероятных правонарушений в информационной сфере и опубликовало «Постановление по защите интернет - пространства», где были выделены области, в которых возможны нарушения: экономическая, образовательная, сфера поддержания общественной стабильности и защиты граждан. Основные положения стратегии информационной войны были внесены в Военно-политическое руководство КНР в 2002 году, когда НОАК объявила о растущей необходимости противостоять врагам в условии информационных войн. В то же время была сформирована и опубликована оборонная политика Китая, в которой делался упор на модернизации ВС КНР, их информатизации. В документе впервые появилась официальная формулировка «противостояние в локальных войнах в условиях информатизации вооруженных сил»[[131]](#footnote-131).

Развитие интернета продолжало набирать обороты, и в 2003 году Канцелярией ЦК КПК было опубликовано «Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности»[[132]](#footnote-132), где говорилось о необходимости предпринимать шаги по укреплению защиты стратегической инфраструктуры, проверке киберпространства на наличие возможных угроз, а также начале разработки мер по привлечению высококвалифицированных специалистов в области информационной безопасности.

Одной из таких мер стала реализация в 2004 году Министерством государственной безопасности ставшего впоследствии легендарным проекта «Золотой щит»: фильтрация интернет - трафика между китайскими провайдерами и международными сетями передачи информации специальными серверами, благодаря чему государственной властью фактически был взят тотальный контроль над информационным пространством страны. Делалось это для того, чтобы формировалось «правильное» восприятие действительности при ограничении доступа населения к иностранным источникам информации[[133]](#footnote-133). Важно отметить, что «щит», хоть и был нацелен прежде всего на внутреннее регулирование интернета, но и являлся одной из мер по обеспечению кибербезопасности страны, так как «уберегал» население от множества иностранных сайтов и возможных контактов с иностранными ведомствами, которые могли дискредитировать политический строй и выстраиваемую политику КПК.

В ноябре 2006 года была принята «Государственная стратегия по развитию информатизации на период с 2006 по 2020 годы»[[134]](#footnote-134). В стратегии были сформированы положения, затрагивающие развитие киберпространства, кибербезопасности, акцентировалось внимание на снижении зависимости от внешних ИКТ, прежде всего западных. «К 2020 г. Китай должен превратиться в государство инновационного типа, такова цель нашей  страны в области научно-технического развития на ближайшие 15 лет» - объявил генеральный секретарь ЦК КПК Ху Цзиньтао в 2006 году на встрече с учеными Китая[[135]](#footnote-135). В частности, на начальном этапе предполагалось создать структуры, которые будут регулировать всю деятельность в информационной сфере. Именно в данной стратегии были определены базовые векторы последующей государственной политики в области кибербезопасности[[136]](#footnote-136).

Формирующаяся стратегия Китая в киберпространстве продолжала быть основанной на защите суверенного права в обеспечении кибербезопасности внутри страны, важно отметить, что акцент делался именно на политическом аспекте проблемы. Так, в июне 2013 года во время выступлении на Форуме в Чэнду[[137]](#footnote-137), приуроченному к визиту Си Цзиньпина в Соединенные Штаты, Цай Минчжао, глава Пресс-канцелярии Госсовета КНР, отметил различия использования интернета разными государствами и потребовал проявить уважение к действиям руководства КНР по обеспечению кибербезопасности в своей стране. Вместе с тем, была подчеркнута заинтересованность КНР в международном сотрудничестве с целью осваивания новых возможностей в киберпространстве и обеспечении его безопасности[[138]](#footnote-138). Такая трактовка полностью отражала уже сложившуюся на тот момент позицию руководства страны и продвигалась на всевозможных уровнях международной деятельности КНР. Годом ранее в Будапеште, будучи ответственным представителем МИД Китая, Хуан Хуйкан, на конференции по кибербезопасности отметил, что соблюдение суверенитета является главным принципом китайской политики в киберпространстве[[139]](#footnote-139).

В 2014 году в Китае прошла первая встреча Группы по вопросам безопасности и информатизации[[140]](#footnote-140), на которой президент Си Цзиньпин дал напутствие сделать информационную безопасность главным приоритетом для Китая[[141]](#footnote-141). Вероятно, такие решения руководства страны были продиктованы и тем, что в 2013 году Китай вошел[[142]](#footnote-142) в число стран, понесших самые большие потери от киберпреступлений в мире, оказавшись на втором месте после США.

Тем временем идея о суверенной кибербезопасности продолжала развиваться и в положениях нового Закона о национальной безопасности, принятого в Китае в 2015 году, была снова подчеркнута необходимость укрепления защиты национальных информационных систем и установления суверенитета киберпространства в Китае. Более подробно эти вопросы раскрыл опубликованный черновик Закона о кибербезопасности[[143]](#footnote-143). Новый закон предполагал обязательную регистрацию в интернет-сервисах под настоящими именами, привлечение операторов к участию в правительственных расследованиях, крупные инвестиции в сферу кибербезопасности, введение множества обязательств по хранению персональных данных в Китае, которые, как предполагалось, должны храниться только в стране. В 2016 году закон был окончательно принят, а в 2017-м году вступил в силу[[144]](#footnote-144).

Регулирование закона предусматривает не только контроль интернета на национальном уровне, но и затрагивает отношения Китая с другими странами, так как закон внёс обязательную сертификацию оборудования сетевых операторов, запретил экспорт каких-либо экономических, технологических, научных данных, которые представляют потенциальную угрозу национальной безопасности или общественным интересам страны, за границу. Данное положение вызвало неоднозначную реакцию, в результате которой более 50 американских, европейских и японских компаний подписали коллективное письмо на имя премьер-министра Ли Кэцяна еще в июне 2016 года, когда закон был только принят и не вступил в силу. В письме компании утверждали, что новый закон будет препятствовать работе иностранных компаний в Китае[[145]](#footnote-145). А уже после вступления закона в силу, США опубликовали официальный призыв к Китаю[[146]](#footnote-146) с просьбой не допустить полного ввода новых правил, так как они препятствуют международному обмену информацией. Никаких официальных ответных заявлений на это не последовало. Тем временем закон продолжает поэтапно вступать в силу. Ожидается, что процесс завершится к концу 2018 года.

С принятием закона о кибербезопасности страны, руководство стало всё чаще говорить о своих намерениях стать мощнейшей кибердержавой. Такие намерения были описаны и в планах в рамках 13-й пятилетки, где было указано, что Китай в рамках нового пятилетнего плана увеличит свои технические возможности контроля над киберпространством, а также будет продвигать многостороннюю, прозрачную и демократичную международную систему по управлению интернетом. Помимо этого в планах указано, что КНР «усилит борьбу с врагами в суверенном онлайн-пространстве и увеличит контроль над общественными настроениями в сети интернет»[[147]](#footnote-147).

Это же намерение отражено и в опубликованной 27 июля 2016 года Национальной стратегии развития информатизации, которая была представлена как руководство для развития информационных технологий в Китае на ближайшее десятилетие. В тексте документа представлены три этапа, которые необходимо пройти Китаю для достижения этой цели. Согласно стратегии, первый этап завершится в 2020 году, в результате которого КНР выйдет на передовой мировой уровень по нескольким ключевым технологиям, индустрия информационных технологий станет намного более конкурентоспособной, а информатизация станет главной движущей силой модернизации страны. Второй этап, который продлится до 2025 года характеризуется формированием ведущей в всем мире сети мобильной связи, позволяющей Китаю окончательно прекратить использовать любые зарубежные технологии. На третьем этапе, который должен продлиться уже до 2050 года, Китай станет современным социалистическим государством с окончательно укрепившимся статусом кибердержавы. Также в Стратегии был подчеркнут проход процесса информатизации страны под централизованным руководством Центральной руководящей группы по кибербезопасности и информатизации, которая и будет утверждать основные решения в данной сфере[[148]](#footnote-148).

Говоря о намерениях Китая сотрудничать с другими странами для достижения своих целей, необходимо упомянуть о вышедшей 3 марта 2017 года, еще до вступления Закона о кибербезопасности в силу, китайской Международной стратегии взаимодействия в киберпространстве[[149]](#footnote-149). Ссылка на документ очень быстро разлетелась по Интернету, но подобная реакция мирового сообщества совсем неудивительна: для такого влиятельного игрока на международной арене в целом, и в киберпространстве в частности, публикация документа подобного рода – большое событие.

  Стратегия содержит в себе четыре главы. В тексте представлено не так много статистики, цитирования международных договоров и двусторонних соглашений, однако в документе присутствует достаточно частое упоминание роли ООН и группы правительственных экспертов, а также резолюции ООН 2009 года, утверждающей создание глобальной культуры кибербезопасности[[150]](#footnote-150). Вообще Китай с самого начала обсуждения проблем кибербезопасности еще в 1990-х годах активно призывал к центральной роли ООН в решении всех проблем. Это послание прослеживалось и в новом документе. Несмотря на глобальный характер стратегии, Китай вновь подчеркнул некоторые традиционные для него доминанты в киберпространстве, как необходимость уважать и не нарушать государственный суверенитет в области информационно-коммуникационных технологий. В документе также подчеркивается, что никакая страна не должна стремиться доминировать в виртуальном пространстве и навязывать свои правила поведения другим, что некоторые эксперты сочли достаточно прозрачным намёком на действия США. Очевидно, что регулирование киберпространства в экономической и военной сферах довольно часто вызывает труднопреодолимые сложности, именно поэтому полное внедрение норм международного права (здесь остается не раскрытым вопрос, всех ли норм и всех ли видов права) должно быть тщательно проработано сначала на национальном уровне, затем уже на международном. Своими заявлениями в стратегии Китай говорит о том, что прежде, чем применять к себе нормы международного права в киберпространстве, сначала он тщательно изучит их воздействие на сферу кибербезопасности именно внутри страны.

В целом документ не стал откровением, но его появление подчеркнуло необходимость в более четких в своей цели и немедленных в своей реализации решений основных проблем киберпространства и предотвращения появления новых вызовов.

На сегодняшний день руководство КНР продолжает придерживаться намеченных в опубликованных документах целей. 21 апреля 2018 года на совещании по кибербезопасности и информатизации Председатель КНР Си Цзиньпин напомнил о стоящих перед правительством задачах и призвал не упустить историческую возможность развития информатизации. Также Си призвал улучшить потенциал управления в киберпространстве и создать управляющую сеть, возглавляемую страной, сказал, что управление киберпространством в рамках ООН должно быть расширенным, а негосударственные организации должны играть более эффективную роль. Данным заявлением Си сослался на стратегию, обнародованную чуть больше года назад, что подтверждает приверженность Китая намеченному курсу. Председатель также призвал к построению цифрового шелкового пути 21-го века посредством укрепления сотрудничества со странами вдоль пояса. Ван Хунин, глава Секретариата ЦК КПК, в своей итоговой речи совещания призвал принять конкретные меры для реализации речи Си, «руководящего документа» по кибербезопасности и информатизации в новую эпоху[[151]](#footnote-151).

Рассмотрев развитие интернета в Китае, методы обеспечения кибербезопасности, становится ясно, что интернет на территории КНР воспринимается как сфера, которая содержит в себе не только черты модернизации, но и риски. Изначально КПК выстраивала достаточно жесткую политику относительно интернета, как и любого СМИ. Дав согласие на развитие интернета в 1996 году, в 2006 году руководство уже приняло Государственную стратегию по развитию информатизации. С целью реализации поставленных целей в глобальном киберпространстве, Китай уделял особое внимание совершенствованию киберсредств, взаимодействуя с хакерами. Важное значение имеет принятый в 2015-м году Закон о кибербезопасности, который затрагивает не только контроль интернета на национальном уровне, но и отношения Китая в киберпространстве с другими странами. В последних обнародованных документах и речах руководства Китая прослеживается намерение стать мощнейшей кибер державой в мире, но при этом Китай также проявляет инициативы в сотрудничестве с другими странами для достижения своих целей киберпространстве, что сказано в Международной стратегии взаимодействия в киберпространстве, опубликованной 2017-м году.

Стоит отметить, что и Китай, и Соединенные Штаты, осознают возрастающую роль интернета, важность и необходимость во внедрении кибербезопасности, и прилагают усилия, чтобы укрепить не только свою национальную информационную безопасность, но и внести вклад в развитие норм по регулированию международного киберпространства, однако имеющиеся противоречия в виде, например, демократических принципов, которых придерживаются США, и которые считаются определяющими по отношению к американской государственной политике, в том числе и политике в киберпространстве, но совершенно отрицаются Китаем, делают данную сферу еще более подверженной противостоянию.

3. ПРОТИВОСТОЯНИЕ И СОТРУДНИЧЕСТВО США И КНР В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

* 1. Кибербезопасность как проблема в отношениях США и КНР

Переживая периоды потепления и охлаждения, китайско‑американские отношения всегда оставались достаточно сложными и трудно предсказуемыми. С приходом интернета в страны, со становлением кибербезопасности новой важной составляющей международных отношений, обе стороны достаточно часто прибегали к кибератакам в отношении друг друга, что, конечно же, влияло на общее состояние двусторонних отношений и вынуждало руководства обеих стран относиться друг к другу с большей осторожностью. Высокий уровень развития технологий в Китае и США при наличии политических разногласий, и Пекин, и Вашингтон расценивают как угрозу национальной безопасности.

Перед правительством США долгое время стояла задача в минимизации количества кибератак со стороны КНР и их угроз, так как существуют исторические примеры, когда кибератаки становились ответом Китая на внешнеполитические акции США. Например, в 1999 году, после того как американская авиация по ошибке разбомбила посольство КНР в Белграде, китайские хакеры (которые называют себя 红客 («хункэ» - красный гость) по аналогии с китайским словом хакер — 黑客 («хэйкэ» - черный гость) организовали массовые атаки на американские правительственные сайты, в результате которых был взломан сайт Белого дома[[152]](#footnote-152). Именно данный инцидент можно назвать первым эпизодом конфликтного характера в американо-китайских отношениях в киберпространстве. Далее последовал случай, когда в 2001 году, пролетая над Южно-Китайским морем вблизи китайского острова Хайнань, американский самолет-разведчик EP-3E столкнулся с китайским истребителем J-811. Китайский летчик катапультировался, но, к сожалению, погиб. А команда американских разведчиков, вынужденная совершить экстренную посадку, оказалась на острове, где их арестовали (были отпущены на свободу, только после официального письма с извинениями китайским властям от правительства США). После данного происшествия американские и китайские хакеры в течение месяца совершали кибератаки на правительственные сайты в качестве мести. В китайских СМИ это назвали «большой войной» американских и китайских хакеров[[153]](#footnote-153). По подсчетам самих китайцев, тогда было взломано 1036 американских сайтов, включая 18 военных и 39 правительственных[[154]](#footnote-154).

В то же время стоит отметить, что кибератаки не являлись для КНР лишь ответом на американские действия на мировой арене. Осуществлялись атаки и без видимого повода, что, несомненно, тревожило американское политическое руководство. Примером является проникновение китайских хакеров в американскую информационную инфраструктуру, что стало причиной отключения электроэнергии на северо-западе США в 2003 году. Впоследствии атаки пострадали более 50 млн человек в штатах Мичиган, Нью-Йорк, Огайо, и даже в приграничных штатах Канады[[155]](#footnote-155). Позже американские спецслужбы признали виновником атаки Пекин, киберподразделения которого испытывали свои возможности.

Несмотря на уже открытые обвинения Пекина Вашингтоном, атаки продолжались, и следующим примером превентивных кибератак КНР может служить операция «Титановый дождь» 2004 года, в ходе которой сотни сетей NASA и других правительственных организаций США подвергались атакам в течение трех лет. Согласно опубликованным несколькими годами позже результатам расследования организации по обеспечению безопасности SANS Institute, атаки производились из китайской провинции Гуандун и, вероятно, были организованы китайскими военными хакерами[[156]](#footnote-156).

Примерно с конца 2000-х годов США начинает открыто обвинять Китай не только в атаках на правительственные структуры, но и в коммерческом шпионаже. В 2010 году США заявили, что пятью китайскими военными чиновниками была осуществлена попытка кражи коммерческих секретов. Американцы указали и на связь между армией Китая и коммерческими компаниями КНР. Так, Вашингтоном было заявлено, что китайской компанией, производящей сталь, были наняты специалисты НОАК, с целью создания базы данных для хранения украденной информации об американских разработках[[157]](#footnote-157). В заключении название компании указано не было.

Выше описанные конфликты позволяют нам проследить эволюцию китайской политики в киберпространстве в первом десятилетии XXI в. Если в начале 2000-х годов атаковалась в большей части засекреченная государственная информация и целью кибератак, к примеру, являлись сети NASA, то к 2010 году была осознана ценность технологической и экономической информации.

Несмотря на то, что в свободном доступе имеется информация о количестве совершаемых хакерских атак в мире, где на интерактивной карте можно увидеть не только направления кибератак в реальном времени, но и то, что именно Китай совершает больше всего киберпреступлений против американской экономики[[158]](#footnote-158), руководство КНР также множество раз заявляло о попытках США подорвать китайскую систему национальной безопасности. В отчёте, изданном в 2009 году, китайцы утверждают, что 40 процентов кибератак на китайские компьютеры были произведены именно в США[[159]](#footnote-159).

Таким образом, мы можем наблюдать зародившуюся конфронтацию США и КНР в сфере кибербезопасности. Началом данной конфронтации послужило решение КНР использовать свои возможности осуществления кибератак как ответ на внешнеполитические действия американского руководства. Успешность атак 1999 и 2001 годов дали толчок к развитию киберсферы в КНР. С 2003 по 2010 года КНР использует кибербезопасность как инструмент оказания давления на США, проводя превентивные кибератаки и проверяя предельные возможности своих создаваемых киберподразделений. Ответом США на данную политику КНР стало развитие собственных кадров в сфере кибербезопасности. Примером тут может послужить статистика из вышеупомянутого отчёта, опубликованного в 2009 году. В итоге, существовавшие политические разногласия привели также и к гонке информационных вооружений между КНР и США.

Вне государственного уровня политика кибербезопасности США и КНР напрямую затрагивает ТНК и поток инвестиций по всему миру. В совокупности данные факторы позволяют судить о том, что кибербезопасность для США и КНР относится к задачам первостепенной важности. Таким образом, США были вынуждены задуматься о необходимом выборе между экономическим процветанием и политической стабильностью, которая включает в себя национальную безопасность, и определить для себя, возможно ли дальнейшее сотрудничество с Китаем в целом[[160]](#footnote-160). В то же время американское руководство осознавало, что сотрудничества с КНР в киберпространстве по существующим правилам добиться будет проблематично. Во-первых, Китай одержим идеями полного контроля Интернета, власти КНР были критично настроены и по отношению к ICANN - Корпорации по управлению доменными именами и IP-адресами, которая формально является независимой международной некоммерческой организацией, но расположена в США и находится в юридической связи с Министерством торговли США. Китайцев не устраивала подотчётность ICANN властям США, представители КНР обвиняли ICANN в пособничестве США и игнорировании интересов других стран в киберпространстве, а после выдачи ICANN домена «.tw» Тайваню китайцы обвиняли США и в использовании Комиссии для реализации своих внешнеполитических целей. Наделение Тайваня отдельным от Китая доменом подрывало политику Китая в отношении Тайваня, официально рассматриваемому в КНР в качестве провинции. Несомненно, данное решение Комиссии показывало Китаю успешность киберполитики США в ключевых для КНР регионах. После Тайваньского доменного кризиса правительство КНР заявило, что США используют киберпространство как продолжение своей внешней политики и потребовали роспуска ICANN. В качестве альтернативы Китай предлагал создать международную организацию по управлению интернетом, которая контролировалась бы ООН. Результатом действий КНР стал проект Правил поведения в области обеспечения международной информационной безопасности, вынесенный на обсуждение Генеральной Ассамблее ООН в сентябре 2011 года. Данный проект контрастировал с проектом США и ЕС, согласно которому, в случаях, угрожающих национальной безопасности, допускается проникновение госструктур в международные информационные сети[[161]](#footnote-161).

Противостояние в сфере кибербезопасности между Китаем и США продолжалось. Так, в Учжэне на Первой Всемирной интернет-конференции китайские организаторы вечером подсунули под дверь участникам конференции черновик декларации об “Интернет-суверенитете”. Предполагалось, что данная декларация будет рассмотрена на пленарном заседании на следующий день. Черновик вызвал бурю возмущения. Журналисты узнали о нем в пятницу 21 ноября 2014 года, и новость о нем тут же была распространена во всех ведущих западных интернет-СМИ[[162]](#footnote-162).

Сам текст предлагаемой декларации был откровенно популистским и не предлагал никаких решений поднятых на конференции проблем. В первом пункте декларации китайцы говорят об угрозе Интернета для национального суверенитета. Согласно второму пункту мощь одного государства в киберсфере не должна означать угрозы для суверенитета другого государства. Третий пункт провозглашает необходимость государствам отказаться от использования кибератак. Данный пункт вызвал больше всего эмоций, так как, благодаря множеству исследований, всем участникам конференции уже давно было известно, что КНР использует кибератаки чаще любых других государств. В четвертом пункте говорится о борьбе с терроризмом. Также упоминается влияние Интернета на культурное развитие граждан и социализацию детей и молодёжи.

В результате декларация так и не была заявлена на заседании. Данной декларацией КНР пожелали показать себя борцами за разумное использование Интернета во благо общества и процветания, несмотря на огромное количество выдвигаемых против них обвинений, которые продолжали появляться. Так, в январе 2013 крупнейшие американские газеты обвинили Китай в том, что он взломал компьютеры, чтобы преследовать журналистов и мешать им сообщать о китайских чиновниках[[163]](#footnote-163). Также в феврале 2013 года фирмой Mandiant, базирующейся на предоставлении услуг кибербезопасности, был представлен крупный материал, разоблачающий китайский экономический шпионаж[[164]](#footnote-164). Особенностью данного доклада было то, что в нём не просто говорилось о подозрениях, а приводились данные о конкретном объекте, причастном к НОАК – военном подразделении 61398, где работают лучшие специалисты Китая в сфере кибербезопасности. Mandiant отслеживала всю кибер активность в течение нескольких лет, и ей удалось установить, что большинство атак на компании и государственные учреждения США, исходили именно от подразделения 61398[[165]](#footnote-165). В докладе были приведены доказательства, которые было крайне сложно оспорить. Установка конкретного источника атак стала поводом для неотложного диалога с властями Китая. Спустя пару месяцев после обнародования доклада Mandiant, который, безусловно, оказывал давление на Китай, государственное новостное агентство КНР 新华 (Синьхуа) сделало публикацию о том, что НОАК планирует провести в конце июня испытания, которые позволят протестировать новые виды сил с использованием цифровых технологий с целью подготовки к информационной войне[[166]](#footnote-166). Агентство отметило, что это первый случай, когда НОАК проводит подобные испытания.
Данное заявление стало вызывать опасения у западных СМИ, прозвавших испытание «цифровыми военными играми»[[167]](#footnote-167).

Разоблачительное признание Эдварда Сноудена в июне 2013 года лишь обострило обстановку. Согласно показаниям Сноудена, которые он дал уже будучи бежавшим в Гонконг, США взламывали китайский университеты, в том числе такие, как университет Цинхуа[[168]](#footnote-168). Университет Цинхуа являлся домом для 6 китайских опорных сетей, среди них были и Китайская образовательная и исследовательская сеть – Cernet[[169]](#footnote-169), через которую могут быть получены данные миллионов граждан КНР. Обнародование широкомасштабного надзора со стороны АНБ через американские интернет-фирмы подорвало одним ударом усилия Вашингтона, направленные на то, чтобы занять высокие позиции в отношении китайского шпионажа и усилия американских фирм по выстраиванию репутации независимости от Вашингтона. Более того, разоблачения Сноудена случились за несколько дней до первой встречи Си Цзиньпина на посту президента Китая с президентом Обамой. Информационный фон данной встречи был отрицательным: все СМИ писали только о Сноудене. Дальнейшие откровения Сноудена, кульминацией которых стало подтверждение о глубоком проникновении АНБ в Huawei, укрепили китайскую позицию по поводу американского шпионажа, даже когда средства массовой информации, сообщающие о китайском шпионаже сократились (во многом благодаря тому, что высокопоставленные китайские лидеры сдерживали активность НОАК после отчета Mandiant и после того как западные журналисты стали больше интересоваться сообщениями о файлах Сноудена).

Откровения Сноудена по поводу Huawei затронули одну из самых болезненных проблем в отношениях США и КНР в киберпространстве, ведь еще в конце 2012 года государственными структурами Китая и Соединенных Штатов были публично высказаны подозрения в создании оборудования (продукция фирм Huawei и ZTE с китайской стороны и Cisco с американской стороны) с недокументированными возможностями, благодаря которому происходили атаки на сети государств.

Вообще стоит отметить односторонность характера открытости Китая того времени в привлечении передовых западных ИКТ. Несмотря на то, что разработки собственного производства не афишировались в должной степени, их низкая цена позволила им завоевать мировой рынок. На сегодняшний день имидж компании Huawei, как одной из ведущих фирм в мире в сфере телекоммуникаций, позволяет КНР наращивать своё влияние в киберпространстве по всему миру. США воспринимают Huawei как угрозу и в военной сфере. У США вызывают вопросы состав руководства фирмы Huawei (к примеру, основателем и главой фирмы является служивший в НОАК Жень Чженвей)[[170]](#footnote-170). Учитывая приближенность военных кругов к осуществлению деятельности Huawei как в КНР, так и за рубежом, американцы сделали выводы об использовании продукции Huawei для осуществления слежки и шпионажа посредством установки в устройства различных шпионских программ и устройств.

Одними из первых серьезных ответных мер на китайские кибератаки стали заявления в 2014 году администрацией США о возможных санкциях против Китая. Такие меры, они заявили, могут быть приняты в ответ на хакерские действия со стороны китайских компаний, которые нарушают кибербезопасность с целью  получения экономической выгоды[[171]](#footnote-171). Стоит отметить, что американский президент сделал данное заявление за неделю до официального визита в США председателя КНР Си Цзиньпина, на переговорах с которым обсуждалась тема кибератак.

Уровень эскалации конфликта можно оценить, используя исследование корпорации RAND «Война с Китаем», которое было выпущено в 2016 году[[172]](#footnote-172). Согласно исследованию, в результате развития масштабного конфликта США потеряет немало авианосцев, подлодок, самолётов и ракет. Также будет нарушена и кибербезопасность страны в результате удара по компьютерным системам и спутникам. Авторы исследования сделали вывод, что нельзя говорить со стопроцентной уверенностью, что США способны выиграть кибервойну. По мнению авторов, явного победителя в данной войне не будет.

В то же время и Китай продолжал критиковать США за вмешательство в киберпространство КНР и попытки дестабилизации кибербезопасности страны. Пекин нередко упрекал[[173]](#footnote-173) США в использовании кибербезопасности для расширения американского влияния и утверждения американского политического строя в мире. Также в КНР отмечали, что США нередко нарушает право на частную жизнь граждан Китая, прикрываясь лозунгами о защите американской кибербезопасности[[174]](#footnote-174).

В 2017 наметилась новая тенденция в противостоянии США и КНР в киберпространстве. Представители обеих стран заявили о необходимости разделения киберпространства на различные зоны ответственности, если не получается договориться друг с другом о кооперации по кибербезопасности. На XIX съезде КПК был намечен план по перестройке мирового порядка и о размежевании сфер интересов с США для того, чтобы минимизировать возможные угрозы эскалации противоречий между Китаем и США. Несомненно, размежевание сфер интересов подразумевало и определение границ в киберпространстве. Реакции американцев на предложенный КПК план не последовало.

Осенью 2017 года генерал Лакруа, исполняющий обязанности генерального директора секретариата Межамериканского совета обороны, выступая с заявлением о необходимости создания зоны кибербезопасности между странами Северной и Южной Америки[[175]](#footnote-175), подчеркнул важность объединения стран для достижения кибербезопасности, так как малые страны, не обладающие значительными экономическими ресурсами не способны сами обеспечить собственную кибербезопасность. Лакруа отметил, что существуют тенденции вмешательства в киберпространство Латинской Америки как со стороны Китая, так и со стороны России. Для американских властей недопустимо распространение китайского ПО в Латинской Америке, так как с его помощью КНР сможет подключаться в внутренним американским сетям и осуществлять и экономический, и политический, шпионажи, а также кибератаки. Таким образом, мы видим, как между США и КНР началось противостояние за сферы влияния в киберпространстве.

В борьбе за сферы влияния в киберпространстве перевес сейчас не на стороне США. Американские фирмы до сих пор чаще других повергаются кибератакам. В 2017 году, в среднем убытки фирм, зарегистрированных в США, от кибератак составили 21,22 млн. долларов. На втором месте – заметно отстающая по убыткам Германия (11,15 млн. долларов)[[176]](#footnote-176). Для США действия Китая означают не только экономическую, но и политическую уязвимость. Несмотря на то, что основной целью китайских кибератак, начиная с 2010 года, является получение прибыли, американцы всерьез обеспокоены уязвимостью своей системы национальной безопасности. Руководство США понимает, что в определённых обстоятельствах они не смогут отразить массированную кибератаку со стороны КНР.

 Американцы обеспокоены и ростом уровня технологий, производимых в Китае и используемых по всему миру. Активная внутренняя экономическая политика Китая лишь способствует распространению китайских устройств на международном рынке, в том числе в США и в странах, наиболее тесно с США связанных. Однако несмотря на распространение китайских технологий практически во все страны мира, сами китайцы ограничивают влияние на Интернет извне. Все зарубежные компании, базирующиеся на территории Китая, любое юридическое лицо, должны действовать согласно требованиям руководства КНР, существующему законодательству: таким образом, фирмы, специализирующиеся в ИКТ-сфере, перед выходом на китайский рынок должны, как аналогичные китайские компании, получить специальное разрешение в Министерстве промышленности и информатизации[[177]](#footnote-177).

Одним из главных требований правительства Китая является запрет на распространение любой информации, способной подорвать доверие к власти. С данным требованием связан конфликт китайского руководства с Google, произошедший в 2010 году, когда поисковик не согласился с требованиями, отказавшись от фильтрации запросов китайского населения, что, безусловно, привнесло еще больший накал в непростые отношения Китая с Соединенными Штатами. Политическая составляющая разразившегося скандала привела к обвинениям в отсутствии свободы слова в КНР, приобретению корпорацией Google административных ресурсов.

Попытки ограничить вмешательство во внутренние сети по примеру КНР начали предпринимать и США, где стала популярной идея о создании государственной сети 5G[[178]](#footnote-178), которая будет служить щитом от кибератак со стороны Китая. Согласно документам, на создание сети должно уйти 3 года. В 2018 году планируется обсудить способы создания, развития и, разумеется, финансирования проекта.

Говоря о противостоянии Китая и США в киберпространстве, необходимо отметить партнёрство КНР в области кибербезопасности с Россией. Сообщения о намерении подписать договор о сотрудничестве в сфере международной информационной безопасности, о мерах доверия и предотвращения перерастания киберинцидентов в полномасштабный международный конфликт появились еще осенью 2014 года, когда подобное соглашение существовало только между РФ и США[[179]](#footnote-179), а соглашение КНР и США в данном направлении было приостановлено после официально предъявленных американскими властями обвинений в межгосударственном кибершпионаже. 30 апреля 2015 года на сайте Правительства РФ появилось распоряжение о подписании Соглашения[[180]](#footnote-180). Стоит отметить, что подписанию данного соглашения предшествовало многолетнее сотрудничество Китая и России в рамках ШОС, одной из наиболее активных структур на сегодняшний день, где вопрос информационной безопасности уже давно стоит на повестке дня[[181]](#footnote-181). Так, в 2007 году в рамках ШОС был утверждён Долгосрочный план действий по информационной безопасности[[182]](#footnote-182). В 2009 году между членами организации было подписано межправительственное соглашение, определившее основные направления взаимодействия государств по противодействию киберугрозам[[183]](#footnote-183). В ноябре 2016 года Ван Кайвэнь, заместитель Генерального секретаря ШОС, отметил, что создание международной информационной среды, для которой характерны мир, сотрудничество и гармония - один из главных приоритетов деятельности ШОС в области информационной безопасности[[184]](#footnote-184). Группа экспертов по международной информационной безопасности ШОС разработала «Правила поведения в области обеспечения международной информационной безопасности»[[185]](#footnote-185), однако процесс установления каких-либо правил в киберпространстве, по которым могли бы действовать акторы международных отношений, происходит достаточно сложно, даже если это пытается осуществить такая организация, как ШОС. Это связано опять же с разностью подходов к этому вопросу. Соединенные Штаты придерживались либерального подхода и, соответственно, выступали за минимальную фильтрацию контента в Интернете. Китай с Россией, наоборот, выступали за регулирование киберпространства, его контроль, и адаптацию к суверенитету государств. В области кибербезопасности, по большому счету, на сегодняшний день в мире три основных актора: США, КНР и РФ. Обвинения в атаках в основном исходили от США, когда со стороны КНР и РФ выражались претензии касательно монополизации управления мировым интернетом, американского вмешательства во внутренние дела стран. При всем этом никаких громких скандалов между КНР и РФ в киберпространстве в последние годы не происходило, поэтому установленное партнерство и соглашения между Россией и Китаем в этой сфере выглядят логично. К тому же, помимо соглашений на высшем уровне между Пекином и Москвой, практическое сотрудничество между странами также очень активно: совместное строительство Ростелекома с китайским Huawei подводной линии связи[[186]](#footnote-186), увеличение экспорта российского ПО в Китай.

Таким образом, противостояние США и КНР в киберпространстве стало продолжением политических разногласий в других сферах. Изначально Китай использовал киберсферу как инструмент ответа на внешнеполитические акции США. После ряда успешных кибератак в 2000-е годы руководство КНР осознало, что кибербезопасность является сильным инструментом воздействия на политику США. В ответ на китайские разработки в сфере кибербезопасности США начали разрабатывать зеркальные меры и также осуществлять кибератаки на китайские внутренние сети. Начиная с конца 2000-х годов целью китайских кибератак становится получение прибыли. КНР осуществляет экономический шпионаж посредством новейших информационных технологий. В то же время США также используют опыт Китая в киберпространстве и прибегают как к экономическому, так и к политическому шпионажу и осуществляют кибератаки, что было доказано показаниями Э. Сноудена, в которых сообщалось о тотальной слежке как за миллионами граждан и руководителями крупных компаний, так и за лидерами разных государств, включая Китай. Сноуден и его заявления послужили неким временным уравнителем в отношениях США и КНР в киберпространстве.

3.2. Попытки гармонизации интересов США и КНР в области обеспечения кибербезопасности

Несмотря на эскалацию противоречий США и КНР в киберпространстве, руководствами стран предпринимаются и попытки налаживания сотрудничества в данной области.

До 2013 года мы можем говорить о низком уровне контактов между институтами США и КНР по вопросам кибербезопасности. Только в 2013 году состоялся первый диалог по вопросам регулирования Интернет-деятельности на высшем уровне, который вскоре был назван переворотом в области кибербезопасности с учетом стратегических интересов США и КНР. Си Цзиньпин, генеральный секретарь ЦК КПК и председатель КНР, встретился с Джейкобом Лью, 76-м министром финансов США, где предметом разговора, помимо ядерной угрозы со стороны КНДР, стала и область кибербезопасности[[187]](#footnote-187). Министр финансов США подчеркнул, что Вашингтон видит разницу между преступными кибератаками, которые являются привычной угрозой, и шпионажем со стороны предприятий, спонсированных государством[[188]](#footnote-188). Одной из главных предпосылок данной встречи являлся телефонный разговор между Си Цзиньпином и Бараком Обамой непосредственно после того, как Си Цзиньпин был избран генеральным секретарём ЦК Коммунистической партии КНР и председателем КНР. В это же время новый премьер-министр КНР Ли Кэцян заявил о заинтересованности в установлении мирных отношений с США[[189]](#footnote-189), именно тогда впервые прозвучало понятие нового типа отношений двух стран.

Итогом переговоров на высшем уровне между США и КНР стало создание рабочей группы по вопросам кибербезопасности в апреле 2013 года[[190]](#footnote-190). Кооперация двух стран была возможной, так как руководства КНР и США стремились к осуществлению различных целей. США стремились ограничить сетевой шпионаж и уменьшить экономические потери в результате слежки со стороны КНР, а в КНР в тот момент были сосредоточены на ограничении диссидентской информации для китайских граждан, так как она была способна подорвать авторитет местного правительства. Первые встречи рабочей группы были проведены в рамках пятого американо-китайского стратегического и экономического диалога в Вашингтоне[[191]](#footnote-191).

Создание рабочей группы являлось одной из попыток Соединенных Штатов наладить еще больше пошатнувшиеся отношения с Китаем после раскрытия Эдвардом Сноуденом информации о кибершпионаже против Китая, проводимом со стороны Америки примерно с 2009 года, однако, ни США, ни КНР не были готовы к тесному сотрудничеству. КНР продолжала экономический шпионаж, а США по-прежнему предпринимали попытки дестабилизировать внутреннее положение дел в Китае. После официальных обвинений в адрес Китая со стороны США в коммерческом шпионаже, работа группы была свернута.

Спустя два года в 2015 году в ходе встречи Обамы и Си Цзиньпина были выделены основные мотивы новой попытки сотрудничества двух государств[[192]](#footnote-192). Наряду с обеспечением мира, сотрудничеством в космической сфере и ядерной энергетике, была отмечена и кибербезопасность. Сообщалось, что обе стороны повторно утвердили своё намерение ввести обязательства в области кибербезопасности с сентября 2015 года для борьбы с преступной киберактивностью, взломами или намеренной поддержкой кибернетической кражи интеллектуальной собственности для получения коммерческой выгоды. Как сказал Си Цзиньпин тогда же в сентябре 2015 года: «Холодная война уже давно закончилась. США и КНР должны предпринять совместные усилия по созданию новой модели отношений между двумя странами и реализации бесконфликтного, неконфронтационного, взаимного уважения и сотрудничества»[[193]](#footnote-193).

Важной вехой в развитии сотрудничества двух стран по кибербезопасности стало подписание соглашения[[194]](#footnote-194). Стороны договорились по следующим пунктам: осуществлять борьбу и пресекать попытки кибератак; не допускать экономический (коммерческий) шпионаж; содействовать кибер-нормотворчеству; активно бороться с киберпреступностью во всех её проявлениях. Более подробно данные области были расписаны в документе на сайте Федерации американских учёных.

Существует несколько противоречивых точек зрения касательно данного договора. Некоторые аналитики считали, что это соглашение являлось долгожданным шагом, что оно свидетельствует о правильных тенденциях в китайско-американском сотрудничестве в киберпространстве и может стать первым шагом в сокращении китайских кибератак[[195]](#footnote-195). По их мнению, успехом дипломатии Обамы стало открытое осуждение экономического шпионажа в договоре, в результате чего Китай согласился признать экономический шпионаж как отдельное преступление в сфере кибербезопасности[[196]](#footnote-196). Помимо этого мы можем наблюдать количественное снижение числа кибератак после подписания договора[[197]](#footnote-197). Для КНР данный договор также открывал новые возможности в сфере кибербезопасности, позволял им расширять сферы своей киберактивности и проводить переговоры по кибербезопасности с западными странами.

В то же время в США некоторыми был негативно воспринят данный договор. Ставился вопрос о соблюдении данного договора со стороны КНР[[198]](#footnote-198). Экономические выгоды от нарушения данного договора превышали, по мнению скептиков, ответственность КНР перед США в выполнении условий данного договора. Для КНР было невыгодно прекращение коммерческого шпионажа и беспрекословное соблюдение условий договора[[199]](#footnote-199). Некоторые аналитики прямо говорили о бесполезности соглашения, так как Си Цзиньпин так и не признал факт экономического шпионажа, осуществляемого непосредственно КНР. В то же время критиковались и механизмы соблюдения договора по киберпространству. Скептики утверждали, что в договоре не прописаны санкции за нарушение положений Соглашения и отсутствует государственный или надгосударственный орган, следящий за исполнением обеими сторонами условий Соглашения[[200]](#footnote-200). Также существовала такая проблема, как толкование договора. Условия соглашения требовали от двух стран соблюдения их соответствующих национальных законов. Как было сказано в 1 главе данного исследования, Соединенные Штаты и Китай имеют принципиально разные подходы к управлению киберпространством внутри стран.

В связи с этим в КНР и США после подписания соглашения всё чаще выступали эксперты, заявляя о необходимости в дополнении длинного перечня китайско-американских расхождений признанием различия подходов в понимании киберугрозы и кибербезопасности. Попыткой поиска решений был доклад RAND от 2016 года, где Скотт Гарольд и Мартин Либби после подробного анализа позиции США и КНР в киберпространстве, предлагают модель поиска согласия в вопросах на которые у обеих сторон разные взгляды[[201]](#footnote-201).

Некоторые аналитики назвали это соглашение долгожданным шагом, свидетельствующим о правильных тенденциях в китайско-американском сотрудничестве в киберпространстве и важным шагом в сокращении китайских кибератак[[202]](#footnote-202).

Соответственно, подписанное соглашение Обамы и Си не разрешило все имевшиеся проблемы, но оно, бесспорно, послужило отличным инструментом для ослабления существовавшей напряженности по кибер-вопросам. В целом, несмотря на множество недочетов данного соглашения, оно рассматривается как успешное, как минимум потому, что удалось достичь признания Китаем признаков коммерческого кибер шпионажа.

Соглашение стало поводом для следующей значимой встречи представителей США и КНР по вопросам кибербезопасности в Пекине в 2016 году[[203]](#footnote-203), которая по своей сути являлась продолжением встречи 2015-го года. Делегацию США возглавил координатор госдепартамента по проблемам в киберпространстве Кристофер Пэйнтер, также в обсуждении с американской стороны участвовали представители Пентагона, Министерства юстиции, Министерства внутренней безопасности и других ведомств. В делегацию Китая, возглавляемую директором Департамента по контролю за вооружениями МИД Ван Кун, также входили представители Министерства обороны, Министерства промышленности и информационных технологий, Министерства общественной безопасности, профильной администрации КНР по вопросам киберпространства и других ведомств. Сюзанн Сполдинг, представляющая Департамент внутренней безопасности США, отметила, что и Китай, и США заняты созданием линий связи для обмена информацией о кибер-угрозах[[204]](#footnote-204). Прогресс, очевидно, не был быстрым, ведь прошел на тот момент почти год с момента подписания соглашения, а такая важная мера, как линии связи, не была реализована.

Тогда же в июне 2016 года после обвинений со стороны Соединённых Штатов Америки во взломе систем американских компаний Китаем, китайские и американские официальные лица объявили о совместных планах на сближение киберстратегий государств. Посол США в Китае Макс Бокус тогда отметил: «Сегодня мы здесь для того, чтобы обеспечить соблюдение соглашений, сделанных двумя президентами; решений, которые показывают, что мы можем совместно работать в областях, в которых есть различия, чтобы выстроить отношения сотрудничества». По его словам, сотрудничество в области кибербезопасности должно стать важной частью двусторонних отношений Китая и США, и каждый совместно сделанный шаг позволит добиться большего доверия[[205]](#footnote-205). Уже имелись фактические доказательства успешности подписанного соглашения для США. Так, в этом же месяце издание Bloomberg сообщило, что, по мнению официальных лиц из Министерства юстиции США, соглашение о кибербезопасности США с Китаем помогло снизить число случаев взломов. Так как правительственные агентства всегда следят за всевозможными атаками, исходящими из Китая, случаи нападений действительно стали реже, отметил министр юстиции и генеральный прокурор Джон Карлин. Карлин процитировал доклад компании FireEye Inc., в соответствии с которым с августа случаи атак из Китая уменьшились на 80%[[206]](#footnote-206).

В декабре 2016 года состоялась уже третья встреча на высоком уровне в Вашингтоне, на которой продолжала рассматриваться тема киберпространства, киберпреступности и кибербезопасности стран[[207]](#footnote-207). Во встрече приняли участие министр общей безопасности Китая и член Госсовета КНР, Го Шэнкунь, а также министр юстиции и генеральный прокурор США, Лоретта Линч. В соответствии с опубликованной на официальном сайте Департамента внутренней безопасности США информации по поводу проведенной встречи, обе стороны достигли понимания по следующим пунктам: борьба с киберпреступностью и другими видами преступности в киберпространстве; защита сетей; использование технологий и коммуникаций, которые способствуют террористическим действиям; механизм горячей линии; продолжение диалога: стороны согласились провести аналогичную встречу на высшем уровне в декабре 2017 года[[208]](#footnote-208). Все три встречи, которые были проведены в 2016 году и так или иначе касались урегулирования вопроса кибербезопасности в отношениях США и КНР, имели большое значение для обеих сторон.

В конце 2016 года перед официальным вступлением Дональда Трампа в должность президента США, министр общественной безопасности КНР Го сделал заявление, что «Китай готов прилагать максимальные усилия для дальнейшего развития двустороннего сотрудничества в области кибербезопасности с новой административной командой»[[209]](#footnote-209), что было достаточно важным шагом, показывающим стремление Китая продолжить начатое налаживание отношений в киберпространстве. Президент Дональд Трамп в свою очередь пообещал, что у него будет собственный план действий США по кибербезопасности, который он представит в течение 90 дней после вступления в должность, но позже эта дата была отложена[[210]](#footnote-210), в целом отношение нового президента многие оценивали как агрессивно настроенное.

Однако, несмотря на это, в 2017 году успешно прошли четыре китайско-американских диалога на высоком уровне. Среди которых был проведен и октябрьский диалог по вопросам кибербезопасности, в ходе которого состоялся углубленный обмен мнениями по ситуации с двусторонним сотрудничеством[[211]](#footnote-211). Это был важный шаг в осуществлении стратегического направления обеих стран. Председатель КНР Си Цзиньпин отметил: «Нам необходимо превратить вопросы кибербезопасности в точку китайско-американского сотрудничества, а не точку трений и конфликтов»[[212]](#footnote-212).

Сразу после того, как диалог между правоохранительными органами по кибербезопасности США и Китая состоялся, 6 октября появилась большая статья известного китайского эксперта, тесно связанного с китайской администрацией в сфере киберпространства, а также директора Исследовательского центра управления киберпространством в Университете Фудань, Шень И, где он выразил обеспокоенность тем, что Трамп – представитель республиканской партии США и его взгляды на развитие диалога между КНР и США могут слишком сильно отличаться от уже начатого пути развития отношений в киберпространстве с администрацией Обамы. «Необходимо, чтобы мы сохраняли трезвое, последовательное и четкое признание того, как отношения в сфере кибербезопасности будут стратегически влиять на отношения между США и Китаем», - пишет он. Также Шень отметил стремление Китая к поиску прочного сотрудничества с США, подчеркнул становление Китая все более уверенным, более искусным и более активным игроком в определении повестки дня китайско-американских отношений кибербезопасности.

В целом, оценивая развитие американо-китайского диалога в области кибербезопасности, необходимо отметить низкий уровень контактов до 2013 года, связанный с накалёнными отношениями в киберпространстве и нежеланием идти на уступки. Созданная по результатам встречи 2013-го года Группа по вопросам кибербезопасности достаточно скоро прекратила свою деятельность из-за продолжившихся атак и обвинений. И только спустя два года Китай и Соединенные Штаты снова на официальном уровне утвердили свои намерения о введении общих норм в области кибербезопасности для борьбы с киберпреступностью, которая беспокоила обе стороны. Тогда же в 2015 году было подписано важное соглашение, которое, несмотря на то, что считалось достаточно противоречивым, в итоге оказалось успешным, так как после подписания наблюдалось количественное снижение кибератак. После этого в 2016-м году было проведено три успешных встречи по вопросам кибербезопасности, в 2017-м году - около четырех диалогов на высоком уровне, среди которых были и диалоги по вопросам кибербезопасности.

Этот тип эволюции отражает чувствительность и сложность принятия совместных решений для США и КНР. Углубление сотрудничества в области кибербезопасности означает для обеих стран, что им необходимо принять максимально прагматичный подход и конкретные меры по решению назревших кибервопросов.  Помимо совместной работы, нацеленной на сокращение атак, обе стороны должны также активизировать сотрудничество в области кибер-контртерроризма. Киберпространство обеспечивает практически идеальную платформу для потенциальных террористов. И в случае обретения ими способности вести кибервойну, потенциальные издержки для международного сообщества могут стать ужасно огромными. Именно по данной причине США и КНР следует сотрудничать и координировать свои действия также с остальным миром, чтобы предотвратить возможные атаки и их последствия.

ЗАКЛЮЧЕНИЕ

Понятие кибербезопасности зародилось не так давно, оно многогранно и характеризуется множеством составляющих. Исследуемые США и КНР имеют принципиально разные подходы к управлению киберпространством внутри стран. Соединенные Штаты трактуют кибербезопасность с позиции предоставления гарантий населению доступа к информации. Защита гражданских свобод и права на частную жизнь остаются фундаментальными целями в практически всех издаваемых законодательных актах США, затрагивающих политику в киберпространстве. В Китае же руководство страны в процессе формирования политики в области кибербезопасности уделяет внимание возрастающей роли интернета, взаимозависимости стран в глобальном киберпространстве, а также возможным угрозам, поэтому видит необходимость в контроле внутреннего интернета и осуществляет его.

Руководствами стран принимаются меры по защите своих данных в информационной сети, формируются системы обеспечения кибербезопасности. Институциональный аспект обеспечения кибербезопасности в США отличается своей трехуровневой системой, позволяющей действовать каждой структуре автономно, при этом соблюдая общую стратегию. В китайской системе обеспечения кибербезопасности необходимо выделить интеграцию военных и гражданских структур, модернизацию НОАК, нацеленную на развитие информатизации и улучшение взаимодействия всех структур при проведении совместных операций. Стоит отметить, что и у Соединенных Штатов, и у Китая, формирование институтов продолжается, происходит постоянный поиск лучших специалистов, финансирование институтов, изучающих вопрос кибербезопасности, а также комплексный мониторинг различных структур по обеспечению защиты киберпространства.

Рассмотрев законодательные базы США и КНР в области кибербезопасности, становится ясно, что и Китай, и Соединенные Штаты, осознают возрастающую роль интернета, необходимость во внедрении кибербезопасности во все информационные структуры, и прилагают усилия, чтобы укрепить не только свою национальную информационную безопасность, но и внести вклад в развитие норм по регулированию международного киберпространства.

Проанализировав основные конфликты и споры в киберпространстве между США и КНР, становится ясно, что между странами существует противостояние, ставшее продолжением политических разногласий в других сферах. Китайский шпионаж, в большей части коммерческий, американская слежка, доказанная откровениями Сноудена, всё это длится в течение достаточно долгого времени. Уровень развития информационных технологий в обеих странах оказывает взаимное давление США и КНР, создавая киберугрозы в диапазоне отношений, касающихся и политических, и деловых, и экономических интересов. Это делает китайско-американский диалог в вопросах кибербезопасности еще более актуальным и важным. Несмотря на сложность принятия совместных решений для США и КНР, страны все же идут на контакт и проводят встречи различных уровней, подписывают совместные соглашения, осознавая важность такой общей сферы, как киберпространство, и признавая наличие общих угроз, среди которых терроризм, против которого необходимо сотрудничество и координация совместной деятельности.

Обсуждая принятие единой стратегии в киберпространстве, оба государства согласны, что без общепринятых норм поведения в Интернете дальнейшее международное сотрудничество в данном вопросе не представляется возможным, они продолжают участвовать в инициативах по построению безопасности в киберпространстве международного уровня, однако пойти на уступки по определяющим вопросам, таким, как взгляды США и КНР на свободу Интернета и информации, на сегодняшний день представляется маловероятно возможным для них. Несмотря на это, стоит отметить, что сосредоточив внимание на этических принципах кибербезопасности, Соединенные Штаты и Китай способны наметить успешный путь в решении спора. Будучи основными игроками в глобальном киберпространстве, и КНР, и США могут рассчитывать на дивиденды от совместного сотрудничества в разработке и установлении общих норм в киберпространстве. Поскольку сложившееся взаимное недоверие в киберпространстве негативно влияет на двусторонние отношения в целом, синергия в установлении норм способна ослабить напряжения между ними. Кроме того, сотрудничество США и КНР в решении данного вопроса может стать основополагающим шагом в содействии многосторонним международным усилиям, направленным на обеспечение безопасного мирового киберпространства.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники:

Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности. // Международный союз электросвязи. – 2008. URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения: 16.01.2018).

Концепция стратегии кибербезопасности Российской Федерации // Сайт Совета Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 22.12.2017).

Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // Министерство Иностранных Дел Российской Федерации. 29.01.2015. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset\_publisher/UsCUTiw2pO53/content/id/916241 (дата обращения: 04.04.2018).

Один из приоритетов ШОС – стремление создать международную информационную среду, для которой характерны мир, сотрудничество и гармония // Шанхайская Организация Сотрудничества. 27.11.2016. URL: http://rus.sectsco.org/news/20161127/160697.html (дата обращения: 04.04.2018).

Официальное описание проекта Подводная ВОЛС «Камчатка – Сахалин – Магадан» // Ростелеком. URL: https://www.rostelecom.ru/projects/FarEast\_FOCL/about/ (дата обращения: 04.04.2018).

Распоряжение от 30 апреля 2015 г. № 788-р. О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Правительство Российской Федерации. 30.04.2015. URL: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 04.04.2018).

Резолюция A/RES/57/239, принятая Генеральной Ассамблеей [по докладу Второго комитета (A/57/529/Add.3)]. 57/239. Создание глобальной культуры кибербезопасности. 20.12.2002 // Генеральная Ассамблея Организации Объединенных Наций. – 31.01.2003. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата обращения: 27.12.2017).

Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская Организация Сотрудничества. 16.06.2009. URL: http://rus.sectsco.org/load/203996/ (дата обращения: 04.04.2018).

64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур // Генеральная Ассамблея ООН. 21.12.2009. URL: http://www.un.org/ga/search/view\_doc.asp?symbol=A/RES/64/211&referer=https://www.google.ch/&Lang=R (дата обращения: 16.03.2018).

An Act to establish the Department of Homeland Security, and for other purposes. Public Law 107–296. // 107th Congress. Homeland Security Act of 2002. // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/hr\_5005\_enr.pdf (дата обращения: 26.01.2018).

Average annualized cost of cyber attacks on companies in selected countries as of August 2017 (in million U.S. dollars) // The Statistic Portal Statista. URL: https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ (дата обращения: 31.03.2018).

Budget in brief. Fiscal year 2017 // U.S. Department Of Homeland Security 16.02.2016. URL: https://www.dhs.gov/sites/default/files/publications/FY2017\_BIB-MASTER.pdf (дата обращения: 01.03.2018).

Convention télégraphique internationale de Paris (1865) et Règlement de service international (1865) // ITU. URL: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.1.61.fr.200.pdf (дата обращения: 16.01.2018).

Department of Defense Strategy for Operating in Cyberspace. / U.S. Department of Defense, 2011. // U.S. Department of Defense. URL: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения: 28.02.2018).

Department Of Homeland Security. Statement On The President’s Fiscal Year 2019 Budget // U.S. Department Of Homeland Security 12.02.2018. URL: https://www.dhs.gov/news/2018/02/12/department-homeland-security-statement-president-s-fiscal-year-2019-budget (дата обращения: 01.03.2018).

Digital Attack Map. Top daily DDoS attacks worldwide // Digital Attack Map. URL: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17650&view=map (дата обращения: 22.03.2018).

Fact sheet: President Xi Jinping’s State Visit to the United States // The White House. Office of the Press Secretary. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (дата обращения: 11.04.2018).

First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes // Office of Public Affairs, U.S.the Department of Justice. 01.12.2015. URL: http://worldjpn.grips.ac.jp/documents/texts/USC/20151201.D1E.html (дата обращения: 07.04.2018).

First U.S.-China Law Enforcement and Cybersecurity Dialogue // Department of Justice. Office of Public Affairs. 06.10.2017. URL: https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue (дата обращения: 18.04.2018).

Global Cybersecurity Index (GCI) 2013. ITU 2013 // International Telecommunication Union – 2013. URL: https://www.itu.int/md/T13-SG17-R-0004 (дата обращения: 17.01.2018).

Global Cybersecurity Index (GCI) 2017. ITU 2017 // International Telecommunication Union – 2017. URL: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (дата обращения: 17.01.2018).

Gompert David C., Cevallos Astrid Stuth, Garafola Cristina L. War with China. Thinking Through the Unthinkable / David C. Gompert, Astrid Stuth Cevallos, Cristina L. Garafola // RAND Corporation. 28.07.2016. URL: https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1100/RR1140/RAND\_RR1140.pdf (дата обращения: 28.03.2018).

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. / General Assembly of the United Nations. 24.06.2013 / General Assembly of the United Nations .URL: http://www.un.org/ga/search/view\_doc.asp?symbol=A/68/98 (дата обращения: 28.02.2018).

Harold Scott W., Libicki Martin C., Cevallos Astrid Stuth. Getting to Yes with China in Cyberspace / Scott W. Harold, Martin C. Libicki, Astrid Stuth Cevallos. // RAND Corporation. 2016. URL: https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1300/RR1335/RAND\_RR1335.pdf (дата обращения: 28.03.2018).

Hearing on NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative // U.S. Senate Committee on Homeland Security and Governmental Affairs 4.03.2008. URL: https://www.hsgac.senate.gov/hearings/nspd-54/hspd-23-and-the-comprehensive-national-cyber-security-initiative (дата обращения: 31.01.2018).

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 17.12.2003. URL: https://www.dhs.gov/homeland-security-presidential-directive-7 (дата обращения: 25.02.2018).

International respect needed in cyber security: official. // Xinhua, English.news.cn. 08.06.2013. URL: http://english.peopledaily.com.cn/90883/8278445.html (дата обращения: 13.03.2018).

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / The White House. May 2011 // Office of the White House Press Secretary. URL: https://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_for\_cyberspace.pdf (дата обращения: 25.02.2018).

International Strategy of Cooperation on Cyberspace // 新华网Xinhua News. 01.03.2017. URL: http://www.xinhuanet.com/english/china/2017-03/01/c\_136094371.htm (дата обращения: 16.03.2018).

Joint Summary of Outcomes: Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue // U.S.the Department of Homeland Security. 15.06.2016. URL: http://worldjpn.grips.ac.jp/documents/texts/USC/20160615.D1E.html (дата обращения: 15.04.2018).

Mr. Mccaul (for himself, Mr. Thonpson of Mississippi, Mr. Ratcliffe, Mr. Richmond, Mr. Katko, Mr. Hurd, Mr. Donovan, Mr. Gallagher, Mr. Higgins of Louisiana, Mr. Garett, and Mr. Fitzpatrick) H. R. 3359. Cybersecurity and Infrastructure Security Agency Act of 2017 / Mr. Mccaul (for himself, Mr. Thonpson of Mississippi, Mr. Ratcliffe, Mr. Richmond, Mr. Katko, Mr. Hurd, Mr. Donovan, Mr. Gallagher, Mr. Higgins of Louisiana, Mr. Garett, and Mr. Fitzpatrick) // U.S. House of Representatives. Document Repository. 24.07.2017. URL: http://docs.house.gov/billsthisweek/20171211/HR3359.pdf (дата обращения: 31.01.2018).

National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 01.03.2018).

National Strategy for Information Sharing and Safeguarding // The White House, 2012. URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy\_1.pdf (дата обращения: 28.02.2018).

Pellerin Cheryl. U.S. Cyber Command Chief Testifies on Challenges, Security Initiatives. / Cheryl Pellerin. // U.S. Department of Defence. 5.04.2016. URL: https://www.defense.gov/News/Article/Article/713755/us-cyber-command-chief-testifies-on-challenges-security-initiatives/ (дата обращения: 31.01.2018).

Peter Warren Singer: "Cybersecurity and Cyberwar: What Everyone Needs to Know" | Talks at Google. // Youtube “Talks at Google” channel. 10.02.2014.URL: https://www.youtube.com/watch?v=h0SXO5KUZIo (дата обращения: 25.12.2017).

Presidential Decision Directive/NSC-63 / The White House, Washington // The White House. 22.05.1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (дата обращения: 25.02.2018).

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order. // The White House. 11.05.2017. URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (дата обращения: 31.01.2018).

Press Briefing by Principal Deputy Press Secretary Sarah Sanders and Homeland Security Advisor Tom Bossert // The White House. 11.05.2017. URL: https://www.whitehouse.gov/briefings-statements/press-briefing-principal-deputy-press-secretary-sarah-sanders-homeland-security-advisor-tom-bossert-051117/ (дата обращения: 31.01.2018).

Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference // The White House. Office of the Press Secretary. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint (дата обращения: 07.04.2018).

Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California. News trancript / U.S. Department of Defence. 23.04.2015 // U.S. Department of Defence. URL: https://www.defense.gov/News/Transcripts/Transcript-View/Article/607043/remarks-by-secretary-carter-at-the-drell-lecture-cemex-auditorium-stanford-grad/ (дата обращения: 28.02.2018).

Report of the Chairman of HLEG To ITU Secretary-General, Dr. Hamadoun I. Touré by Chief Judge Stein Schjølberg, Judge at the Moss Tingrett Court, Norway // ITU Global Cybersecurity Agenda (GCA). High-Level Experts Group (HLEG). URL: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (дата обращения: 16.01.2018).

Rollins J., Henning A. C. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. / J. Rollins, A.C. Henning // The White House, Washington DC, 2009. URL: https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf (дата обращения: 31.01.2018).

Schmitt Georg. To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity / Georg Schmitt // World Economic Forum 24.01.2018. URL: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/ (дата обращения: 26.01.2018).

Segal Adam. Stabilizing cybersecurity in the U.S.-China relationship. / Adam Segal // The National Bureau of Asian Research. September 2015. URL: http://nbr.org/downloads/pdfs/psa/US-China\_brief\_Segal\_Sept2015.pdf (дата обращения: 07.04.2018).

1. The Comprehensive National Cybersecurity Initiative // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 31.01.2018).

The DOD Cyber Strategy / U.S. Department of Defense. April 2015. // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf (дата обращения: 28.02.2018).

The National Strategy to Secure Cyber Space // The White House, Washington DC, USA, 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 26.01.2018).

Third U. S. – China High-Level Joint Dialogue on Cybercrime and Related Issues // Homeland Security. 8.12.2016. URL: https://www.dhs.gov/news/2016/12/08/third-us-china-highlevel-joint-dialogue-cybercrime-and-related-issues (дата обращения: 15.04.2018).

US Deterrence against Chinese Cyber Espionage. The Danger of Proliferating Covert Cyber Operations // Netherlands Institute of International Relations. September 2015. URL: https://www.academia.edu/15721992/US\_Deterrence\_against\_Chinese\_Cyber\_Espionage\_The\_Danger\_of\_Proliferating\_Covert\_Cyber\_Operations (дата обращения: 28.03.2018).

White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace\_Policy\_Review\_final\_0.pdf (дата обращения: 22.12.2017).

1. Xinhua Headlines: Xi outlines blueprint to develop China's strength in cyberspace // 新华网 Xinhua News. 21.04.2018. URL: http://www.xinhuanet.com/english/2018-04/21/c\_137127374.htm (дата обращения: 16.03.2018).
2. 中华人民共和国网络安全法 Чжунхуа жэньминь гунхэго ванло аньцюань фа [Закон о кибербезопасности КНР] // 全国人民代表大会 Цюаньго жэньминь дайбяо дахуэй [Всекитайское собрание народных представителей]. 7.11.2016. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content\_2001605.htm (дата обращения: 22.12.2017).

中央网络安全和信息化领导小组成立:从网络大国迈向网络强国Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу чэнли: цун ванло даго май сян ванло цянго [Ведущая центральная группа по вопросам сетевой информации и информатизации: от крупного информационного государства к крупной интернет-державе] // 新华社Синьхуа шэ［Агентство Синьхуа]. URL: http://news.xinhuanet.com/politics/ 2014 02/27/c\_119538719.htm (дата обращения: 10.02.2018).

中央网络安全和信息化领导小组成立Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу чэнли [Основание ведущей группы по кибербезопасности и информатизации] // 新华网 Синьхуаван [Информационное агентство Синьхуа] 28.02.2014. URL: http://www.xinhuanet.com/info/2014-02/28/c\_133148759.htm (дата обращения: 13.03.2018).

中央网络安全和信息化领导小组第一次会议召开 习近平发表重要讲话Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу диицы хуэйи чжаокай Сицзиньпин фабяо чжунъяо цзянхуа [Первое совещание Центральной группы по информационной безопасности и информатизации. Важная речь Си Цзиньпина] // 中华人民共和国国家互联网信息办公室Чжунхуа жэньминь гунхэго гоцзя хуляньван синьси баньгунши [Национальное интернет-информационное бюро КНР] 27.02.2014. URL: http://www.cac.gov.cn/2014-02/27/c\_133148354.htm (дата обращения: 13.03.2018).

1. 习近平：让互联网更好造福国家和人民Си Цзиньпин：жан хуляньван гэнхао цзаофу гоцзя хэ жэньминь [Си Цзиньпин: улучшить интернет для страны и для народа] // 新华社Синьхуа шэ［Агентство Синьхуа］19.04.2016. URL: http://www.xinhuanet.com/politics/2016-04/19/c\_1118672059.htm (дата обращения: 08.02.2018).

军地联手搭建融合创新平台应对网络空间安全威胁 Цзюньди ляньшоу дацзянь жунхэ чуансинь пинтай индуй ванло кунцзянь аньцюань вэйсе [В Пекине создан Инновационный центр военно-гражданского слияния в области кибербезопасности]// 新华网Синьхуаван. 26.12.2017. URL: http://www.xinhuanet.com/2017-12/26/c\_1122170496.htm (дата обращения: 13.02.2018).

国家信息化领导小组关于加强信息安全保障工作的意见 (中办发[2003] 27号) Гоцзя синьсихуа линдао сяоцзу гуаньюй цзяцян синьси аньцюань баочжан гунцзо дэ ицзянь (Чжунбаньфа [2003] 27 Хао) [Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности (опубликовано Главным управлением ЦК КПК № 27 от 2003 г.)] // EIC. XM. GOV. CN: Информационный центр г. Сямэнь. URL: http://eic.xm.gov.cn/xgfw/aqcp/djbh/201411/P020141104292325316962.pdf (дата обращения: 09.03.2018).

手机加密的方法Шоуцзи цзями дэ фанфа [метод шифрования сотовой связи]. 发明专利说明书Фамин чжуаньли шоминшу [описание патента изобретения]// 中华人民共和国国家知识产权局Чжунхуа жэньминь гунхэго гоцзя чжиши чаньцюаньцзюй [Государственное ведомство интеллектуальной собственности Китайской Народной Республики] 9.09.1999 URL: https://patentimages.storage.googleapis.com/73/fb/81/f7540b88b0da7a/CN1115924C.pdf (дата обращения: 09.03.2018).

联网新闻信息服务管理规定 Ляньван синьвэнь синьси фуу гуаньли гуйдин [Положение по регулированию новостных информационных услуг в интернете] // CAC. GOV. CN: официальный сайт Центральной ведущей группы по кибербезопасности. URL: http://www.cac.gov.cn/2005‑09/30/c\_126468838.htm (дата обращения: 09.03.2018).

胡锦涛在全国科学技术大会上的讲话(全文) Хуцзиньтао цзай цюань гокэсюэ цзишудахуэйшан дэ цзянхуа (Цюань вэнь) [Речь Ху Цзиньтао на Национальной научно-технической конференции (полная речь)] //中国共产党新闻Чжунго гунчаньдан синьвэнь [Новости КПК] 10.01.2006. URL: http://cpc.people.com.cn/GB/64093/64094/4455445.html (дата обращения: 09.03.2018).

譚瑾瑜Тан Цзиньюй. 大陸十三五規劃趨勢與台灣因應建言Далу шисаньу гуихуа цюши ю тайвань иньин цзяньянь [Тенденции тринадцатой пятилетки в Китае и ответ Тайваня на выдвинутые предложения] / 譚瑾瑜Тан Цзиньюй // 財團法人.國家政策研究基金會 Цайтуан фажэнь. Гоцзя чжэнцэ яньцзю цзицзиньхуи [Консорциум. Фонд исследований национальной политики]. 02.12.2014. URL: https://www.npf.org.tw/3/14471 (дата обращения: 13.03.2018).

郝叶力博士Хао Ели боши [Доктор Хао Ели]// 数据治理和网络安全研究联盟Шуцзюй чжили хэ ванло аньцюань яньцзю ляньмэн [Исследовательский центр по дата-данным и кибербезопасности]. URL: http://www.dgcs-research.net/a/lianmengchengyuan/lianmengzhuyaochengyuan/2018/0103/68.html (дата обращения: 10.02.2018).

2002年中国的国防 2002 нянь чжунго дэ гофан [Национальная оборона Китая в 2002 году] // 中华人民共和国国务院新闻办公室Чжунхуа жэньминь гунхэго гоуюань синьвэнь бангунши [Информационное бюро Государственного совета Народной Республики Китай]. 12.2002. URL: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925.htm (дата обращения: 09.03.2018).

2006━2020年国家信息化发展战略2006━2020 нянь гоцзя синьсихуа фачжань чжаньлюэ [Государственная стратегия по развитию информатизации. 2006—2020] // 新华网 Синьхуаван [информационное агентство «Синьхуа»]. URL: http://news.xinhuanet.com/politics/2006‑05/09/content\_4524651.htm (дата обращения: 09.03.2018).

Литература:

Барри Ч. Чарльз Барри о подходах США и НАТО в области международной информационной безопасности. Взгляд на национальные и международные проблемы кибербезопасности. / Ч. Барри // Digital Report. 01.05.2015. URL: https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/ (дата обращения: 07.04.2018).

Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание / М. М.Безкоровайный, С. А. Лосев, А. Л. Татузов // Информатизация и связь. – 2011. – №. 6. – С.27-32.

Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности – 2014. №1(2). - С.24.

В США могут создать единую государственную 5G сеть для защиты от Китая // Information Security. Информационная безопасность. 29.01.2018. URL: http://www.itsec.ru/newstext.php?news\_id=121015 (дата обращения: 31.03.2018).

Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности / Г. Ибрагимова // Индекс безопасности. 2013. № 1 (104). С. 169 — 184.

1. Информационное общество и международные отношения: учебник / Р. В. Болгов, Н. А. Васильева, С. М. Виноградова, К. А. Панцерев; под ред. К. А. Панцерева; С7-Петерб. гос. ун-т. – СПб.: Изд-во СПбГУ, 2014. – 384 с.
2. Кибербезопасность // Securitylab.ru. URL: https://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC/ (дата обращения: 22.12.2017).

Кибервойна. // SecurityLab.ru. URL: https://www.securitylab.ru/news/tags/%ea%e8%e1%e5%f0%e2%ee%e9%ed%e0/ (дата обращения: 25.12.2017).

Китай пройдет три этапа на пути к кибердержаве // Russian.news.ch Синьхуа Новости. URL: http://russian.news.cn/2016-07/27/c\_135544806.htm (дата обращения: 13.03.2018).

Китай, Россия, Таджикистан и Узбекистан предлагают принять Правила обеспечения международной информационной безопасности // Новости ООН. 18.10.2012. URL: https://news.un.org/ru/story/2012/10/1211561 (дата обращения: 22.03.2018).

Мухин А. Новая стратегия национальной безопасности США – информационная бомба? / А. Мухин // Международный дискуссионный клуб Валдай. 26.12.2017. URL: http://ru.valdaiclub.com/a/highlights/strategiya-natsbezopasnosti-ssha/ (дата обращения: 01.03.2018).

Мы за интернационализацию управления интернетом. Спецпредставитель президента РФ о подходе Москвы к международной информационной безопасности. // Коммерсант.ru. 16.06.2014. URL: http://www.kommersant.ru/doc/2492206 (дата обращения: 04.04.2018).

Разумов Е. А. Политика КНР по обеспечению кибербезопасности. / Е. А. Разумов // Россия и АТР – 2017 №4. – С. 161.

Старкин С. В. Анализ разведывательной информации по транснациональному терроризму в современных внешнеполитических условиях: подходы американских теоретиков / С. В. Старкин // Гуманитарные исследования. 2011. № 1 (37). С. 6-11.

1. Старкин С. В. Проблемы типологизации разведывательной информации в американском теоретическом дискурсе / С. В. Старкин //Вестник Нижегородского университета им. Н. И. Лобачевского. - 2011. № 1. - С. 329-335.

Сыч О. Колонка Олега Сыча: как устроены национальные системы киберзащиты США, Китая и России / О. Сыч // Ain. 11.03.2015. URL: http://ain.ua/2015/03/11/569063 (дата обращения: 08.02.2018).

Цаканян В.Т. Роль кибербезопасности в мировой политике / В.Т. Цаканян // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2017. Т. 17. No 2. С. 339—348.

Юферев С. НОАК держит в тайне информацию о Силах стратегической поддержки / С. Юферев // Военное обозрение 25.12.2017. URL: https://topwar.ru/132683-narodno-osvoboditelnaya-armiya-kitaya-derzhit-v-tayne-informaciyu-o-silah-strategicheskoy-podderzhki.html (дата обращения: 13.02.2018).

Bulik Mark. 1988: ‘The Internet’ Comes Down With a Virus. / Mark Bulik // The New York Times. 06.08.2014. URL: https://www.nytimes.com/times-insider/2014/08/06/1988-the-internet-comes-down-with-a-virus/ (дата обращения: 21.12.2017).

Cadell Cate. Chinese state media says U.S. should take some blame for cyber attack. / Cate Cadell // Reuters. 17.05.2017. URL: https://www.reuters.com/article/us-cyber-attack-china/chinese-state-media-says-u-s-should-take-some-blame-for-cyber-attack-idUSKCN18D0G5 (дата обращения: 29.03.2018).

Chang A. Warring State. China’s Cybersecurity Strategy. / A. Chang // CRYPTOME. ORG December, 2014. URL: https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file‑14‑1205.pdf (дата обращения: 10.02.2018).

Chen Te-Ping. Snowden Alleges U.S. Hacking in China / Te-Ping Chen // The Wall Street Journal. 23.06.2013. URL: https://www.wsj.com/articles/SB10001424127887324577904578562483284884530 (дата обращения: 27.03.2018).

Chin Josh. Inside the Slow Workings of the U.S.-China Cybersecurity Agreement. / Josh Chin // The Wall Street Journal. 15.06.2016. URL: https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/ (дата обращения: 11.04.2018).

China faces talent gap in cybersecurity, says official // The Star Online. 14.12.2017. URL: https://www.thestar.com.my/news/regional/2017/12/14/china-faces-talent-gap-in-cybersecurity-says-official/ (дата обращения: 13.02.2018).

China's military to drill on digitalized forces // Xinhuanet. 29 May 2013. URL: http://news.xinhuanet.com/english/china/2013–05/29/c\_132415053.htm (дата обращения: 27.03.2018).

Chinese government to strengthen international cooperation on cyber issues: official // Xinhua, English.news.cn. 04.10.2012. URL: http://news.xinhuanet.com/english/china/2012–10/04/c\_131888329.htm. (дата обращения: 13.03.2018).

Dadich Scott. The President in Conversation With MIT’s Joi and WIRED’s Scott Dadich. Barack Obama, neural nets, self-driving cars, and the future of the world. / Scott Dadich. // WIRED November 2016. URL: https://www.wired.com/2016/10/president-obama-mit-joi-ito-interview/ (дата обращения: 31.01.2018).

Dilanian Ken. Russia May Be Hacking Us More, But China Is Hacking Us Much Less. / Ken Dilanian. // NBC News. 12.10.2016. URL: https://www.nbcnews.com/news/us-news/russia-may-be-hacking-us-more-china-hacking-us-much-n664836 (дата обращения: 11.04.2018).

Gan Nectar. China ‘willing to work with Trump on cybersecurity’ / Nectar Gan. // South China Morning Post. Diplomacy&Defence. 08.12.2016. URL: http://www.scmp.com/news/china/diplomacy-defence/article/2052881/china-willing-work-trump-cybersecurity (дата обращения: 15.04.2018).

Gerstein Daniel M. Define Acceptable Cyberspace Behavior. The U.S.-China cybersecurity agreement is a welcome step, but also highlights bigger problems. / Daniel M. Gerstein // U.S. News. 26.09.2015. URL: http://www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights -bigger-issues (дата обращения: 07.04.2018).

Gertz Bill. PLA’s new Strategic Support Force remains an enigma. / Bill Gertz // Asia Times. 18.12.2017. URL: http://www.atimes.com/plas-new-strategic-support-force-remains-enigma/ (дата обращения: 10.02.2018).

Goodman Peter S. Huawei Founder Ren Zhengfei Dismisses Chinese Military Connections. / Goodman Peter S. // International Business Times. 01.22.2015. URL: http://www.ibtimes.com/huawei-founder-ren-zhengfei-dismisses-chinese-military-connections-1791228 (дата обращения: 28.03.2018).

Hirschfeld Davis Julie, Sanger David E. Obama and Xi Jinping of China Agree to Steps on Cybertheft. / Davis Julie Hirschfeld, David E. Sanger. // NYTimes, 26.09.2015. URL:http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html (дата обращения: 22.03.2018).

Huileng Tan. China to USA: 'Stop deliberately distorting' our global strategy / Tan Huileng // CNBC. 20.12.2017. URL: https://www.cnbc.com/2017/12/20/china-us-beijing-reacts-to-trumps-america-first-policy.html (дата обращения: 01.03.2018).

Jones Terril Yue. U.S., China agree to work together on cyber security. / Terril Yue Jones // Reuters. 23.04.2013. URL: https://www.reuters.com/article/us-china-us-cyber/u-s-china-agree-to-work-together-on-cyber-security-idUSBRE93C05T20130413 (дата обращения: 07.04.2018).

Lemire Jonathan. Trump's Cybersecurity Review Misses Deadline / Jonathan Lemire. // U.S. News. 20.04.2017. URL: https://www.usnews.com/news/politics/articles/2017-04-20/trumps-cybersecurity-review-misses-deadline (дата обращения: 15.04.2018).

Lew Tells China Cyber Attacks ‘Very Serious Threat To Our Economic Interests’ // CBS DC. 20.03.2013. URL: http://washington.cbslocal.com/2013/03/20/us-treasury-secretary-tells-china-cyber-attacks-a-very-serious-threat-to-our-economic-interests/ (дата обращения: 07.04.2018).

Li Xiaokun, Zhang Yunbi. Core interests at heart of new US ties / Xiaokun Li, Yunbi Zhang // China Daily. 20.03.2013. URL: http://www.chinadaily.com.cn/china/2013–03/20/content\_16321491.htm (дата обращения: 07.04.2018).

Lieberthal K. G., Singer P. W. Cybersecurity and U.S. – China Relations / K. G. Lieberthal, P. W. Singer // Brookings. 23.02.2012. URL: http://www.brookings.edu/research/papers/2012/02/23-cybersecurity-china-us-singer-lieberthal (дата обращения: 31.03.2018).

Lindsay Jon R. The Impact of China on Cybersecurity / Jon R. Lindsay // International Security. 2015. Vol. 39. № 3. P. 7 — 47.

MacGregor A. China, U.S. making moves to implement cybersecurity agreements / A. MacGregor // The Stack.14.06.2016. URL: https://thestack.com/security/2016/06/14/china-u-s-making-moves-toimplement-cybersecurity-agreements/ (дата обращения: 15.04.2018).

MacWhorter Dan. Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators. / Dan MacWhorter // FireEye. 19.02.2013. URL: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (дата обращения: 08.02.2018).

Manjoo Farhad. Hacking the Old Gray Lady. The Chinese attack against the New York Times worked to perfection. / Farhad Manjoo. // Slate. 31.01.2013. URL: http://www.slate.com/articles/technology/technology/2013/01/new\_york\_times\_chinese\_hackers\_the\_attack\_against\_the\_newspaper\_of\_record.html (дата обращения: 27.03.2018).

1. Marks Joseph. Trump Acknowledges Russian Hacking, Points to Poor Defenses. / Joseph Marks. // Nextgov. 11.01.2017. URL: http://www.nextgov.com/cybersecurity/2017/01/trump-acknowledges-russian-hacking-poor-cyber-defenses/134510/ (дата обращения: 31.01.2018).

McWhorter Dan. Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators / Dan McWhorter // FireEye. 19.02.2013. URL: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (дата обращения: 08.02.2018).

Mehta Aaron. A digital migraine? How the Americas can step up cybersecurity strategies / Aaron Mehta // Federal Times. 28.22.2017. URL: https://www.federaltimes.com/smr/cybercon/2017/11/29/a-digital-migraine-how-the-americas-can-step-up-cybersecurity-strategies/ (дата обращения: 31.03.2018).

Messmer Ellen. Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says / Ellen Messmer // CNN. 12.05.1999. URL: http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/ (дата обращения: 20.03.2018).

Miles Tom. U.S. asks China not to enforce cyber security law / Tom Miles // Reuters. 26.09.2017. URL: https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1 (дата обращения: 29.03.2018).

Norton-Taylor Richard. Titan Rain - how Chinese hackers targeted Whitehall / Richard Norton-Taylor // The Guardian. 05.09.2007. URL: https://www.theguardian.com/technology/2007/sep/04/news.internet (дата обращения: 20.03.2018).

O'Brien Robert D., Shiran Shen. The U.S., China, and Cybersecurity: The Ethical Underpinnings of a Controversial Geopolitical Issue / Robert D. O'Brien, Shen Shiran. / Сarnegie Council for Ethics in International Affairs. 24.05.2013. URL: https://www.carnegiecouncil.org/publications/articles\_papers\_reports/0156 (дата обращения: 22.03.2018).

Panda Ankit. Xi Jinping: China Should Become a 'Cyber Power'. Xi Jinping has great ambitions for China in cyberspace. / Ankit Panda // The Diplomat 04.03.2014. URL: https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/ (дата обращения: 13.03.2018).

Pei, Minxin. How China and America See Each Other. And Why They Are on a Collision Course / Minxin Pei // Foreign Affairs. — 2014. — Vol. 93, N 2.

Petukhov A. Y., Komarov I. D., Starkin S. S., Markova A. V. Transition of Rivalry between USA and China to New Internet-Space / A. Y. Petukhov, I. D. Komarov, S. S. Starkin, A. V. Markova // Advances in Environmental Biology. 2014. № 8 (13). Р. 290-293.

Sandle Paul. Cyber crime costs global economy $445 billion a year: report / Paul Sandle // Reuters. 09.06.2014. URL: https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609 (дата обращения: 13.03.2018).

Segal Adam. From Net Politics and Digital and Cyberspace Policy Program: China’s New Cybersecurity Law / Adam Segal // Council on Foreign Relations 08.07.2015. URL: https://www.cfr.org/blog/chinas-new-cybersecurity-law (дата обращения: 13.03.2018).

Sheldon R., McReynolds J. Civil-Military Integration and Cybersecurity. In China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron,. New York: Oxford University Press, 2015. 398 P.

1. Shen Yi, “Responding to the Challenge of the ‘Offensive Internet Freedom Strategy’: Analyzing Sino-US Competition and Cooperation in Global Cyberspase,” [“Yingdui jingongxing hulianwang ziyou zhanlue de tiaozhan: Xi Zhong-Mei zai quanqiu xinxi kongjian de jingzheng yu hezuo”], Worls Economics and Politics [Shijie jingji yu zhengzhi], No. 2, 2012, pp.69-79.

Shu Catherine. China Tried To Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration / Catherine Shu. // TechCrunch 21.11.2014. URL: https://techcrunch.com/2014/11/20/worldinternetconference-declaration/ (дата обращения: 22.03.2018).

Sulmeyer Michael. Cybersecurity in the 2017 National Security Strategy / Michael Sulmeyer. // Lawfare. 19.12.2017. URL: https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy (дата обращения: 01.03.2018).

Swaine Michael D. Chinese Views on Cybersecurity in Foreign Relations / Michael D. Swaine // Cornegie Endowment for International Peace. China Leadership Minitor, no.42. URL: http://carnegieendowment.org/email/South\_Asia/img/CLM42MSnew.pdf (дата обращения: 28.03.2018).

Sweet William. The Blackout of 2003 / William Sweet // IEEE Spectrum. 01.08.2003. URL: https://spectrum.ieee.org/energy/the-smarter-grid/the-blackout-of-2003 (дата обращения: 20.03.2018).

Syeed N. U. S. Cyber Deal With China Is Reducing Hacking / N. Syeed // Bloomberg. 28.06.2016. URL: https://www.bloomberg.com/news/articles/2016–06–28/u-s-cyber-deal-with-china-isreducing- hacking-official-says (дата обращения: 15.04.2018).

1. Tang Rose. China-U.S. cyber war escalates / Rose Tang // CNN. 01.05.2001. URL: http://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/ (дата обращения: 20.03.2018).

The Obama-Xi Cyber Mirage. A digital arms deal that is full of promises but no enforcement. // The Wall Street Journal. 27.09.2015. URL: https://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248 (дата обращения: 11.04.2018).

Tiezzi Shannon. Xi Jinping Leads Internet Security Group / Shannon Tiezzi // The Diplomat 27.02.2014. URL: https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/ (дата обращения: 10.02.2018).

1. Ting Shi, Riley M. China Halts Cybersecurity Cooperation after U.S. Spying Charges. / Ting Shi, M. Riley // Bloomberg Technology 20.05.2014/ URL: http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html (дата обращения: 28.02.2018).

Ventre D. Chinese Cybersecurity and Defense. / D. Ventre // London: Wiley - ISTE, 2014. 301 p.

1. Vranicar D. China to Conduct Digital War Games / D. Vranicar // Xinhuanet. 29 May 2013. URL: http:// www.technewsworld.com/story/78151.html (дата обращения: 27.03.2018).

Wagner Jack. China's Cybersecurity Law: What You Need to Know: The law, which comes into effect June 1, raises data protection concerns for foreign firms. / Jack Wagner // The Diplomat. 01.06.2017. URL: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ (дата обращения: 13.03.2018).

Walcott John. U.S. Is Drafting Potential Sanctions Over China Cyber Hacking. / John Walcott // Bloomberg. 31.08.2015. URL: http://www.bloomberg.com/news/articles/2015-08-31/u-s-said-to-draft-potential-sanctions-over-china-cyber-hacking (дата обращения: 09.03.2018).

Weiss Brennan. NATO made one of its biggest policy shifts in decades to send a message to Russia / Brennan Weiss // Business Insider. 13.12.2017. URL: http://www.businessinsider.com/nato-targeting-countries-russia-china-north-korea-with-cyberweapons-2017-12?nr\_email\_referer=1&utm\_source=Sailthru&utm\_medium=email&utm\_content=MilitarySelect&pt=385758&ct=Sailthru\_BI\_Newsletters&mt=8&utm\_campaign=BI%20Military%20%26%20Defense%202017-12-13&utm\_term=Military%20Select%20-%20Engaged%2C%20Active%2C%20Passive%2C%20Disengaged (дата обращения: 01.03.2018).

Wilhelm Alex. China and the United States agree to create a joint cybersecurity working group / Alex Wilhelm // The Next Web. 13.04.2013. URL: http://thenextweb.com/insider/2013/04/13/china-and-the-united-states-will-create-a-joint-working-group-to-deal-with-cybersecurity/ (дата обращения: 07.04.2018).

Yan Sophia. China's new cybersecurity law takes effect today, and many are confused / Sophia Yan // CNBC. 31.05.2017. URL: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html (дата обращения: 13.03.2018).

Yoon Eunice. Chinese President Xi’s business forum speech: The take from Beijing / Eunice Yoon. // СNBC. 10.04.2018. URL: https://www.cnbc.com/2018/04/10/chinese-president-business-forum-speech.html (дата обращения: 14.04.2018).

勿忘2001中美黑客大战 Уван 2001 Чжунмэй хэйкэ дачжань [Не забыть об американо-китайской хакерской войне 2001 года] // 铁血网 Тесюэван [tiexue.net] 6.12.2009. URL: http://bbs.tiexue.net/post2\_3975999\_1.html (дата обращения: 20.03.2018).

方滨兴，杜阿宁， \_张熙，王忠儒. Фан Биньсин, Чжун Си, Ван Яжунжу. 国家网络空间安全国际战略研究 Гоцзя ванло кунцзянь аньцюань гоцзи чжаньлюэ яньцзю [Исследование международной стратегии национальной безопасности в области киберпространства] // 中国工程科学 . Chinese academy of engineering journal. 2016. № 6. P. 13 — 16.

逸思Исы. 中美执法及网络安全对话 Чжунмэй чжифа цзи ванло аньцюань дуйхуа [Китайско-американское правоприменение и диалог по кибербезопасности]/逸思 Исы //網易新闻 Ванъи синьвэнь. URL: http://news.163.com/17/1005/12/D000JU35000187VE.html (дата обращения: 18.04.2018).

郝叶力Хао Ели. 网络空间规则之争要找准痛点 Ванло кунцзян гуйцзэ чжичжэнъ яо чжао чжуньтун дянь [Поиск уязвимостей в киберпространстве] /郝叶力 Хао Ели //網易新闻 Ванъи синьвэнь 12.12.2015. URL: http://news.163.com/15/1212/10/BAKJQVU600014JB6.html (дата обращения: 10.02.2018).

麦燕庭 Май Яньтин. 传习近平创建信息领导小组评论忧走集权回头路 Чуань Си Цзиньпин чуанцзянь синьси линдао сяоцзу пинлунь ю цзоу цзицюань хуэйтоулу [Си Цзиньпин учреждает руководящую группу по государственной информатизации]／麦燕庭 Май Яньтин // 世界之声 Шицзе чжишэн. URL: http://cn.rfi.fr/中国/20140108-传习近平创建信息领导小组评论忧走集权回头路 (дата обращения: 08.02.2018).

1. 中央网络安全和信息化领导小组第一次会议召开 习近平发表重要讲话Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу диицы хуэйи чжаокай Сицзиньпин фабяо чжунъяо цзянхуа [Первое совещание Центральной группы по информационной безопасности и информатизации. Важная речь Си Цзиньпина] // 中华人民共和国国家互联网信息办公室Чжунхуа жэньминь гунхэго гоцзя хуляньван синьси баньгунши [Национальное интернет-информационное бюро КНР] 27.02.2014. URL: http://www.cac.gov.cn/2014-02/27/c\_133148354.htm (дата обращения: 13.03.2018) [↑](#footnote-ref-1)
2. Third U. S. – China High-Level Joint Dialogue on Cybercrime and Related Issues. Joint Summary of Outcomes // Homeland Security. 8.12.2016. URL: https://www.dhs.gov/news/2016/12/08/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues (дата обращения: 15.04.2018). [↑](#footnote-ref-2)
3. The DOD Cyber Strategy // U.S. Department of Defense. April 2015. URL: http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-3)
4. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / The White House. May 2011 // Office of the White House Press Secretary. URL: https://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_for\_cyberspace.pdf (дата обращения: 25.02.2018). [↑](#footnote-ref-4)
5. International Strategy of Cooperation on Cyberspace // 新华网Xinhua News. 01.03.2017. URL: http://www.xinhuanet.com/english/china/2017-03/01/c\_136094371.htm (дата обращения: 16.03.2018). [↑](#footnote-ref-5)
6. 中华人民共和国网络安全法 Чжунхуа жэньминь гунхэго ванло аньцюань фа [Закон о кибербезопасности КНР] // 全国人民代表大会 Цюаньго жэньминь дайбяо дахуэй [Всекитайское собрание народных представителей]. 7.11.2016. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content\_2001605.htm (дата обращения: 22.12.2017). [↑](#footnote-ref-6)
7. 胡锦涛在全国科学技术大会上的讲话(全文) Хуцзиньтао цзай цюань гокэсюэ цзишудахуэйшан дэ цзянхуа (Цюань вэнь) [Речь Ху Цзиньтао на Национальной научно-технической конференции (полная речь)] //中国共产党新闻Чжунго гунчаньдан синьвэнь [Новости КПК] 10.01.2006. URL: http://cpc.people.com.cn/GB/64093/64094/4455445.html (дата обращения: 09.03.2018). [↑](#footnote-ref-7)
8. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference // The White House. Office of the Press Secretary. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint (дата обращения: 07.04.2018). [↑](#footnote-ref-8)
9. Average annualized cost of cyber attacks on companies in selected countries as of August 2017 (in million U.S. dollars) // The Statistic Portal Statista. URL: https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ (дата обращения: 31.03.2018). [↑](#footnote-ref-9)
10. Digital Attack Map. Top daily DDoS attacks worldwide // Digital Attack Map. URL: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17650&view=map (дата обращения: 22.03.2018). [↑](#footnote-ref-10)
11. Бажанов Е. Движущие силы политики США в отношении Китая / Е. Бажанов // М.: Наука, Главная редакция восточной литературы, - 1982. – С. 240. [↑](#footnote-ref-11)
12. Труш С. «Новая модель отношений» КНР-США: поиск на экспертном уровне / С. Труш // США и Канада: экономика, политика, культура. – 2015. - №12 (552). С. 37-52. [↑](#footnote-ref-12)
13. Парканский, А. Б. Мифы и реалии американо-китайских экономических отношений / А. Б. Парканский // США — Канада: экономика, политика, культура. — 2015. — № 3. — С. 19—35. [↑](#footnote-ref-13)
14. Тимофеев О. А. Тема отношений США с КНР в президентской кампании 2012 года / О. А. Тимофеев // США — Канада: экономика, политика, культура. — 2013. — № 2. — С. 47—56. [↑](#footnote-ref-14)
15. Давыдов А. С. Китайско-американские отношения «нового типа» и фактор России в глобальном и региональном измерениях / А. С. Давыдов // Китай в мировой и региональной политике. История и современность. — 2014. — Т. 19, № 19. — С. 121—134. [↑](#footnote-ref-15)
16. Лексютина Я.В. США и Китай: линии соперничества и противоречий.— СПб.: СПбГУ, 2011. — 230 с. [↑](#footnote-ref-16)
17. Nye Joseph S. The Future of U.S.-China Relations / Joseph S. Nye // China US Focus. 10.03.2015. URL: https://www.chinausfocus.com/foreign-policy/the-future-of-us-china-relations (дата обращения: 19.04.2018). [↑](#footnote-ref-17)
18. China, the U.S. and the ‘Thucydides Trap:’ Q&A with Professor Harry Harding // The Wall Streer Journal. 03.03.2016. URL: https://blogs.wsj.com/chinarealtime/2016/03/03/china-the-u-s-and-the-thucydides-trap-qa-with-professor-harry-harding/ (дата обращения: 19.04.2018). [↑](#footnote-ref-18)
19. Lampton David M. A New Type of Major-Power Relationship: Seeking a Durable Foundation for U.S.-China Ties / David M. Lampton // Asia Policy №16, July 2013. pp. 51-68. [↑](#footnote-ref-19)
20. Sutter Robert G. US-China Relations: Perilous Past, Uncertain Present / Robert G. Sutter // Rowman & Littlefield, - 2017 – p. 336. [↑](#footnote-ref-20)
21. 譚瑾瑜Тан Цзиньюй. 大陸十三五規劃趨勢與台灣因應建言Далу шисаньу гуихуа цюши ю тайвань иньин цзяньянь [Тенденции тринадцатой пятилетки в Китае и ответ Тайваня на выдвинутые предложения]/ 譚瑾瑜Тан Цзиньюй // 財團法人.國家政策研究基金會 Цайтуан фажэнь. Гоцзя чжэнцэ яньцзю цзицзиньхуи [Консорциум. Фонд исследований национальной политики]. 02.12.2014. URL: https://www.npf.org.tw/3/14471 (дата обращения: 10.02.2018). [↑](#footnote-ref-21)
22. Pei Minxin. How China and America See Each Other. And Why They Are on a Collision Course / Minxin Pei // Foreign Affairs. — 2014. — Vol. 93, N 2. [↑](#footnote-ref-22)
23. Старкин С. В. Анализ разведывательной информации по транснациональному терроризму в современных внешнеполитических условиях: подходы американских теоретиков / С. В. Старкин // Гуманитарные исследования. 2011. № 1 (37). С. 6-11. [↑](#footnote-ref-23)
24. Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание / М. М. Безкоровайный, С. А. Лосев, А. Л. Татузов // Информатизация и связь. – 2011. – №. 6. – С. 27-32. [↑](#footnote-ref-24)
25. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности / Г. Ибрагимова // Индекс безопасности. 2013. № 1 (104). С. 169 — 184. [↑](#footnote-ref-25)
26. Разумов Е. А. Политика КНР по обеспечению кибербезопасности. / Е. А. Разумов // Россия и АТР – 2017 №4. – С. 161. [↑](#footnote-ref-26)
27. Информационное общество и международные отношения: учебник / Р. В. Болгов, Н. А. Васильева, С. М. Виноградова, К. А. Панцерев; под ред. К. А. Панцерева; С7-Петерб. гос. ун-т. – СПб.: Изд-во СПбГУ, 2014. – с. 311. [↑](#footnote-ref-27)
28. Болгов Р. В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Дисс.. канд. полит. наук. СПб.: СПбГУ, 2011. URL: http://www.avnrf.ru/attachments/article/504/диссер%20пот%20ИТ%202011.pdf (дата обращения: 19.04.2018). [↑](#footnote-ref-28)
29. Болгов Р. В. Информационные технологии в модернизации вооруженных сил КНР: политические аспекты / Р. В. Болгов // ПОЛИТЭКС. 2010. № 4. С. 269-276. [↑](#footnote-ref-29)
30. Steinberg Joseph. Issues With the China-US Cybersecurity Agreement / Joseph Steinberg. // Inc. 27.09.2015 /URL: http://www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.html (дата обращения: 19.04.2018). [↑](#footnote-ref-30)
31. Sheldon R., McReynolds J. Civil-Military Integration and Cybersecurity. In China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron,. New York: Oxford University Press, 2015. 398 P. [↑](#footnote-ref-31)
32. Segal Adam. Stabilizing cybersecurity in the U.S.-China relationship. / Adam Segal // The National Bureau of Asian Research. September 2015. URL: http://nbr.org/downloads/pdfs/psa/US-China\_brief\_Segal\_Sept2015.pdf (дата обращения: 07.04.2018). [↑](#footnote-ref-32)
33. Ventre D. Chinese Cybersecurity and Defense. London: Wiley‑ISTE, 2014. 301 p. [↑](#footnote-ref-33)
34. Hathaway Melissa, Demchak Chris, Kerben Jason, McArdle Jennifer, Spidalieri Francesca. Cyber Readiness Index 2.0. A Plan for Cyber Readiness: a Baseline and an Index / Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri // Potomac Institute for Policy Studies. 2015. URL: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-2.0-web-2016.pdf (дата обращения: 19.04.2018). [↑](#footnote-ref-34)
35. 郝叶力Хао Ели. 网络空间规则之争要找准痛点 Ванло кунцзян гуйцзэ чжичжэнъ яо чжао чжуньтун дянь [Поиск уязвимостей в киберпространстве] /郝叶力 Хао Ели //網易新闻 Ванъи синьвэнь 12.12.2015. URL: http://news.163.com/15/1212/10/BAKJQVU600014JB6.html (дата обращения: 10.02.2018). [↑](#footnote-ref-35)
36. Petukhov A. Y., Komarov I. D., Starkin S. S., Markova A. V. Transition of Rivalry between USA and China to New Internet-Space / A. Y. Petukhov, I. D. Komarov, S. S. Starkin, A. V. Markova // Advances in Environmental Biology. 2014. № 8 (13). Р. 290-293. [↑](#footnote-ref-36)
37. Юрченко Г. Возможности Китая по проведению компьютерных cетевых операций и кибершпионажу / Г. Юрченко // BELVPO. COM: информационный портал «Военно-политическое обозрение». URL: http://www.belvpo.com/9984.htm (дата обращения: 19.04.2018). [↑](#footnote-ref-37)
38. Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога / К. Антипов // Проблемы Дальнего Востока. 2013. № 6. С. 39 — 54. [↑](#footnote-ref-38)
39. Булавин А. О подходах США и Китая к обеспечению кибербезопасности / А. Булавин // Общество: политика, экономика и право. 2014. № 1. С. 27 — 31. [↑](#footnote-ref-39)
40. Swaine Michael D. Chinese Views on Cybersecurity in Foreign Relations / Michael D. Swaine // Cornegie Endowment for International Peace. China Leadership Minitor, no.42. URL: http://carnegieendowment.org/email/South\_Asia/img/CLM42MSnew.pdf (дата обращения: 08.02.2018). [↑](#footnote-ref-40)
41. Sulmeyer Michael. Cybersecurity in the 2017 National Security Strategy / Michael Sulmeyer // Lawfare. 19.12.2017. URL: https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy (дата обращения: 01.03.2018). [↑](#footnote-ref-41)
42. Shen Yi. New Challenges for China and the U.S. in a Networked World: Governing Global Cyberspace / Yi Shen // China US Focus. 28.06.2011. URL: https://www.chinausfocus.com/peace-security/new-challenges-for-china-and-the-u-s-in-a-networked-world-governing-global-cyberspace (дата обращения: 19.04.2018). [↑](#footnote-ref-42)
43. Chen Gang, Lim Wen Xin. Xi Jinping’s Economic Cybersecurity Agreement with Barack Obama / Chen Gang, Lim Wen Xin // International Public Policy Review. 28.03.2016. URL: http://ippreview.com/index.php/Home/Blog/single/id/35.html (дата обращения: 20.04.2018). [↑](#footnote-ref-43)
44. 方滨兴，杜阿宁， 张熙，王忠儒. Фан Биньсин, Чжун Си, Ван Яжунжу. 国家网络空间安全国际战略研究 Гоцзя ванло кунцзянь аньцюань гоцзи чжаньлюэ яньцзю [Исследование международной стратегии национальной безопасности в области киберпространства] // 中国工程科学 . Chinese academy of engineering journal. 2016. № 6. P. 13 — 16. [↑](#footnote-ref-44)
45. 王桂芳. Ван Гуйфан. 大国网络竞争与中国网络安全战略选择 Даго ванло цзинчжэнъ юй чжунго ванло аньцюань чжаньлюэ сюаньцзэ [Кибер-конкурен­ция между Великими державами и стратегический выбор кибербезопасности Китая] // 国际安全研究Гоцзя аньцюань яньцзю [исследования в области междунароной безопасности] 2017. № 2. P. 27 — 46. [↑](#footnote-ref-45)
46. Bulik Mark. 1988: ‘The Internet’ Comes Down With a Virus. / Mark Bulik // The New York Times. 06.08.2014. URL: https://www.nytimes.com/times-insider/2014/08/06/1988-the-internet-comes-down-with-a-virus/ (дата обращения: 21.12.2017). [↑](#footnote-ref-46)
47. Информационное общество и международные отношения: учебник / Р. В. Болгов, Н. А. Васильева, С. М. Виноградова, К. А. Панцерев; под ред. К. А. Панцерева; С7-Петерб. гос. ун-т. – СПб.: Изд-во СПбГУ, 2014. – с. 311. [↑](#footnote-ref-47)
48. Концепция стратегии кибербезопасности Российской Федерации // Сайт Совета Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 22.12.2017). [↑](#footnote-ref-48)
49. Кибербезопасность // Securitylab.ru. URL: https://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC/ (дата обращения: 22.12.2017). [↑](#footnote-ref-49)
50. 中华人民共和国网络安全法 Чжунхуа жэньминь гунхэго ванло аньцюань фа [Закон о кибербезопасности КНР] // 全国人民代表大会 Цюаньго жэньминь дайбяо дахуэй [Всекитайское собрание народных представителей]. 7.11.2016. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content\_2001605.htm (дата обращения: 22.12.2017). [↑](#footnote-ref-50)
51. White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace\_Policy\_Review\_final\_0.pdf (дата обращения: 22.12.2017). [↑](#footnote-ref-51)
52. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Вопросы кибербезопасности – 2014. №1(2). - С. 26. [↑](#footnote-ref-52)
53. Peter Warren Singer: "Cybersecurity and Cyberwar: What Everyone Needs to Know" | Talks at Google. // Youtube “Talks at Google” channel. 10.02.2014. URL: https://www.youtube.com/watch?v=h0SXO5KUZIo (дата обращения: 25.12.2017). [↑](#footnote-ref-53)
54. Кибервойна. // SecurityLab.ru. URL: https://www.securitylab.ru/news/tags/%ea%e8%e1%e5%f0%e2%ee%e9%ed%e0/ (дата обращения: 25.12.2017). [↑](#footnote-ref-54)
55. Cyberwar. // Oxford Living Dictionaries. URL: https://en.oxforddictionaries.com/definition/cyberwar (дата обращения: 25.12.2017). [↑](#footnote-ref-55)
56. Резолюция A/RES/57/239, принятая Генеральной Ассамблеей [по докладу Второго комитета (A/57/529/Add.3)]. 57/239. Создание глобальной культуры кибербезопасности. 20.12.2002 // Генеральная Ассамблея Организации Объединенных Наций. 31.01.2003. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата обращения: 27.12.2017). [↑](#footnote-ref-56)
57. International Telecommunication Union (ITU) // ITU. URL: https://www.itu.int/en/about/Pages/default.aspx (дата обращения: 16.01.2018). [↑](#footnote-ref-57)
58. Convention télégraphique internationale de Paris (1865) et

Règlement de service international (1865) // ITU. URL: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.1.61.fr.200.pdf (дата обращения: 16.01.2018). [↑](#footnote-ref-58)
59. Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности. Международный союз электросвязи. // Международный союз электросвязи 2008. URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения: 16.01.2018). [↑](#footnote-ref-59)
60. Report of the Chairman of HLEG To ITU Secretary-General, Dr. Hamadoun I. Touré by Chief Judge Stein Schjølberg, Judge at the Moss Tingrett Court, Norway // ITU Global Cybersecurity Agenda (GCA). High-Level Experts Group (HLEG). URL: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (дата обращения: 16.01.2018). [↑](#footnote-ref-60)
61. Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности. // Международный союз электросвязи 2008. URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения: 17.01.2018). [↑](#footnote-ref-61)
62. International Multilateral Partnership Against Cyber Threats. IMPACT. // IMPACT. URL: http://www.impact-alliance.org/home/index.html (дата обращения: 17.01.2018). [↑](#footnote-ref-62)
63. Global Cybersecurity Index (GCI) 2013. ITU 2013 // International Telecommunication Union 2013. URL: https://www.itu.int/md/T13-SG17-R-0004 (дата обращения: 17.01.2018). [↑](#footnote-ref-63)
64. Global Cybersecurity Index (GCI) 2017. ITU 2017 // International Telecommunication Union 2017. URL: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (дата обращения: 17.01.2018). [↑](#footnote-ref-64)
65. Schmitt Georg. To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity / Georg Schmitt // World Economic Forum. 24.01.2018. URL: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/ (дата обращения: 26.01.2018). [↑](#footnote-ref-65)
66. Global Cyber Security Center // URL: https://www.gcsec.org/about-gcsec (дата обращения: 26.01.2018). [↑](#footnote-ref-66)
67. Schmitt Georg. To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity / Georg Schmitt // World Economic Forum. 24.01.2018. URL: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/ (дата обращения: 26.01.2018). [↑](#footnote-ref-67)
68. An Act to establish the Department of Homeland Security, and for other purposes. Public Law 107–296. // 107th Congress. Homeland Security Act of 2002. // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/hr\_5005\_enr.pdf (дата обращения: 26.01.2018). [↑](#footnote-ref-68)
69. The National Strategy to Secure Cyber Space // The White House, Washington DC, USA, 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 26.01.2018). [↑](#footnote-ref-69)
70. Rollins J., Henning A. C. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. / J. Rollins, A. C. Henning // The White House, Washington DC, 2009. URL: https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf (дата обращения: 31.01.2018). [↑](#footnote-ref-70)
71. The Comprehensive National Cybersecurity Initiative // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 31.01.2018). [↑](#footnote-ref-71)
72. Global Cybersecurity Index (GCI) 2017. ITU 2017 // International Telecommunication Union 2017. URL: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (дата обращения: 17.01.2018). [↑](#footnote-ref-72)
73. Resource Center for State Cybersecurity // National Governors Association. URL: https://www.nga.org/cms/center/issues/hsps/state-cybersecurity (дата обращения: 31.01.2018). [↑](#footnote-ref-73)
74. Старкин С. В. Анализ разведывательной информации по транснациональному терроризму в современных внешнеполитических условиях: подходы американских теоретиков / С. В. Старкин // Гуманитарные исследования. 2011. № 1 (37). С. 6-11. [↑](#footnote-ref-74)
75. Pellerin Cheryl. U.S. Cyber Command Chief Testifies on Challenges, Security Initiatives. / Cheryl Pellerin. // U.S. Department of Defence. 5.04.2016. URL: https://www.defense.gov/News/Article/Article/713755/us-cyber-command-chief-testifies-on-challenges-security-initiatives/ (дата обращения: 31.01.2018). [↑](#footnote-ref-75)
76. Marks Joseph. Trump Acknowledges Russian Hacking, Points to Poor Defenses. / Joseph Marks. // Nextgov. 11.01.2017. URL: http://www.nextgov.com/cybersecurity/2017/01/trump-acknowledges-russian-hacking-poor-cyber-defenses/134510/ (дата обращения: 31.01.2018). [↑](#footnote-ref-76)
77. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order. // The White House. 11.05.2017. URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (дата обращения: 31.01.2018). [↑](#footnote-ref-77)
78. Press Briefing by Principal Deputy Press Secretary Sarah Sanders and Homeland Security Advisor Tom Bossert // The White House. 11.05.2017. URL: https://www.whitehouse.gov/briefings-statements/press-briefing-principal-deputy-press-secretary-sarah-sanders-homeland-security-advisor-tom-bossert-051117/ (дата обращения: 31.01.2018). [↑](#footnote-ref-78)
79. Mr. Mccaul (for himself, Mr. Thonpson, Mr. Ratcliffe, Mr. Richmond, Mr. Katko, Mr. Hurd, Mr. Donovan, Mr. Gallagher, Mr. Higgins, Mr. Garett, and Mr. Fitzpatrick.) H. R. 3359. Cybersecurity and Infrastructure Security Agency Act of 2017 / Mr. Mccaul (for himself, Mr. Thonpson of Mississippi, Mr. Ratcliffe, Mr. Richmond, Mr. Katko, Mr. Hurd, Mr. Donovan, Mr. Gallagher, Mr. Higgins of Louisiana, Mr. Garett, and Mr. Fitzpatrick.) // U.S. House of Representatives. Document Repository. 24.07.2017. URL: http://docs.house.gov/billsthisweek/20171211/HR3359.pdf (дата обращения: 31.01.2018). [↑](#footnote-ref-79)
80. Сadell Cate. China's Xi says country will not close door to global internet / Cate Сadell. // Reauters. 03.12.2017. URL: https://www.reuters.com/article/us-china-cyber/chinas-xi-says-country-will-not-close-door-to-global-internet-idUSKBN1DX01S (дата обращения: 08.02.2018). [↑](#footnote-ref-80)
81. Yoon Eunice. Chinese President Xi’s business forum speech: The take from Beijing / Eunice Yoon. // СNBC. 10.04.2018. URL: https://www.cnbc.com/2018/04/10/chinese-president-business-forum-speech.html (дата обращения: 14.04.2018). [↑](#footnote-ref-81)
82. 习近平：让互联网更好造福国家和人民Си Цзиньпин：жан хуляньван гэнхао цзаофу гоцзя хэ жэньминь [Си Цзиньпин: улучшить интернет для страны и для народа] // 新华社Синьхуа шэ［Агентство Синьхуа］19.04.2016. URL: http://www.xinhuanet.com/politics/2016-04/19/c\_1118672059.htm (дата обращения: 08.02.2018). [↑](#footnote-ref-82)
83. 麦燕庭 Май Яньтин. 传习近平创建信息领导小组评论忧走集权回头路 Чуань Си Цзиньпин чуанцзянь синьси линдао сяоцзу пинлунь ю цзоу цзицюань хуэйтоулу [Си Цзиньпин учреждает руководящую группу по государственной информатизации]／麦燕庭 Май Яньтин // 世界之声 Шицзе чжишэн. URL: http://cn.rfi.fr/中国/20140108-传习近平创建信息领导小组评论忧走集权回头路 (дата обращения: 08.02.2018). [↑](#footnote-ref-83)
84. Swaine Michael D. Chinese Views on Cybersecurity in Foreign Relations / Michael D. Swaine // Cornegie Endowment for International Peace. China Leadership Minitor, no.42. URL: http://carnegieendowment.org/email/South\_Asia/img/CLM42MSnew.pdf (дата обращения: 08.02.2018). [↑](#footnote-ref-84)
85. Sheldon R., McReynolds J. Civil-Military Integration and Cybersecurity. In China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron,. New York: Oxford University Press, 2015. P. 191. [↑](#footnote-ref-85)
86. Lindsay Jon R. The Impact of China on Cybersecurity / Jon R. Lindsay // International Security. 2015. Vol. 39. № 3. P. 7 — 47. [↑](#footnote-ref-86)
87. McWhorter Dan. Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators / Dan McWhorter. // FireEye. 19.02.2013. URL: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (дата обращения: 08.02.2018). [↑](#footnote-ref-87)
88. Сыч О. Колонка Олега Сыча: как устроены национальные системы киберзащиты США, Китая и России / О. Сыч // Ain. 11.03.2015. URL: http://ain.ua/2015/03/11/569063 (дата обращения: 08.02.2018). [↑](#footnote-ref-88)
89. Разумов Е. А. Политика КНР по обеспечению кибербезопасности. / Е. А. Разумов // Россия и АТР – 2017 №4. – С. 161. [↑](#footnote-ref-89)
90. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности / Г. Ибрагимова // Индекс безопасности. 2013. № 1 (104). С. 169 — 184. [↑](#footnote-ref-90)
91. Gertz Bill. PLA’s new Strategic Support Force remains an enigma. / Bill Gertz // Asia Times. 18.12.2017. URL: http://www.atimes.com/plas-new-strategic-support-force-remains-enigma/ (дата обращения: 10.02.2018). [↑](#footnote-ref-91)
92. 譚瑾瑜Тан Цзиньюй. 大陸十三五規劃趨勢與台灣因應建言Далу шисаньу гуихуа цюши ю тайвань иньин цзяньянь [Тенденции тринадцатой пятилетки в Китае и ответ Тайваня на выдвинутые предложения]/ 譚瑾瑜Тан Цзиньюй //財團法人.國家政策研究基金會 Цайтуан фажэнь. Гоцзя чжэнцэ яньцзю цзицзиньхуи [Консорциум. Фонд исследований национальной политики]. 02.12.2014. URL: https://www.npf.org.tw/3/14471 (дата обращения: 10.02.2018). [↑](#footnote-ref-92)
93. Chang A. Warring State. China’s Cybersecurity Strategy. / A. Chang // CRYPTOME.ORG December, 2014. URL: https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file‑14‑1205.pdf (дата обращения: 10.02.2018). [↑](#footnote-ref-93)
94. Tiezzi Shannon. Xi Jinping Leads Internet Security Group / Shannon Tiezzi // The Diplomat 27.02.2014. URL: https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/ (дата обращения: 10.02.2018). [↑](#footnote-ref-94)
95. 中央网络安全和信息化领导小组成立:从网络大国迈向网络强国Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу чэнли: цун ванло даго май сян ванло цянго [Ведущая центральная группа по вопросам сетевой информации и информатизации: от крупного информационного государства к крупной интернет-державе] // 新华社27.02.2014. Синьхуа шэ 27.02.2014.［Агентство Синьхуа 27.02.2014.]. URL: http://news.xinhuanet.com/politics/2014 02/27/c\_119538719.htm (дата обращения: 10.02.2018). [↑](#footnote-ref-95)
96. 郝叶力博士Хао Ели боши [Доктор Хао Ели]// 数据治理和网络安全研究联盟06.01.2018 Шуцзюй чжили хэ ванло аньцюань яньцзю ляньмэн 06.01.2018 [Исследовательский центр по дата-данным и кибербезопасности 06.01.2018]. URL: http://www.dgcs-research.net/a/lianmengchengyuan/lianmengzhuyaochengyuan/2018/0103/68.html (дата обращения: 10.02.2018). [↑](#footnote-ref-96)
97. 郝叶力Хао Ели. 网络空间规则之争要找准痛点 Ванло кунцзян гуйцзэ чжичжэнъ яо чжао чжуньтун дянь [Поиск уязвимостей в киберпространстве] /郝叶力 Хао Ели //網易新闻 Ванъи синьвэнь 12.12.2015. URL: http://news.163.com/15/1212/10/BAKJQVU600014JB6.html (дата обращения: 10.02.2018). [↑](#footnote-ref-97)
98. Юферев С. НОАК держит в тайне информацию о Силах стратегической поддержки / С. Юферев // Военное обозрение 25.12.2017. URL: https://topwar.ru/132683-narodno-osvoboditelnaya-armiya-kitaya-derzhit-v-tayne-informaciyu-o-silah-strategicheskoy-podderzhki.html (дата обращения: 13.02.2018). [↑](#footnote-ref-98)
99. Petukhov A. Y., Komarov I. D., Starkin S. S., Markova A. V. Transition of Rivalry between USA and China to New Internet-Space / A. Y. Petukhov, I. D. Komarov, S. S. Starkin, A. V. Markova // Advances in Environmental Biology. 2014. № 8 (13). Р. 290-293. [↑](#footnote-ref-99)
100. China faces talent gap in cybersecurity, says official // The Star Online. 14.12.2017. URL: https://www.thestar.com.my/news/regional/2017/12/14/china-faces-talent-gap-in-cybersecurity-says-official/ (дата обращения: 13.02.2018). [↑](#footnote-ref-100)
101. 军地联手搭建融合创新平台应对网络空间安全威胁 Цзюньди ляньшоу дацзянь жунхэ чуансинь пинтай индуй ванло кунцзянь аньцюань вэйсе [В Пекине создан Инновационный центр военно-гражданского слияния в области кибербезопасности]// 新华网Синьхуаван. 26.12.2017. URL: http://www.xinhuanet.com/2017-12/26/c\_1122170496.htm (дата обращения: 13.02.2018). [↑](#footnote-ref-101)
102. Clinton William. National Security Strategy / Washington DC: Government Printing Office. February 1995. P. 8. [↑](#footnote-ref-102)
103. Presidential Decision Directive / NSC-63 / The White House, Washington // The White House. 22.05.1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (дата обращения: 25.02.2018). [↑](#footnote-ref-103)
104. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 25.02.2018). [↑](#footnote-ref-104)
105. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 17.12.2003. URL: https://www.dhs.gov/homeland-security-presidential-directive-7 (дата обращения: 25.02.2018). [↑](#footnote-ref-105)
106. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 25.02.2018). [↑](#footnote-ref-106)
107. The Comprehensive National Cybersecurity Initiative 2009 // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 25.02.2018). [↑](#footnote-ref-107)
108. White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace\_Policy\_Review\_final\_0.pdf (дата обращения: 25.02.2018). [↑](#footnote-ref-108)
109. The Comprehensive National Cybersecurity Initiative 2009 // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 25.02.2018). [↑](#footnote-ref-109)
110. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / The White House. May 2011 // Office of the White House Press Secretary. URL: https://www.whitehouse.gov/sites/default/files/rss\_viewer/international\_strategy\_for\_cyberspace.pdf (дата обращения: 25.02.2018). [↑](#footnote-ref-110)
111. Department of Defense Strategy for Operating in Cyberspace. / U.S. Department of Defense, 2011. // U.S. Department of Defense. URL: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-111)
112. Department of Defense Strategy for Operating in Cyberspace. / U.S. Department of Defense, 2011. // U.S. Department of Defense. URL: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-112)
113. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. / General Assembly of the United Nations. 24.06.2013 / General Assembly of the United Nations .URL: http://www.un.org/ga/search/view\_doc.asp?symbol=A/68/98 (дата обращения: 28.02.2018). [↑](#footnote-ref-113)
114. Ting Shi, Riley M. China Halts Cybersecurity Cooperation after U.S. Spying Charges. / Ting Shi, M. Riley // Bloomberg Technology 20.05.2014. URL: http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html (дата обращения: 28.02.2018). [↑](#footnote-ref-114)
115. Старкин С. В. Проблемы типологизации разведывательной информации в американском теоретическом дискурсе / С. В. Старкин // Вестник Нижегородского университета им. Н. И. Лобачевского. - 2011. № 1. - С. 331. [↑](#footnote-ref-115)
116. National Strategy for Information Sharing and Safeguarding / The White House // The White House, 2012. URL: https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy\_1.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-116)
117. The DOD Cyber Strategy / U.S. Department of Defense. April 2015. // U.S. Department of Defense. URL: http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-117)
118. The DOD Cyber Strategy // U.S. Department of Defense. April 2015. URL: http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf (дата обращения: 28.02.2018). [↑](#footnote-ref-118)
119. Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California. News trancript // U.S. Department of Defence. 23.04.2015. URL: https://www.defense.gov/News/Transcripts/Transcript-View/Article/607043/remarks-by-secretary-carter-at-the-drell-lecture-cemex-auditorium-stanford-grad/ (дата обращения: 28.02.2018). [↑](#footnote-ref-119)
120. National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 01.03.2018). [↑](#footnote-ref-120)
121. Huileng Tan. China to USA: 'Stop deliberately distorting' our global strategy / Tan Huileng // CNBC. 20.12.2017. URL: https://www.cnbc.com/2017/12/20/china-us-beijing-reacts-to-trumps-america-first-policy.html (дата обращения: 01.03.2018). [↑](#footnote-ref-121)
122. Weiss Brennan. NATO made one of its biggest policy shifts in decades to send a message to Russia / Brennan Weiss // Business Insider. 13.12.2017. URL: http://www.businessinsider.com/nato-targeting-countries-russia-china-north-korea-with-cyberweapons-2017-12?nr\_email\_referer=1&utm\_source=Sailthru&utm\_medium=email&utm\_content=MilitarySelect&pt=385758&ct=Sailthru\_BI\_Newsletters&mt=8&utm\_campaign=BI%20Military%20%26%20Defense%202017-12-13&utm\_term=Military%20Select%20-%20Engaged%2C%20Active%2C%20Passive%2C%20Disengaged (дата обращения: 01.03.2018). [↑](#footnote-ref-122)
123. Мухин А. Новая стратегия национальной безопасности США – информационная бомба? / А. Мухин // Международный дискуссионный клуб Валдай. 26.12.2017. URL: http://ru.valdaiclub.com/a/highlights/strategiya-natsbezopasnosti-ssha/ (дата обращения: 01.03.2018). [↑](#footnote-ref-123)
124. National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 01.03.2018). [↑](#footnote-ref-124)
125. Sulmeyer Michael. Cybersecurity in the 2017 National Security Strategy / Michael Sulmeyer. // Lawfare. 19.12.2017. URL: https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy (дата обращения: 01.03.2018). [↑](#footnote-ref-125)
126. National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения: 01.03.2018). [↑](#footnote-ref-126)
127. Department Of Homeland Security Statement On The President’s Fiscal Year 2019 Budget // U.S. Department Of Homeland Security 12.02.2018. URL: https://www.dhs.gov/news/2018/02/12/department-homeland-security-statement-president-s-fiscal-year-2019-budget (дата обращения: 01.03.2018). [↑](#footnote-ref-127)
128. Budget in brief. Fiscal year 2017 // U.S. Department Of Homeland Security 16.02.2016. URL: https://www.dhs.gov/sites/default/files/publications/FY2017\_BIB-MASTER.pdf (дата обращения: 01.03.2018). [↑](#footnote-ref-128)
129. Walcott John. U.S. Is Drafting Potential Sanctions Over China Cyber Hacking. / John Walcott // Bloomberg. 31.08.2015. URL: http://www.bloomberg.com/news/articles/2015-08-31/u-s-said-to-draft-potential-sanctions-over-china-cyber-hacking (дата обращения: 09.03.2018). [↑](#footnote-ref-129)
130. 手机加密的方法Шоуцзи цзями дэ фанфа [метод шифрования сотовой связи]. 发明专利说明书Фамин чжуаньли шоминшу [описание патента изобретения]// 中华人民共和国国家知识产权局Чжунхуа жэньминь гунхэго гоцзя чжиши чаньцюаньцзюй [Государственное ведомство интеллектуальной собственности Китайской Народной Республики] 09.09.1999 URL: https://patentimages.storage.googleapis.com/73/fb/81/f7540b88b0da7a/CN1115924C.pdf (дата обращения: 09.03.2018). [↑](#footnote-ref-130)
131. 2002年中国的国防 2002 нянь чжунго дэ гофан [Национальная оборона Китая в 2002 году] // 中华人民共和国国务院新闻办公室2002. Чжунхуа жэньминь гунхэго гоуюань синьвэнь бангунши. 2002［Информационное бюро Государственного совета Народной Республики Китай. 2002] URL: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925.htm (дата обращения: 09.03.2018). [↑](#footnote-ref-131)
132. 国家信息化领导小组关于加强信息安全保障工作的意见 (中办发[2003] 27号) Гоцзя синьсихуа линдао сяоцзу гуаньюй цзяцян синьси аньцюань баочжан гунцзо дэ ицзянь (Чжунбаньфа[2003] 27Хао) [Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности (опубликовано Главным управлением ЦК КПК № 27 от 2003 г.)] // EIC. XM. GOV. CN: Информационный центр г. Сямэнь. URL: http://eic.xm.gov.cn/xgfw/aqcp/djbh/201411/P020141104292325316962.pdf (дата обращения: 09.03.2018). [↑](#footnote-ref-132)
133. 联网新闻信息服务管理规定 Ляньван синьвэнь синьси фуу гуаньли гуйдин [Положение по регулированию новостных информационных услуг в интернете] // CAC. GOV. CN: официальный сайт Центральной ведущей группы по кибербезопасности. 30.09.2005. URL: http://www.cac.gov.cn/2005‑09/30/c\_126468838.htm (дата обращения: 09.03.2018). [↑](#footnote-ref-133)
134. 2006━2020年国家信息化发展战略2006━2020 нян гоцзя синьсихуа фачжань чжаньлюэ [Государственная стратегия по развитию информатизации. 2006—2020] // 新华网 09.05.2005. Синьхуаван 09.05.2005. [Информационное агентство «Синьхуа» 09.05.2005.] URL: http://news.xinhuanet.com/politics/2006‑05/09/content\_4524651.htm (дата обращения: 09.03.2018). [↑](#footnote-ref-134)
135. 胡锦涛在全国科学技术大会上的讲话(全文) Хуцзиньтао цзай цюань гокэсюэ цзишудахуэйшан дэ цзянхуа (Цюань вэнь) [Речь Ху Цзиньтао на Национальной научно-технической конференции (полная речь)] //中国共产党新闻Чжунго гунчаньдан синьвэнь [Новости КПК] 10.01.2006. URL: http://cpc.people.com.cn/GB/64093/64094/4455445.html (дата обращения: 09.03.2018). [↑](#footnote-ref-135)
136. 2006━2020年国家信息化发展战略2006━2020 нян гоцзя синьсихуа фачжань чжаньлюэ [Государственная стратегия по развитию информатизации. 2006—2020] // 新华网 09.05.2006. Синьхуаван 09.05.2006. [Информационное агентство «Синьхуа» 09.05.2006.]. URL: http://news.xinhuanet.com/politics/2006‑05/09/content\_4524651.htm (дата обращения: 09.03.2018). [↑](#footnote-ref-136)
137. Fortune Global Forum 2013 // Fortune Live Media. URL: http://www.fortuneconferences.com/global-forum-2013/2013-speakers/ (дата обращения: 13.03.2018) [↑](#footnote-ref-137)
138. International respect needed in cyber security: official. // Xinhua, English.news.cn. 08.06.2013. URL:

http://english.peopledaily.com.cn/90883/8278445.html (дата обращения: 13.03.2018). [↑](#footnote-ref-138)
139. Chinese government to strengthen international cooperation on cyber issues: official // Xinhua, English.news.cn. 04.10.2012. URL: http://news.xinhuanet.com/english/china/2012–10/04/c\_131888329.htm. (дата обращения: 13.03.2018). [↑](#footnote-ref-139)
140. 中央网络安全和信息化领导小组成立Чжунъян ванло аньцюань хэ синьсихуа линдао сяоцзу чэнли [Основание ведущей группы по кибербезопасности и информатизации] // 新华网 28.02.2014. Синьхуаван 28.02.2014. [Информационное агентство Синьхуа 28.02.2014] URL: http://www.xinhuanet.com/info/2014-02/28/c\_133148759.htm (дата обращения: 13.03.2018). [↑](#footnote-ref-140)
141. Panda Ankit. Xi Jinping: China Should Become a 'Cyber Power'. Xi Jinping has great ambitions for China in cyberspace. / Ankit Panda // The Diplomat 04.03.2014. URL: https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/ (дата обращения: 13.03.2018). [↑](#footnote-ref-141)
142. Sandle Paul. Cyber crime costs global economy $445 billion a year: report / Paul Sandle // Reuters. 09.06.2014. URL: https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609 (дата обращения: 13.03.2018). [↑](#footnote-ref-142)
143. Segal Adam. From Net Politics and Digital and Cyberspace Policy Program: China’s New Cybersecurity Law / Adam Segal // Council on Foreign Relations 08.07.2015. URL: https://www.cfr.org/blog/chinas-new-cybersecurity-law (дата обращения: 13.03.2018). [↑](#footnote-ref-143)
144. Yan Sophia. China's new cybersecurity law takes effect today, and many are confused / Sophia Yan // CNBC. 31.05.2017. URL: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html (дата обращения: 13.03.2018). [↑](#footnote-ref-144)
145. Wagner Jack. China's Cybersecurity Law: What You Need to Know: The law, which comes into effect June 1, raises data protection concerns for foreign firms. / Jack Wagner // The Diplomat. 01.06.2017. URL: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ (дата обращения: 13.03.2018). [↑](#footnote-ref-145)
146. Miles Tom. U.S. asks China not to enforce cyber security law / Tom Miles // Reuters. 26.09.2017. URL: https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1 (дата обращения: 13.03.2018). [↑](#footnote-ref-146)
147. 譚瑾瑜Тан Цзиньюй. 大陸十三五規劃趨勢與台灣因應建言Далу шисаньу гуихуа цюши ю тайвань иньин цзяньянь [Тенденции тринадцатой пятилетки в Китае и ответ Тайваня на выдвинутые предложения]/ 譚瑾瑜Тан Цзиньюй //財團法人.國家政策研究基金會 Цайтуан фажэнь. Гоцзя чжэнцэ яньцзю цзицзиньхуи [Консорциум. Фонд исследований национальной политики]. 02.12.2014. URL: https://www.npf.org.tw/3/14471 (дата обращения: 13.03.2018). [↑](#footnote-ref-147)
148. Китай пройдет три этапа на пути к кибердержаве // Russian.news.ch Синьхуа Новости. URL: http://russian.news.cn/2016-07/27/c\_135544806.htm (дата обращения: 13.03.2018). [↑](#footnote-ref-148)
149. International Strategy of Cooperation on Cyberspace // 新华网Xinhua News. 01.03.2017. URL: http://www.xinhuanet.com/english/china/2017-03/01/c\_136094371.htm (дата обращения: 16.03.2018). [↑](#footnote-ref-149)
150. UN GA 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур // Генеральная Ассамблея ООН. 21.12.2009. URL: http://www.un.org/ga/search/view\_doc.asp?symbol=A/RES/64/211&referer=https://www.google.ch/&Lang=R (дата обращения: 16.03.2018). [↑](#footnote-ref-150)
151. Xinhua Headlines: Xi outlines blueprint to develop China's strength in cyberspace // 新华网 Xinhua News. 21.04.2018. URL: http://www.xinhuanet.com/english/2018-04/21/c\_137127374.htm (дата обращения: 22.04.2018). [↑](#footnote-ref-151)
152. Messmer Ellen. Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says / Ellen Messmer // CNN. 12.05.1999. URL: http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/ (дата обращения: 20.03.2018). [↑](#footnote-ref-152)
153. 勿忘2001中美黑客大战 Уван 2001 Чжунмэй хэйкэ дачжань [Не забыть об американо-китайской хакерской войне 2001 года] // 铁血网 06.12.2009. Тесюэван 06.12.2009. [tiexue.net 06.12.2009.] URL: http://bbs.tiexue.net/post2\_3975999\_1.html (дата обращения: 20.03.2018). [↑](#footnote-ref-153)
154. Tang Rose. China-U.S. cyber war escalates / Rose Tang // CNN. 01.05.2001. URL: http://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/ (дата обращения: 20.03.2018). [↑](#footnote-ref-154)
155. Sweet William. The Blackout of 2003 / William Sweet // IEEE Spectrum. 01.08.2003. URL: https://spectrum.ieee.org/energy/the-smarter-grid/the-blackout-of-2003 (дата обращения: 20.03.2018). [↑](#footnote-ref-155)
156. Norton-Taylor Richard. Titan Rain - how Chinese hackers targeted Whitehall / Richard Norton-Taylor // The Guardian. 05.09.2007. URL: https://www.theguardian.com/technology/2007/sep/04/news.internet (дата обращения: 20.03.2018). [↑](#footnote-ref-156)
157. Старкин С. В. Анализ разведывательной информации по транснациональному терроризму в современных внешне-политических условиях: подходы американских теоретиков / С. В. Старкин // Гуманитарные исследования. - 2011. № 1 (37). С. 7. [↑](#footnote-ref-157)
158. Digital Attack Map. Top daily DDoS attacks worldwide // Digital Attack Map. URL: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17650&view=map (дата обращения: 22.03.2018). [↑](#footnote-ref-158)
159. O'Brien Robert D., Shiran Shen. The U.S., China, and Cybersecurity: The Ethical Underpinnings of a Controversial Geopolitical Issue / Robert D. O'Brien, Shen Shiran. / Сarnegie Council for Ethics in International Affairs. 24.05.2013. URL: https://www.carnegiecouncil.org/publications/articles\_papers\_reports/0156 (дата обращения: 22.03.2018). [↑](#footnote-ref-159)
160. Hirschfeld Davis Julie, Sanger David E. Obama and Xi Jinping of China Agree to Steps on Cybertheft. / Davis Julie Hirschfeld, David E. Sanger // NYTimes, 26.09.2015. URL: http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html (дата обращения: 22.03.2018). [↑](#footnote-ref-160)
161. Китай, Россия, Таджикистан и Узбекистан предлагают принять Правила обеспечения международной информационной безопасности // Новости ООН. 18.10.2012. URL: https://news.un.org/ru/story/2012/10/1211561 (дата обращения: 22.03.2018). [↑](#footnote-ref-161)
162. Shu Catherine. China Tried To Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration / Catherine Shu. // TechCrunch 21.11.2014. URL: https://techcrunch.com/2014/11/20/worldinternetconference-declaration/ (дата обращения: 22.03.2018). [↑](#footnote-ref-162)
163. Manjoo Farhad. Hacking the Old Gray Lady. The Chinese attack against the New York Times worked to perfection. / Farhad Manjoo // Slate. 31.01.2013. URL: http://www.slate.com/articles/technology/technology/2013/01/new\_york\_times\_chinese\_hackers\_the\_attack\_against\_the\_newspaper\_of\_record.html (дата обращения: 27.03.2018). [↑](#footnote-ref-163)
164. MacWhorter Dan. Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators. / Dan MacWhorter // FireEye. 19.02.2013. URL: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (дата обращения: 27.03.2018). [↑](#footnote-ref-164)
165. Report APT1: Exposing One of China’s Cyber Espionage Units // Mandiant. URL: http:// intelreport.mandiant.com/Mandiant\_APT1\_Report.pdf (дата обращения: 27.03.2018). [↑](#footnote-ref-165)
166. China's military to drill on digitalized forces // Xinhuanet. 29 May 2013. URL: http://news.

xinhuanet.com/english/china/2013–05/29/c\_132415053.htm (дата обращения: 27.03.2018). [↑](#footnote-ref-166)
167. Vranicar D. China to Conduct Digital War Games / D. Vranicar // Xinhuanet. 29 May 2013. URL: http:// www.technewsworld.com/story/78151.html (дата обращения: 27.03.2018). [↑](#footnote-ref-167)
168. Chen Te-Ping. Snowden Alleges U.S. Hacking in China / Te-Ping Chen // The Wall Street Journal. 23.06.2013. URL: https://www.wsj.com/articles/SB10001424127887324577904578562483284884530 (дата обращения: 27.03.2018). [↑](#footnote-ref-168)
169. 中国教育和科研计算机网 Чжунго цзяоюй хэ кэянь цзисуань цзиван [Образовательная сеть China Education and Research Network] // URL: http://www.edu.cn/ (дата обращения: 27.03.2018). [↑](#footnote-ref-169)
170. Goodman Peter S. Huawei Founder Ren Zhengfei Dismisses Chinese Military Connections. / Peter S. Goodman // International Business Times. 01.22.2015. URL: http://www.ibtimes.com/huawei-founder-ren-zhengfei-dismisses-chinese-military-connections-1791228 (дата обращения: 28.03.2018). [↑](#footnote-ref-170)
171. US Deterrence against Chinese Cyber Espionage. The Danger of Proliferating Covert Cyber Operations // Netherlands Institute of International Relations. September 2015. URL: https://www.academia.edu/15721992/US\_Deterrence\_against\_Chinese\_Cyber\_Espionage\_The\_Danger\_of\_Proliferating\_Covert\_Cyber\_Operations (дата обращения: 28.03.2018). [↑](#footnote-ref-171)
172. Gompert David C., Cevallos Astrid Stuth, Garafola Cristina L. War with China. Thinking Through the Unthinkable / David C. Gompert, Astrid Stuth Cevallos, Cristina L. Garafola // RAND Corporation. 28.07.2016. URL: https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1100/RR1140/RAND\_RR1140.pdf (дата обращения: 28.03.2018). [↑](#footnote-ref-172)
173. Swaine Michael D. Chinese Views on Cybersecurity in Foreign Relations / Michael D. Swaine // Cornegie Endowment for International Peace. China Leadership Minitor, no.42. URL: http://carnegieendowment.org/email/South\_Asia/img/CLM42MSnew.pdf (дата обращения: 28.03.2018). [↑](#footnote-ref-173)
174. Cadell Cate. Chinese state media says U.S. should take some blame for cyber attack. / Cate Cadell // Reuters. 17.05.2017. URL: https://www.reuters.com/article/us-cyber-attack-china/chinese-state-media-says-u-s-should-take-some-blame-for-cyber-attack-idUSKCN18D0G5 (дата обращения: 29.03.2018). [↑](#footnote-ref-174)
175. Mehta Aaron. A digital migraine? How the Americas can step up cybersecurity strategies / Aaron Mehta // Federal Times. 28.22.2017. URL: https://www.federaltimes.com/smr/cybercon/2017/11/29/a-digital-migraine-how-the-americas-can-step-up-cybersecurity-strategies/ (дата обращения: 31.03.2018). [↑](#footnote-ref-175)
176. Average annualized cost of cyber attacks on companies in selected countries as of August 2017 (in million U.S. dollars) // The Statistic Portal Statista. URL: https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ (дата обращения: 31.03.2018). [↑](#footnote-ref-176)
177. Lieberthal K. G., Singer P. W. Cybersecurity and U.S. – China Relations / K. G. Lieberthal, P. W. Singer // Brookings. 23.02.2012. URL: http://www.brookings.edu/research/papers/2012/02/23-cybersecurity-china-us-singer-lieberthal (дата обращения: 31.03.2018). [↑](#footnote-ref-177)
178. В США могут создать единую государственную 5G сеть для защиты от Китая // Information Security. Информационная безопасность. 29.01.2018. URL: http://www.itsec.ru/newstext.php?news\_id=121015 (дата обращения: 31.03.2018). [↑](#footnote-ref-178)
179. «Мы за интернационализацию управления интернетом». Спецпредставитель президента РФ о подходе Москвы к международной информационной безопасности. // Коммерсант.ru. 16.06.2014. URL: http://www.kommersant.ru/doc/2492206 (дата обращения: 04.04.2018). [↑](#footnote-ref-179)
180. Распоряжение от 30 апреля 2015 г. № 788-р. О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности // Правительство Российской Федерации. 30.04.2015. URL: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 04.04.2018). [↑](#footnote-ref-180)
181. Информационное общество и международные отношения: учебник / Р. В. Болгов, Н. А. Васильева, С. М. Виноградова, К. А. Панцерев; под ред. К. А. Панцерева; С7-Петерб. гос. ун-т. – СПб.: Изд-во СПбГУ, 2014. – с. 312. [↑](#footnote-ref-181)
182. Один из приоритетов ШОС – стремление создать международную информационную среду, для которой характерны мир, сотрудничество и гармония // Шанхайская Организация Сотрудничества. 27.11.2016. URL: http://rus.sectsco.org/news/20161127/160697.html (дата обращения: 04.04.2018). [↑](#footnote-ref-182)
183. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская Организация Сотрудничества. 16.06.2009. URL: http://rus.sectsco.org/load/203996/ (дата обращения: 04.04.2018). [↑](#footnote-ref-183)
184. Один из приоритетов ШОС – стремление создать международную информационную среду, для которой характерны мир, сотрудничество и гармония // Шанхайская Организация Сотрудничества. 27.11.2016. URL: http://rus.sectsco.org/news/20161127/160697.html (дата обращения: 04.04.2018). [↑](#footnote-ref-184)
185. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // Министерство Иностранных Дел Российской Федерации. 29.01.2015. URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset\_publisher/UsCUTiw2pO53/content/id/916241 (дата обращения: 04.04.2018). [↑](#footnote-ref-185)
186. Официальное описание проекта Подводная ВОЛС «Камчатка – Сахалин – Магадан» // Ростелеком. URL: https://www.rostelecom.ru/projects/FarEast\_FOCL/about/ (дата обращения: 04.04.2018). [↑](#footnote-ref-186)
187. Li Xiaokun, Zhang Yunbi. Core interests at heart of new US ties / Xiaokun Li, Yunbi Zhang // China Daily. 20.03.2013. URL: http://www.chinadaily.com.cn/china/2013–03/20/content\_16321491.htm (дата обращения: 07.04.2018). [↑](#footnote-ref-187)
188. Lew Tells China Cyber Attacks ‘Very Serious Threat To Our Economic Interests’ // CBS DC. 20.03.2013. URL: http://washington.cbslocal.com/2013/03/20/us-treasury-secretary-tells-china-cyber-attacks-a-very-serious-threat-to-our-economic-interests/ (дата обращения: 07.04.2018). [↑](#footnote-ref-188)
189. Чарльз Б. Чарльз Барри о подходах США и НАТО в области международной информационной безопасности. Взгляд на национальные и международные проблемы кибербезопасности. / Б. Чарльз // Digital Report. 01.05.2015. URL: https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/ (дата обращения: 07.04.2018). [↑](#footnote-ref-189)
190. Jones Terril Yue. U.S., China agree to work together on cyber security. / Terril Yue Jones // Reuters. 23.04.2013. URL: https://www.reuters.com/article/us-china-us-cyber/u-s-china-agree-to-work-together-on-cyber-security-idUSBRE93C05T20130413 (дата обращения: 07.04.2018). [↑](#footnote-ref-190)
191. Wilhelm Alex. China and the United States agree to create a joint cybersecurity working group / Alex Wilhelm // The Next Web. 13.04.2013. URL: http://thenextweb.com/insider/2013/04/13/china-and-the-united-states-will-create-a-joint-working-group-to-deal-with-cybersecurity/ (дата обращения: 07.04.2018). [↑](#footnote-ref-191)
192. First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes // Office of Public Affairs, U.S. the Department of Justice. 01.12.2015. URL: http://worldjpn.grips.ac.jp/documents/texts/USC/20151201.D1E.html (дата обращения: 07.04.2018). [↑](#footnote-ref-192)
193. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference // The White House. Office of the Press Secretary. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint (дата обращения: 07.04.2018). [↑](#footnote-ref-193)
194. Segal Adam. Stabilizing cybersecurity in the U.S.-China relationship. / Adam Segal // The National Bureau of Asian Research. September 2015. URL: http://nbr.org/downloads/pdfs/psa/US-China\_brief\_Segal\_Sept2015.pdf (дата обращения: 07.04.2018). [↑](#footnote-ref-194)
195. Gerstein Daniel M. Define Acceptable Cyberspace Behavior. The U.S.-China cybersecurity agreement is a welcome step, but also highlights bigger problems. / Daniel M. Gerstein // U.S. News. 26.09.2015. URL: http://www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights-bigger-issues (дата обращения: 07.04.2018). [↑](#footnote-ref-195)
196. Fact sheet: President Xi Jinping’s State Visit to the United States // The White House. Office of the Press Secretary. 25.09.2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (дата обращения: 11.04.2018). [↑](#footnote-ref-196)
197. Dilanian Ken. Russia May Be Hacking Us More, But China Is Hacking Us Much Less. / Ken. Dilanian // NBC News. 12.10.2016. URL: https://www.nbcnews.com/news/us-news/russia-may-be-hacking-us-more-china-hacking-us-much-n664836 (дата обращения: 11.04.2018). [↑](#footnote-ref-197)
198. Chin Josh. Inside the Slow Workings of the U.S.-China Cybersecurity Agreement. / Josh Chin // The Wall Street Journal. 15.06.2016. URL: https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/ (дата обращения: 11.04.2018). [↑](#footnote-ref-198)
199. Cirenza Patrick. Cyber privateers follow in the wake of their seafaring predecessors. / Patrick Cirenza // Nations&States. Millennial perspectives on world affairs. 28.02.2017. URL: https://nationsandstates.com/2017/02/28/cyber-privateers-follow-in-the-wake-of-their-seafaring-predecessors/ (дата обращения: 11.04.2018). [↑](#footnote-ref-199)
200. The Obama-Xi Cyber Mirage. A digital arms deal that is full of promises but no enforcement. // The Wall Street Journal. 27.09.2015. URL: https://www.wsj.com/articles/the-obama-xi-cyber-mirage-1443387248 (дата обращения: 11.04.2018). [↑](#footnote-ref-200)
201. Harold Scott W., Libicki Martin C., Cevallos Astrid Stuth. Getting to Yes with China in Cyberspace / Scott W. Harold, Martin C. Libicki, Astrid Stuth Cevallos. // RAND Corporation. 2016. URL: https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1300/RR1335/RAND\_RR1335.pdf (дата обращения: 11.04.2018). [↑](#footnote-ref-201)
202. Gerstein Daniel M. Define Acceptable Cyberspace Behavior. The U.S.-China cybersecurity agreement is a welcome step, but also highlights bigger problems. / Daniel M. Gerstein // U.S. News. 26.09.2015. URL: http://www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights -bigger-issues (дата обращения: 11.04.2018). [↑](#footnote-ref-202)
203. Joint Summary of Outcomes: Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue // U.S. the Department of Homeland Security. 15.06.2016. URL: http://worldjpn.grips.ac.jp/documents/texts/USC/20160615.D1E.html (дата обращения: 15.04.2018). [↑](#footnote-ref-203)
204. Chin Josh. Inside the Slow Workings of the U.S.-China Cybersecurity Agreement. / Josh Chin // The Wall Street Journal. 15.06.2016. URL: https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/ (дата обращения: 15.04.2018). [↑](#footnote-ref-204)
205. MacGregor A. China, U.S. making moves to implement cybersecurity agreements / A. MacGregor // The Stack.

14.06.2016. URL: https://thestack.com/security/2016/06/14/china-u-s-making-moves-toimplement-

cybersecurity-agreements/ (дата обращения: 15.04.2018). [↑](#footnote-ref-205)
206. Syeed N. U. S. Cyber Deal With China Is Reducing Hacking / N. Syeed // Bloomberg. 28.06.2016. URL: https://www.bloomberg.com/news/articles/2016–06–28/u-s-cyber-deal-with-china-isreducing-

hacking-official-says (дата обращения: 15.04.2018). [↑](#footnote-ref-206)
207. Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes // Office of Public Affairs, U.S.the Department of Justice. 08.12.2016. URL: https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues (дата обращения: 15.04.2018). [↑](#footnote-ref-207)
208. Third U. S. – China High-Level Joint Dialogue on Cybercrime and Related Issues // Homeland

Security. 08.12.2016. URL: https://www.dhs.gov/news/2016/12/08/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues (дата обращения: 15.04.2018). [↑](#footnote-ref-208)
209. Gan Nectar. China ‘willing to work with Trump on cybersecurity’ / Nectar Gan. // South China Morning Post. Diplomacy&Defence. 08.12.2016. URL: http://www.scmp.com/news/china/diplomacy-defence/article/2052881/china-willing-work-trump-cybersecurity (дата обращения: 15.04.2018). [↑](#footnote-ref-209)
210. Lemire Jonathan. Trump's Cybersecurity Review Misses Deadline / Jonathan Lemire. // U.S. News. 20.04.2017. URL: https://www.usnews.com/news/politics/articles/2017-04-20/trumps-cybersecurity-review-misses-deadline (дата обращения: 15.04.2018). [↑](#footnote-ref-210)
211. First U.S.-China Law Enforcement and Cybersecurity Dialogue // Department of Justice. Office of Public Affairs. 06.10.2017. URL: https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue (дата обращения: 18.04.2018). [↑](#footnote-ref-211)
212. 逸思Исы. 中美执法及网络安全对话 Чжунмэй чжифа цзи ванло аньцюань дуйхуа [Китайско-американское правоприменение и диалог по кибербезопасности] / 逸思 Исы // 網易新闻 Ванъи синьвэнь. URL: http://news.163.com/17/1005/12/D000JU35000187VE.html (дата обращения: 18.04.2018). [↑](#footnote-ref-212)