УДК: 327 + 94

Политика КНР по обеспечению кибербезопасности

Егор Александрович Разумов,
аспирант Института истории, археологии и этнографии народов Дальнего Востока ДВО РАН, Владивосток.
E-mail: razumov.egor@gmail.com

В статье на основе законодательной базы, официальных правительственных документов, таких как доктрины и стратегии, специальных программ развития, материалов из прессы и речей председателя Китайской Народной Республики Си Цзиньпина рассматривается эволюция политики Китая в области информационной безопасности и кибербезопасности. Возрастающая роль информационных технологий ставит перед государством новые вызовы, к которым относятся попытки иностранных акторов вести кибершпионаж против государственных структур, компаний и граждан, а также стремление противоборствующей стороны подорвать критически важную информационную инфраструктуру. Цель данной статьи — дать оценку проводимого Пекином курса по обеспечению кибербезопасности, а также выявить тенденции в восприятии угроз национальной безопасности в информационной сфере у представителей китайской политической элиты. Для этого рассматриваются структуры в государственном аппарате Китая, курирующие данную область. Несмотря на заметные действия представителей «пятого поколения» руководителей КНР в аспекте кибербезопасности, в государственной структуре не сформирована единая организация, которая отвечала бы за вырабатываемый политический курс в информационной сфере. Кроме Центрального военного совета этим занимаются Коммунистическая партия Китая и Госсовет КНР. При этом структура отвечающих за кибербезопасность отделов двух последних органов копирует соответствующую структуру в вооружённых силах страны. Особое место в обеспечении киберпространства КНР отводится Центральной ведущей группе по кибербезопасности и информатизации. Также в статье проводится анализ тенденций в законодательной системе КНР в исследуемой области. Отмечается укрепление технологического потенциала в информационной среде с целью догнать развитые страны, в частности Соединённые Штаты Америки; внедрение информационных технологий в производственный процесс и жизнь граждан; изменение действующей ограничительной модели на модель постепенного «открытия» китайского информационного сегмента.
Ключевые слова: информационная безопасность, киберсуверенитет, информационное пространство, Китай, Си Цзиньпин.

PRC's cybersecurity policy.
Egor Razumov, Institute of History, Archaeology and Ethnography of the Peoples of the Far East, FEB RAS, Vladivostok, Russia. E-mail: razumov.egor@gmail.com.

The article considers the evolution of China's policy in the field of information security and cybersecurity based on the legislative framework, official governmental documents such as doctrines and strategies, special programs of development, press

materials and speeches of the President of the People's Republic of China's Xi Jinping. The increasing role of information technologies poses new challenges to the country, which include attempts of foreign actors to conduct cyber espionage against government institutions, companies and citizens. This list also includes the intention of the opposing side to destabilize critically important information infrastructure. The aim of this article is to evaluate the cybersecurity which is organized by the Chinese government as well as to define the tendencies in perception of threats of the national security in infosphere among the representatives of the political elite. The article reviews the structures of China's state machine in the context of cybersecurity. Despite the noticeable actions of the fifth generation of Chinese leaders, there is no single organization which can be in charge for the political course in the field of information. In addition to the Central Military Commission, there are two more branches who are responsible for that: Chinese Communist Party and China's State Council. The structure of the last two authorities copy the structure of the one in the Armed Forces. The Central leading group for cybersecurity and informatization holds a special place in China's cyberspace. There is a tendency in the legislative system of the Chinese system to strengthen its technological potential in the information sphere in order to catch up with the developed countries, particularly the United States of America; to implement information technology in the production process and people's lives; to change the current restrictive model to the model of the gradual opening of Chinese information segment.
Keywords: information security, cybersovereignty, infosphere, China, Xi Jinping.

Стремительное развитие информационных технологий добавило в систему национальной безопасности Китайской Народной Республики новый аспект — кибербезопасность. Для Китая реализация подходов по обеспечению сохранности собственных цифровых данных имеет два важных направления: во-первых, необходимо обеспечить социальную стабильность и контроль над внутригосударственными процессами, во-вторых, — вести промышленный и экономический шпионаж против иностранных компаний и предприятий. Именно поэтому для Пекина указанная область является приоритетной.

Цель данной статьи — оценка проводимого китайским правительством курса по обеспечению кибербезопасности, а также выявление тенденции по восприятию угроз национальной безопасности в информационной сфере представителями политической элиты. В исследовании рассматривается исключительно политический аспект вопроса, без углубления в его техническую часть.

Задачи работы:

1. Проанализировать официальные документы, законопроекты, государственные программы и стратегии КНР в области обеспечения кибербезопасности.
2. Рассмотреть структуру государственных органов КНР, отвечающих за реализацию политических установок в киберпространстве.
3. Проследить формирование политического курса «пятого поколения» руководителей КНР во главе с Си Цзиньпином по проведению защитных мер в интернете.

Актуальность данной статьи обусловлена нарастающим присутствием Китайской Народной Республики в мировом информационном пространстве, а также действиями китайских государственных служб по обеспечению внутренней информационной безопасности и организации кибератак на критическую инфраструктуру, технологические предприятия иностранных государств.

Следует отметить, что проблематике обеспечения национальной безопасности в киберпространстве КНР посвящены работы американских исследователей Джона Линдсэй [12; 13], Даниэля Вентре [16]. В трудах данных авторов предпринята попытка дать теоретическое обоснование функционирования государственного аппарата Китайской Народной Республики в информационном пространстве. Также следует сказать о попытках Ган Чэня и Вэнь Чиньлима проследить возможности сотрудничества КНР и США в киберпространстве [7].

Среди китайских исследований необходимо выделить работы Фан Биньсина [31] и Ван Гуйфана [33], которые, однако, не имеют конкретных формулировок и зачастую соответствуют официальной позиции правительства Китайской Народной Республики. Также китайские авторы проводят сравнительный анализ подходов к обеспечению информационной безопасности КНР и США, делая большой упор на рассмотрение американской системы безопасности.

В России данная тематика представлена такими авторами, как Г. Ибрагимова [3], Г. Юрченко [5], К. Антипов [1], А. Булавин [2]. При этом стоит отметить, что в подобных исследованиях даётся общая характеристика системы кибербезопасности КНР, а источниковая база в основном состоит из наработок американских учёных.

НОРМАТИВНО-ПРАВОВАЯ БАЗА КНР В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

В нормативно-правовом аспекте обеспечения кибербезопасности КНР необходимо отметить следующие документы, которые являются ключевыми:

В 2000 г. Всекитайским собранием народных представителей была предпринята попытка определить классификацию возможных правонарушений в информационной сфере. В том же году было опубликовано «Постановление ВСНП по защите интернет-пространства», где выделялись те области, в которых могут осуществляться нарушения: экономическая, образовательная, сфера поддержания общественной стабильности и защиты граждан. Возник прецедент, когда государство попыталось создать классификацию вероятных информационных угроз и впоследствии разработать меры по обеспечению безопасности в этой сфере.

В 2003 г. Канцелярия ЦК КПК опубликовала «Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности» [26]. Текст документа закрепляет за ответственными лицами необходимость предпринимать шаги

по укреплению защиты важной и стратегической инфраструктуры, проведению мониторинга интернет-пространства на наличие возможных угроз для КНР, разработке мер для привлечения квалифицированных специалистов в области информационной безопасности, защите технического оборудования, содержащего в себе секретную информацию.

В 2006 г. была принята «Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.» В данном документе определяется важность внимания к области информационных технологий. В частности, предполагается на начальном этапе создать соответствующие структуры для регулирования деятельности в информационной сфере, тем самым делая шаги по укреплению системы по обеспечению технологической и информационной безопасности. Предусматривается установление направлений развития информатизации, определяются базовые векторы государственной политики в этой области. Также стратегия придерживается установки сочетания военной и гражданской продукции, предполагается создание собственного программного обеспечения [20]. Иностранные IT-компании и программное обеспечение (ПО) должны проходить обязательную сертификацию у государственных служб для функционирования на территории Китая.

«Государственная стратегия по обеспечению безопасности информационного пространства» рассматривает сферы, в которых могут возникнуть угрозы безопасности: государственное управление, экономическую, культурную, производственную и социальную сферы. В качестве основных приняты концепции «активной обороны» и «симметричного ответа на возникающие вызовы». Декларируются принципы мира, открытости, безопасности и сотрудничества [19]. В это время начинают продвигаться идеи «здорового информационного общества», «развития интернет-культуры в Китае», «строительства информационной площадки для социализма с китайской спецификой». Таким образом китайское политическое руководство старается заявить о единоличном управлении собственным информационным пространством. Призыв к миротворческим принципам тесно пересекается с внешнеполитическим курсом КНР — невмешательством в дела других государств. Тем самым может обеспечиваться перспектива мирного развития.

Всекитайским собранием народных представителей 27 декабря 2015 г. был принят Антитеррористический закон КНР. Предполагалось производить дешифровку интернет-трафика, использовать административные меры по изъятию у иностранных компаний и предприятий информации при подозрении на её использование для террористических нужд. Также предусматривалось введение цензуры для новостной деятельности на территории континентального Китая [18]. Иными словами, теперь иностранные средства массовых коммуникаций не имеют права публиковать информацию в сети без предварительного согласования с ответственными представителями государственных служб, публикуемая на иностранных и китайских новостных ресурсах информация не должна противоречить официальной позиции государственных СМИ — в частности Информационному агентству

«Синьхуа». В законе прописаны действия государственных органов по контролю над содержимым интернет-трафика. Создаются условия для полного контроля информационного пространства силами Центрального Военного совета в связи с реализацией предусмотренных в законе мер.

Всекитайским собранием народных представителей 7 ноября 2016 г. был принят Закон КНР о кибербезопасности. Он стал прецедентом в китайском законодательстве: в соответствии с ним официальный Пекин имеет право на законодательном уровне контролировать события, происходящие в китайском сегменте Интернета. Теперь публикуемый контент должен будет храниться на территории Китая не менее шести месяцев. Это касается социальных сетей, видео- и письменного блогинга. В законе очень большое внимание уделяется системе идентификации пользователей: для регистрации и проведения каких-либо операций в сети Интернет будет необходимо указать реальные данные пользователей [21]. Если раньше подобная практика имела место на отдельных технологических предприятиях, то теперь она распространилась на всю территорию страны.

В связи с активизацией защитных мер вводятся ограничения в области предоставления интернет-услуг [17; 25; 30]: контроль интернет-приложений, контроль над проведением виртуальных сделок в торгово-экономической сфере, контроль над информационно-вещательными услугами. В региональных народных правительствах утверждаются лица, отвечающие за проведение мероприятий по обеспечению безопасности. При возникновении угроз безопасности страны закон разрешает применение региональными властями мер по ограничению доступа к ведению переписки в Интернете, а также ограничению интернет-трафика. В случае выявления нарушений законом разрешается блокировка сайта, отзыв лицензии и иных разрешающих документов на проведение определённой деятельности.

Антитеррористический закон КНР и Закон КНР по кибербезопасности представляют собой результат проводимой уже несколько десятилетий политики Китая по обеспечению контроля над информационным пространством. С 2004 г. на территории Китайской Народной Республики реализуется проект «Золотой щит»: в сети Интернет блокируется нежелательный для политической власти контент. Однако стремительное развитие технологии ставит под сомнение эффективность данных усилий. Несмотря на попытки центральной власти блокировать VPN-сервисы и иное специализированное программное обеспечение для обхода запрещённых интернет-ресурсов, возможность доступа к противоправному контенту сохраняется, а значит, сохраняется вероятность иностранного влияния на процессы внутри КНР.

При постепенном замедлении темпов роста китайской экономики возрастает вероятность возникновения гражданских волнений и конфликтов с государственной властью. Поэтому, согласно Закону по кибербезопасности КНР, государственные структуры на разных уровнях власти получают обширные полномочия в области контроля над Интернетом. Главными идеями по-прежнему остаются создание «здоровой информационной среды» и обеспечение условий проведения «социализма с китайской спецификой».

Таким образом, если раньше основное внимание уделялось определению степени и характера вероятных угроз (создавалась модель закрытого интернета), то с приходом к управлению страной «пятого поколения» руководителей КНР во главе с Си Цзиньпином первоначальная модель стала изменяться и приобрела представительную функцию для действующей власти. Кроме того, Китай старается влиять на мировую информационную сеть, постепенно включаясь в её экономические процессы.

В 2015 г. Госсовет КНР опубликовал «Инструкцию по продвижению проекта „Интернет+“» [23]. Согласно этому документу, в индустриальном секторе будут внедряться современные и передовые технологии, предполагается применение возможностей Интернета в производстве [22], стимулирование и усиление инновационного развития, расширение сотрудничества китайских и иностранных компаний в области информационного взаимодействия. В рамках проекта планируется к 2025 г. провести компьютеризацию всех имеющихся на территории КНР предприятий.

СТРУКТУРА ГОСУДАРСТВЕННОГО АППАРАТА КНР ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

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 (Министерство индустрии и информационных технологий, Министерство науки и технологий КНР, Министерство государственной безопасности), которые могут быть задействованы в разработке соответствующих защитных мер в информационном пространстве, и ведущие малые группы, специализирующиеся на важных стратегических вопросах. Отмечается, что среди имеющихся ведущих малых групп внешнеполитическим направлением и вопросами национальной безопасности занимаются Центральная малая рабочая группа по внешней политике, Ведущая малая группа по вопросам национальной безопасности и Ведущая малая группа по проблемам Тайваня [2].

Большое влияние на политический курс в информационной сфере имеет Центральная ведущая группа по кибербезопасности и информатизации. Данная структура претерпела серьёзные изменения со своего возникновения в 1993 г. Постепенно подразделение приобрело статус основного центра по контролю над безопасностью в информационной среде. В 2014 г. Ведущая группа по государственной информатизации и Государственная координационная группа по сетевой и информационной безопасности были преобразованы в Центральную ведущую группу по кибербезопасности и информатизации [6]. Главной её целью является развитие информационных систем и поддержка IT-индустрии [32].

С 2013 г. в сфере вооружённых сил КНР стали происходить структурные изменения, связанные с проводимой новым политическим руководством страны реформой Народно-освободительной армии Китая (НОАК). Так,

вместо Генерального штаба НОАК главенствующей единицей стал Объединённый штаб, напрямую подчиняющийся Центральному военному совету при ЦК КПК [3].

По состоянию на 2015 г. в структуре военного аппарата КНР особое место занимает 3-й Департамент. В его функции входит руководство разведывательной деятельностью в Интернете, поиск уязвимостей информационных систем и проработка действий кибервойск по ведению кибератак против гражданских и военных объектов. Также в военный аппарат входят научно-исследовательские институты и центры, специализирующиеся на информационной безопасности, информационный и сертификационный центр, который представляет собой единую структуру по введению в гражданский сектор идеологического контроля над гражданскими информационными технологиями [12].

В качестве основного структурного подразделения НОАК, занимающегося кибершпионажем, можно отметить UNIT № 61398, которое с 2006 г. базируется в Шанхае [13]. Кроме того, в конце 2015 г. правительством КНР введено в строй подразделение стратегической поддержки НОАК [28]. Именно указанные подразделения призваны обеспечивать защищённость военной инфраструктуры от возможного повреждения, а также в случае необходимости производить атаки на важнейшие объекты предполагаемого противника.

РЕАЛИЗАЦИЯ ГОСУДАРСТВЕННОГО КУРСА

Для КНР существует ряд основных угроз, которые влияют на формирование единой политики в области кибербезопасности. Политический курс Китайской Народной Республики в этой области можно разделить на внутренний и внешний.

К первому направлению относится ограничение доступа к определённым информационным и новостным интернет-ресурсам, запрет на использование иностранного программного обеспечения и средств передачи голосовых и текстовых сообщений.

Необходимость контроля над информационным пространством была отмечена председателем «третьего поколения» руководителей КНР Цзян Цзэминем. Для решения данной задачи начала проводиться жёсткая политика по отношению к СМИ. Подобному решению способствовали события 1989 г. на площади Тяньаньмэнь в Пекине, которые поставили вопрос легитимности действующей политической власти и режима. Также одной из причин ужесточения контроля над информационным пространством могла стать угроза, исходившая от религиозного движения Фалуньгун (и впоследствии от их новостного ресурса «Великая Эпоха»), которое было официально запрещено в КНР в конце 90-х гг. XX в.

Американскими учёными отмечается, что к внутренним угрозам кибербезопасности стоит относить освещение различных событий внутри страны [11; 12]. Формирование «благоприятного» новостного фона (отказ

от освещения политических и социальных мероприятий, технологических и природных катастроф в СМИ) может являться стремлением ограничить влияние на Китай извне.

В 2004 г. Министерством государственной безопасности начата реализация проекта «Золотой щит» [16]: специальные серверы осуществляют фильтрацию интернет-трафика между китайскими провайдерами и международными сетями передачи информации. Государственной властью фактически предпринята попытка тотального контроля над информационным пространством. Делается это для того, чтобы ограничить доступ населения к иностранным источникам информации и средствам коммуникации. Тем самым формируется «правильное» восприятие действительности.

Один из аспектов внутреннего политического курса в области кибербезопасности связан с региональными особенностями. Так, в Синьцзян-Уйгурском автономном районе и Тибетском автономном районе значительная часть населения настроена против действующей власти — Коммунистической партии Китая — и может представлять угрозу кибербезопасности КНР.

В этом плане очень показателен массовый демократический протест в Гонконге и на Тайване в 2014 г. Координация действий бастующих осуществлялась через мессенджер Firechat [9]. Особенностью приложения является передача сообщений без подключения к интернету. Принцип работы схож с работой телефонной сети, которая использует мобильные устройства в качестве вышки связи. Mesh-сети (они же беспроводные ячеистые сети) формируют прямую связь между пользователями, которая, разделяясь на части, постепенно поступает адресату. Передача в основном происходит через беспроводную сеть Bluetooth, которая даёт возможность функционирования на расстоянии в 50—60 м от мобильных устройств, а территория охвата зависит от количества задействованных пользователей. Проблема официальных властей в Гонконге заключалась в невозможности контроля над протестующими и неспособности повлиять на ход событий.

Кратким итогом курса китайского правительства на развитие информационных технологий стало создание собственного программного обеспечения. Для осуществления мер безопасности на крупных политических, экономических, культурных и спортивных мероприятиях на территории КНР используются сервисы и услуги следующих китайских компаний:

1. Компанией Huawei обеспечивается защита роутеров и коммуникативных устройств.
2. Компанией Venustech ведётся мониторинг вторжения и предотвращение вероятности появления угроз.
3. В рамках защиты от вирусов и прочего нежелательного программного обеспечения применяется антивирус Qihu 360.
4. Реализация блокировки данных от внешних угроз возможна благодаря ПО от Leadsec.
5. Westone применяется система криптографического шифрования имеющейся информации [12].

Согласно статистическим данным агентства China Internet Network Information Center (CNNIC), на период с начала 2015 г. по декабрь 2016 г.

92,4% работающих на территории КНР предприятий предприняло меры по укреплению собственной защиты в информационном пространстве с использованием антивирусного ПО. Бесплатное ПО на 2016 г. используют 48,6% (в 2015 г. показатель составил 74,1%), платное ПО — 41% на 2016 г. (в 2015 г. показатель составил 2,3%), а одновременно платное и бесплатное ПО используют 47,3% за 2016 г. (23,6% за 2015 г.) [14]. Увеличение численности пользователей сети влечёт за собой необходимость укреплять действующую технологическую инфраструктуру для обеспечения безопасности.

В китайском информационном пространстве функционируют два крупных мессенджера, разработанные компанией Tencent, — WeChat и QQ. Являясь популярными на территории КНР приложениями, они охватывают почти всё население страны. В отличие от иностранных средств передачи информации китайские мессенджеры не имеют хорошей системы шифрования данных [11]. Это даёт возможность органам государственной власти собирать необходимую информацию о пользователях. В дальнейшем это может привести к более успешному пресечению протестных акций.

По статистике агентства CNNIC, количество пользователей сети Интернет на территории Китая составило на начало 2017 г. 751 млн чел. Число пользователей мобильным интернетом составило 723 млн чел. при распространении мобильной сети Интернет на территории Китая в 96,3%, а коэффициент распространения интернета составил 54,3% [15].

К внешнему направлению политического курса в области кибербезопасности КНР относятся кибератаки и прочие действия специализированных государственных подразделений в информационной сфере для нанесения ущерба или повреждения критически важной инфраструктуры сил противника в случае вероятной информационной войны или конфликта.

В области кибератак на иностранные технологические компании Китайская Народная Республика отстаёт от западных стран. Несмотря на значительное экономическое развитие Китая, с начала реализации политики реформ и открытости в 80-х гг. XX в. именно наукоёмкая сфера нуждается в серьёзной модернизации. Стоит отметить, что производственная часть имеет двойственную конверсию: военную и гражданскую. Поэтому кража технической документации может быть использована государственными промышленными корпорациями в собственных интересах.

Кроме этого, информационное пространство может служить Китаю для продвижения внешнеполитического курса через механизмы «мягкой силы». Иными словами, китайские информационные агентства и новостные порталы могут распространять материалы, формирующие положительный образ политической власти, культуры и истории Китая среди иностранной аудитории. Это в свою очередь даёт возможность влиять на общественное сознание иностранных граждан, тем самым упрощая вероятность достижения внешнеполитических целей.

Важным аспектом является продвижение идеологической составляющей — инициативы «Один пояс — один путь». Неточность официальных формулировок единой концепции даёт возможность китайской стороне

реализовывать собственную внешнеэкономическую политику, а информационная среда является качественным инструментом донесения пропагандистской информации до иностранной аудитории.

Другой важной стороной идеологического фактора является подтверждение центральным политическим руководством значимости кибербезопасности. Председатель КНР Си Цзиньпин отмечает важность развития информационных технологий [10], так как «без должного внимания к кибербезопасности не может существовать целостная система национальной безопасности, а без информатизации невозможно провести модернизацию» [8]. В 2015 г. в г. Учжэне на международной конференции по развитию Интернета Си Цзиньпин заявил, что Китай будет отстаивать свои национальные интересы в Интернете и не потерпит компромисса в вопросах обеспечения киберсуверенитета КНР [29].

ЗАКЛЮЧЕНИЕ

Кибербезопасность постепенно стала важнейшим аспектом национальной безопасности Китайской Народной Республики, поэтому властями всё больше внимания уделяется реализации защитных мер в Интернете. Базовой целью подобных действий является обеспечение легитимности действующей власти, а также выполнение представительских функций Коммунистической партии Китая в сети Интернет.

В нормативно-правовой системе КНР прослеживается тенденция замены действующей ограничительной модели на модель постепенного «открытия» китайского информационного сегмента. Это связано с необходимостью включения Китая в мировые информационно-финансовые процессы. Вместе с этим постепенно происходит внедрение информационных технологий в производственный процесс и жизнь граждан. Закон о кибербезопасности КНР и Антитеррористический закон КНР фактически являются итогом работы китайского правительства в информационной сфере. В них описана уже используемая практика ведения ограничительных действий государственных структур. На официальном уровне обосновывается необходимость хранения пользовательских данных на серверах, расположенных непосредственно на территории Китайской Народной Республики.

В государственном аппарате КНР ведущее место по обеспечению кибербезопасности занимает Военный совет при ЦК КПК. Несмотря на формальное разделение правительства на гражданский и военный сектор, вся полнота власти принадлежит председателю КНР Си Цзиньпину. Наибольшее влияние на регулирование информационных процессов имеет руководство НОАК. Поэтому вооружённые силы имеют значительное преимущество над гражданскими структурами, т.к. в полномочия военных входит проведение любых операций, в т.ч. политический, экономический, промышленный шпионаж. Также следует отметить большую вероятность использования военных сил в работе гражданских компаний. Особое место

в обеспечении безопасности киберпространства КНР занимает Центральная ведущая группа по кибербезопасности и информатизации.

Немаловажной для кибербезопасности Китая является идеологическая составляющая. Концентрация всей полноты власти в одних руках повышает значение идеологического фактора для политического курса в информационном пространстве. «Пятое поколение» руководителей КНР неоднократно отмечало значимость кибербезопасности для стабильности государства. Также в этой сфере проводится попытка реализовать инициативу «Пояса и пути», заключающуюся не только в продвижении внешнеэкономического курса, но и в использовании пропагандистских рычагов влияния на иностранные государства.

ЛИТЕРАТУРА И ИСТОЧНИКИ

1. Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 39—54.
2. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика и право. 2014. № 1. С. 27—31.
3. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности // Индекс безопасности. 2013. № 1 (104). С. 169—184.
4. Кашин В. Новый облик дракона // LENTA.RU: новостное интернет-издание «Lenta.ru». URL: https://lenta.ru/articles/2016/01/13/pla/ (дата обращения: 05.12.2016).
5. Юрченко Г. Возможности Китая по проведению компьютерных сетевых операций и кибершпионажу // BELVPO.COM: информационный портал «Военно-политическое обозрение». URL: http://www.belvpo.com/9984.htm (дата обращения: 25.09.2017).
6. Chang A. Warring State. China's Cybersecurity Strategy. December, 2014 // CRYPTOME.ORG: информационный портал. URL: https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf (дата обращения: 07.01.2017).
7. Chen Gang, Lim Wen Xin. Xi Jinping's Economic Cybersecurity Agreement with Barack Obama // IPPREVIEW.COM: информационный портал International Public Policy Review. URL: http://ippreview.com/index.php/Home/Blog/single/id/35.html (дата обращения: 05.12.2016).
8. China Voice: China allows no compromise on cyberspace sovereignty // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/english/2015-12/16/c_134924241.htm (дата обращения: 07.01.2017).
9. Cohen N. Hong Kong Protests Propel FireChat Phone-to-Phone App // NYTIMES.COM: официальный сайт газеты The New York Times. URL: http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html?_r=1 (дата обращения: 05.12.2016).
10. Full Text: Message of Congratulations from Chinese President Xi Jinping // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/english/china/2014-11/19/c_133799639.htm (дата обращения: 07.01.2017).

11. Harwit E. WeChat: social and political development of China's dominant messaging app // Chinese Journal of Communication. 2016. Vol. 10. Issue 3. P. 1—16.
12. Lindsay Jon R., Cheung Tai Ming, Reveron Derek S. China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain. Oxford: Oxford University Press, 2015. 379 p.
13. Lindsay Jon R. The Impact of China on Cybersecurity // International Security. 2015. Vol. 39. № 3. P. 7—47.
14. The 39th Statistical Report on Internet Development in China. January, 2017 // CNNIC.COM.CN: официальный сайт некоммерческой организации China Internet Network Information Center. URL: http://cnnic.com.cn/IDR/ReportDownloads/201706/P020170608523740585924.pdf (дата обращения: 25.09.2017).
15. The 40th China Statistical Report on Internet Development. July, 2017 // CNNIC.NET.CN: официальный сайт некоммерческой организации China Internet Network Information Center. URL: http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf (дата обращения: 25.09.2017).
16. Ventre D. Chinese Cybersecurity and Defense. London: Wiley-ISTE, 2014. 301 p.
17. 互联网信息服务管理办法 = Административные меры по информационному обслуживанию в Интернете // CAC.GOV.CN: официальный сайт Центральной ведущей группы по кибербезопасности. URL: http://www.cac.gov.cn/2000-09/30/c_126193701.htm (дата обращения: 05.12.2016).
18. 中华人民共和国反恐怖主义法 = Антитеррористический Закон КНР // NPC.GOV.CN: официальный сайт Всекитайского собрания народных представителей. URL: http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm (дата обращения: 05.12.2016).
19. 国家网络空间安全战略 = Государственная стратегия по обеспечению безопасности информационного пространства // CAC.GOV.CN: официальный сайт Центральной ведущей группы по кибербезопасности. URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 07.01.2017).
20. 2006—2020年国家信息化发展战略 = Государственная стратегия по развитию информатизации. 2006—2020 // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/politics/2006-05/09/content_4524651.htm (дата обращения: 07.01.2017).
21. 中华人民共和国网络安全法= Закон КНР о кибербезопасности // NPC.GOV.CN: официальный сайт Всекитайского собрания народных представителей. URL: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (дата обращения: 05.12.2016).
22. 国务院关于深化制造业与互联网融合发展的指导意见 = Инструкция Госсовета КНР по углублению интеграции производственных отраслей и интернета // CAC.GOV.CN: официальный сайт Центральной ведущей группы по кибербезопасности. URL: http://www.cac.gov.cn/2016-05/20/c_1118905368.htm (дата обращения: 05.12.2016).
23. 关于积极推进"互联网＋"行动的指导意见 = Инструкция по продвижению проекта «Интернет+» // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/politics/2015-07/04/c_1115815942.htm (дата обращения: 07.01.2017).
24. 联网新闻信息服务管理规定 = 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: 05.12.2016).
25. 国务院出台意见推进信息化发展切实保障信息安全.〔2012〕23号 = Постановление Госсовета КНР по продвижению информатизации и развитию действующей

защиты информационной безопасности № 23 от 2012 г. // GOV.CN: официальный сайт правительства КНР. URL: http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm (дата обращения: 05.12.2016).
26. 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) = 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: 05.12.2016).
27. 全国人民代表大会常务委员会关于加强网络信息保护的决定 = Решение ПК ВСНП по усилению защиты сетевой информации // CAC.GOV.CN: официальный сайт Центральной ведущей группы по кибербезопасности. URL: http://www.cac.gov.cn/2012-12/29/c_133353262.htm (дата обращения: 05.12.2016).
28. 习近平向中国人民解放军陆军火箭军战略支援部队授予军旗并致训词 = Си Цзиньпин вручил военные флаги ракетным войскам и войскам стратегической поддержки НОАК и выступил с наставлением // CPC.PEOPLE.COM.CN: официальный сайт газеты «Жэньминь жибао». URL: http://cpc.people.com.cn/BIG5/n1/2016/0102/c64094-28003839.html (дата обращения: 07.01.2017).
29. 习近平:把我国从网络大国建设成为网络强国 = Си Цзиньпин: превращая наше государство из крупной интернет-державы в Великую интернет-державу // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm (дата обращения: 07.01.2017).
30. 国务院办公厅关于进一步加强互联网上网服务营业场所管理的通知 = Сообщение Канцелярии Госсовета КНР по продвижению усиления регулятивных мер по отношению к предприятиям, оказывающим интернет-услуги // GOV.CN: официальный сайт правительства КНР. URL: http://www.gov.cn/zhengce/content/2016-09/30/content_5114029.htm (дата обращения: 05.12.2016).
31. 方滨兴，杜阿宁，张熙，王忠儒. 国家网络空间安全国际战略研究 = Фан Биньсин, Чжун Си, Ван Яжунжу. Исследование международной стратегии национальной безопасности в области киберпространства // 中国工程科学 2016 年 第18 卷 第6 期. 13-16 页 = Chinese academy of engineering journal. 2016. № 6. P. 13—16.
32. 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 = Ведущая центральная группа по вопросам сетевой информации и информатизации: от крупного информационного государства к крупной интернет-державе // NEWS.XINHUANET.COM: информационное агентство «Синьхуа». URL: http://news.xinhuanet.com/politics/2014-02/27/c_119538719.htm (дата обращения: 02.05.2017).
33. 王桂芳. 大国网络竞争与中国网络安全战略选择 = Ван Гуйфан. Кибер-конкуренция между Великими державами и стратегический выбор кибербезопасности Китая // 国际安全研究2017. № 2. P. 27—46.

REFERENCES

1. Antipov K. Kiberkonflikt v kitaysko-amerikanskikh otnosheniyakh i poiski dialoga [Cyber conflict in Sino-US relations and the search for dialogues]. *Problemy Dal'nego Vostoka*, 2013, no. 6, pp. 39—54. (In Russ.)
2. Bulavin A.V. O podkhodakh SSHA i Kitaya k obespecheniyu kiberbezopasnosti [The approaches of the USA and China to cybersecurity]. *Obshchestvo: politika, ekonomika i pravo,* 2014, no. 1, pp. 27—31. (In Russ.)
3. Ibragimova G. Strategiya KNR v kiberprostranstve: voprosy upravleniya internetom i obespecheniye informatsionnoy bezopasnosti [China's strategy in cyberspace:

Internet governance and information security]. *Indeks bezopasnosti*, 2013, no. 1 (104). pp. 169—184. (In Russ.)
4. Kashin V. *Novyy oblik drakona* [A new appearance of the dragon]. Available at: https://lenta.ru/articles/2016/01/13/pla/ (accessed 05.12.2016). (In Russ.)
5. Yurchenko G. *Vozmozhnosti Kitaya po provedeniyu komp'yuternykh cetevykh operatsiy i kibershpionazhu* [China's possibilities in computer network operations and cyber espionage]. Available at: http://www.belvpo.com/9984.htm (accessed 25.09.2017). (In Russ.)
6. Chang A. *Warring State. China's Cybersecurity Strategy. December, 2014*. Available at: https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf (accessed 07.01.2017). (In Eng.)
7. Chen Gang, Lim Wen Xin. *Xi Jinping's Economic Cybersecurity Agreement with Barack Obama*. Available at: http://ippreview.com/index.php/Home/Blog/single/id/35.html (accessed 05.12.2016). (In Eng.)
8. *China Voice: China allows no compromise on cyberspace sovereignty*. Available at: http://news.xinhuanet.com/english/2015-12/16/c_134924241.htm (accessed 07.01.2017). (In Eng.)
9. Cohen N. *Hong Kong Protests Propel FireChat Phone-to-Phone App*. Available at: http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html?_r=1 (accessed 05.12.2016). (In Eng.)
10. *Full Text: Message of Congratulations from Chinese President Xi Jinping*. Available at: http://news.xinhuanet.com/english/china/2014-11/19/c_133799639.htm (accessed 07.01.2017). (In Eng.)
11. Harwit E. WeChat: social and political development of China's dominant messaging app. *Chinese Journal of Communication*, 2016, vol. 10, issue 3, pp. 1—16. (In Eng.)
12. Lindsay Jon R., Cheung Tai Ming, Reveron Derek S. *China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain*. Oxford, Oxford University Press Publ., 2015, 379 p. (In Eng.)
13. Lindsay Jon R. The Impact of China on Cybersecurity. *International Security*. 2015, vol. 39, no. 3, p. 7—47. (In Eng.)
14. *The 39th Statistical Report on Internet Development in China. January, 2017*. Available at: http://cnnic.com.cn/IDR/ReportDownloads/201706/P020170608523740585924.pdf (accessed 25.09.2017). (In Eng.)
15. *The 40th China Statistical Report on Internet Development. July, 2017*. Available at: http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf (accessed 25.09.2017). (In Eng.)
16. Ventre D. *Chinese Cybersecurity and Defense*. London, Wiley-ISTE Publ., 2014, 301 p. (In Eng.)
17. *互联网信息服务管理办法* [Administrative measures about Internet information services]. Available at: http://www.cac.gov.cn/2000-09/30/c_126193701.htm (accessed 05.12.2016). (In Chin.)
18. *中华人民共和国反恐怖主义法* [Anti-terrorism law of the People's Republic of China]. Available at: http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm (accessed 05.12.2016). (In Chin.)
19. *国家网络空间安全战略* [National strategy for information space security]. Available at: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (accessed 07.01.2017). (In Chin.)
20. *2006—2020年国家信息化发展战略* [2006—2020 National information development strategy]. Available at: http://news.xinhuanet.com/politics/2006-05/09/content_4524651.htm (accessed 05.12.2016). (In Chin.)

21. *国务院关于深化制造业与互联网融合发展的指导意见* [Law of the People's Republic of China on cybersecurity]. Available at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (accessed 05.12.2016). (In Chin.)
22. *国务院关于深化制造业与互联网融合发展的指导意见* [Guiding instructions of the State Council of China on the intensive development of integration of manufacturing branches and the Internet]. Available at: http://www.cac.gov.cn/2016-05/20/c_1118905368.htm (accessed 05.12.2016). (In Chin.)
23. *关于积极推进"互联网+"行动的指导意见* [Instructions on promotion of the project "Internet+"]. Available at: http://news.xinhuanet.com/politics/2015-07/04/c_1115815942.htm (accessed 05.12.2016). (In Chin.)
24. *联网新闻信息服务管理规定* [The statement on information services on the Internet]. Available at: http://www.cac.gov.cn/2005-09/30/c_126468838.htm (accessed 05.12.2016). (In Chin.)
25. *国务院出台意见推进信息化发展切实保障信息安全.〔2012〕23号* [The State Council of China issued the resolution № 23 from 2012 on the promotion of the development of information technology and effective information security]. Available at: http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm (accessed 05.12.2016). (In Chin.)
26. *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)* [The statement of the State Leading Group on strengthening information security]. Available at: http://eic.xm.gov.cn/xgfw/aqcp/djbh/201411/P020141104292325316962.pdf (accessed 05.12.2016). (In. Chin.)
27. *全国人民代表大会常务委员会关于加强网络信息保护的决定* [Decision of the Standing Committee of the National People's Congress on strengthening the protection of network information]. Available at: http://www.cac.gov.cn/2012-12/29/ c_133353262.htm (accessed 05.12.2016). (In Chin.)
28. *习近平向中国人民解放军陆军火箭军战略支援部队授予军旗并致训词* [Xi Jinping presented military flags to the missile forces and the strategic support forces of the Chinese People's Liberation Army and provided guidance]. Available at: http://cpc.people.com.cn/n1/2016/0102/c64094-28003839.html (accessed 05.12.2016). (In Chin.)
29. *习近平:把我国从网络大国建设成为网络强国* [Xi Jinping: China must evolve from a large internet nation to a powerful internet nation]. Available at: http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm (accessed 05.12.2016). (In Chin.)
30. *国务院办公厅关于进一步加强互联网上网服务营业场所管理的通知* [The statement of the General Office of the State Council of China on further strengthening towards the enterprises which provide Internet services]. Available at: http://www.gov.cn/zhengce/content/2016-09/30/content_5114029.htm (accessed 05.12.2016). (In Chin.)
31. 方滨兴, 杜阿宁, 张熙, 王忠儒. 国家网络空间安全国际战略研究 [Fang Binxing, Du Aning, Zhang Xi, Wang Zhongru. Research on the international strategy for national cyberspace security]. *中国工程科学*, no. 6, 2016, pp. 13—16. (In Chin.)
32. *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* [The central network security and information leading group was established: from the network power to the network power]. Available at: http://news.xinhuanet.com/politics/ 2014-02/27/c_119538719.htm (accessed 02.05.2017). (In Chin.)
33. 王桂芳. 大国网络竞争与中国网络安全战略选择 [Cyber competition between Big powers and China's cyber security strategic choice]. *国际安全研究*, 2017, no. 2, pp. 27—46. (In Chin.)