Дата публикации: 16 августа 2020
DOI: 10.5281/zenodo.3911320

Исторические науки

СТРАТЕГИЯ КИТАЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОЛИТИЧЕСКИЙ И ТЕХНИЧЕСКИЙ АСПЕКТЫ

Чекменёва Татьяна Геннадьевна[1], Ершов Богдан Анатольевич[2], Трубицын Сергей Дмитриевич[3], Остапенко Александр Алексеевич[4]

[1]Кандидат политических наук, доцент, Воронежский государственный технический университет, ул. 20-летия Октября, 84, Воронеж, Россия, E-mail: politehist@mail.ru
[2]Доктор исторических наук, профессор, Академик РАЕ, Воронежский государственный технический университет, ул. 20-летия Октября, 84, Воронеж, Россия, E-mail: bogdan.ershov@yandex.ru
[3]Бакалавр, Воронежский государственный технический университет, ул. 20-летия Октября, 84, Воронеж, Россия, E-mail: k-medov@mail.ru
[4]Бакалавр, Воронежский государственный технический университет, ул. 20-летия Октября, 84, Воронеж, Россия, E-mail: k-medov@mail.ru

Аннотация

Возрастающая роль информационных технологий ставит перед современным государством новые вызовы, к которым относятся попытки иностранных агентов вести кибершпионаж против государственных структур, компаний и граждан, а также стремление противоборствующей стороны подорвать важную информационную инфраструктуру. Актуальность данной темы обусловлена возрастающей активностью Китайской Народной Республики в мировом информационном пространстве, а также действиями китайских государственных служб по обеспечению внутренней информационной безопасности и организации кибератак на информационную инфраструктуру.

Цель данной статьи - дать оценку проводимого Китаем курса по обеспечению информационной безопасности, а также выявить тенденции в восприятии угроз национальной безопасности в информационной сфере у представителей китайской политической элиты. В связи с этим, 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 отделов, отвечающих за кибербезопасность, в двух последних органах копирует соответствующую структуру в вооружённых силах страны.

Особое место в обеспечении киберпространства КНР отводится Центральной ведущей группе по кибербезопасности и информатизации. К основным аспектам защиты от информационных и социальных угроз относятся: "Золотой щит", кибер-коэффициент благонадежности и государственный интернет-троллинг. В исследовании рассматривается не только политический аспект вопроса, но и его техническая часть.

Ключевые слова: Китай, информационные технологии, информационная безопасность, «Золотой щит», кибер-коэффициент благонадежности, социальный кредит, интернет-троллинг, деструктивный контент.

I. ВВЕДЕНИЕ

Глобальное сетевое противоборство обусловило необходимость всестороннего и систематического исследования информационного пространства. Однако, наряду с чисто научным интересом, возникла необходимость в его государственном регулировании. Наиболее благоприятная для этого социальная почва сложилась в Китае, где удалось получить весьма впечатляющие результаты контроля над населением через масштабную фильтрацию контента, оценку благонадежности граждан и даже троллинг. Опыт Китая по обеспечению информационной безопасности, это прежде всего способы защиты сознания населения от деструктивного контента, которые во многом могут представлять интерес для России [1;2;3;4].

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.

II. МЕТОДОЛОГИЯ

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.

Сфера кибербезопасности попала в поле зрения китайских властей во второй половине 1990-х гг. Одним из стимулов развития законодательства в этой области послужило создание в 1999 году системы электронного государственного управления (Government Online Project, GOP) и появление необходимости адекватного правового регулирования. Так, в 2000 году были приняты руководящие принципы для системы электронного государственного управления (Guidelines of National Electronic Government Construction, NEGC).

В нормативно-правовом аспекте обеспечения информационной безопасности 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». 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. Предусматривалось 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. 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. 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.

В 2011 году положения о кибербезопасности были внесены в национальное уголовное законодательство КНР, а в 2013 году — в Закон о защите прав и интересов потребителей.

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. 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 блога. 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. 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: 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 технологий 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+“». Согласно этому документу, в индустриальном секторе будут внедряться современные и передовые технологии, предполагается применение возможностей Интернета в производстве, 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.

III. ОБСУЖДЕНИЕ

Проблематике обеспечения национальной безопасности в киберпространстве КНР посвящены работы американских исследователей Джона Линдсэй, Даниэля Вентре. 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 Чинь Лима проследить возможности сотрудничества КНР и США в киберпространстве. Среди китайских исследований необходимо выделить работы Фан Бинь Сина и Ван Гуйфана, которые придерживаются 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 [5, с. 158]. В России данная тематика представлена такими авторами, как Г. Ибрагимова [6], Г. Юрченко [7], К. Антипов [8], А. Булавин [9], Н. Кошурникова [10], в исследованиях которых даётся общая характеристика системы информационной безопасности Китая.

Первоначально термин «информационная безопасность» использовался для обозначения проблем, порождаемых компьютерными сетями. Впоследствии он приобрел более широкий смысл [11, с. 188]. Западный подход сводит вопросы информационной безопасности к техническим проблемам контроля и соблюдения законности в телекоммуникационной сфере.

Исследователи и дипломаты России и стран Азии придерживаются расширенного подхода, разделяя информационную безопасность в соответствии с видами угроз на информационно-техническую (кибербезопасность) и информационно-социальную.

До начала 1990-х гг. в нашей стране практически не существовало ясной государственной позиции по проблеме обеспечения информационной безопасности, что, собственно, и привело к поражению в Холодной войне. Только в сентябре 2000 года Президентом РФ была подписана Доктрина информационной безопасности России. В отличие от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания.

В мировом экспертном сообществе нет единства и в вопросе об определении термина «информационная война», под которым в целом понимается стратегическое противоборство в информационном пространстве в форме информационно-разведывательной, электронной, хакерской, кибернетической, экономической и психологической войны [12].

Как отмечает С.Н. Гриняев, первоначально термин «информационная война» использовал Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью как в военное, так и в мирное время [13]. В связи с появлением новых задач после окончания «холодной войны» термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий [14]. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Американские эксперты выделяют два типа стратегических информационных войн — первого и второго поколения. Война первого поколения (кибервойна) понимается как комплексное воздействие на систему государственного и военного управления противника с одновременным обеспечением защиты собственной информационной инфраструктуры. Инструментом ведения такой войны является кибероружие — совокупность новейших ИКТ и средств, которые позволяют получить несанкционированный доступ к информации и целенаправленно ее видоизменять. Информационная война второго поколения - это манипулирование общественным сознанием и дестабилизация отношений между политическими движениями с целью провокации; подрыв международного авторитета государства-оппонента; нанесение ущерба его жизненно важным интересам в различных сферах. Основным ее инструментарием являются национальные и транснациональные средства массовой информации, а также глобальные информационно-коммуникационные сети. С их помощью можно влиять на мировоззрение, политические взгляды и ценностные установки отдельной личности и общества в целом

В августе 1995 года Национальный Институт Обороны США публикует работу Мартина Либики «Что такое информационная война?»., в которой автор определил семь форм информационной войны: командно-управленческая, разведывательная, психологическая, хакерская, экономическая, электронная и, наконец, кибервойна.

Командно-управленческая - в современном значении нацелена на каналы связи между командованием и исполнителями. Перерезая "шею" (каналы связи) нападающий изолирует «голову» от «туловища». Утверждается, что это лучше, нежели просто убивать «голову». Кстати, Интернет был основан, как оборонный вариант этой войны («рассредоточенная шея»).

Разведовательная война - сбор важной в военном отношении информации (как нападение) и защита собственной.

Электронная война - направлена против средств электронных коммуникаций - радиосвязи, радаров, компьютерных сетей. Ее важный раздел - криптография. Шифровка-расшифровка электронной информации. Психологическая война - пропаганда, промывание мозгов, информационная обработка населения. Либики делит ее на четыре составляющие - подрыв гражданского духа, деморализация вооруженных сил, дезориентация командования и несколько неожиданное звено в этой последовательности - война культур.

Хакерская война - порождение информационной эры. Подразумевает диверсионные действия против гражданских объектов противника и защиту от них (действия против военных расцениваются как электронная война - здесь классификация Либики выглядит расплывчато). От хакеров Либики ожидает следующих действий: тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, хищение информации, хищение услуг (в смысле несанкционированных подключений к сетям), тайный мониторинг сетей, несанкционированный доступ к закрытым данным с целью шантажа. Оружие хакеров по Либики - вирусы, «троянские кони», «логические бомбы», сниферы («нюхалки», «следилки»). Либики считает хакеров серьезной угрозой для США, поскольку Америка - наиболее «сетевая» страна.

Либики отделил кибер-войну от «обычного» хакерства. Поскольку терроризм есть война против отдельных людей, то информационный терроризм означает захват компьютерных данных, позволяющих выследить цель (либо шантажировать ее).

Отличие семантической атаки от хакерства Либики видит в том, что хакер грубо говоря заставляет систему работать неправильно. При семантической атаке компьютерная система работает совершенно правильно, но решения которые она выдает - неверны. Семантическая атака направлена на «органы чувств» компьютерной системы, контролирующей какой-либо процесс с помощью датчиков. Обмануть эти датчики или другие средства ввода значит вывести систему из строя, не нарушив в ней ничего.

Симуляционная война - замена реального поля боя на его компьютерную модель. Таким образом, летчики не поднимаются в воздух, а «воюют» во флай-симуляторах, руководители решают вопросы между собой в стратегической игре.. Либики видит в этом прежде всего демонстрационный эффект, аналогичный схватке двух воинов, предшествовавшей древним битвам.

Последний пункт классификации Либики - война имени Уильяма Гибсона (автора Нейромансера). Подразумевает воплощение оператора в кибернетическое существо, обитающее внутри системы...

Предельная стадия кибервойны, уничтожающая само понятие инфовойны, путем распространения его на любую войну (а также на любой другой акт реального мира), поскольку сама «реальность» (как компьютерная, так и физическая) может быть представлена как информационный поток.

За последнее десятилетие Китайская Народная Республика стала реальным и самым опасным экономическим и геополитическим конкурентом США, претендующим на мировое господство. Поэтому достаточно предсказуемо, но со значительным опозданием, США развязали в отношении Китая информационную войну, рассчитывая без военного вторжения развалить противника изнутри. Однако тотальный мониторинг и управление рисками информационного пространства, заблаговременно внедренные китайским правительством, во многом охладили надежды американцев. Разумеется, использованные Поднебесной в этом отношении технологии заслуживают всестороннего изучения.

Таким образом, руководство Китая, несмотря на столь стремительные социально-технологические изменения, происходящие в современном мире, надеется сохранить в рамках Поднебесной исторически сложившуюся философскую парадигму конфуцианства [16; 17]. Консервация соответствующих ей устоев и традиций, по мнению китайских идеологов, обеспечит стабильность общества и высокие темпы развития экономики. Однако для этого необходимо исключить эрозию мировоззрения китайцев со стороны информационного пространства Запада. А это может быть обеспечено только с помощью жесткой изоляции от западных вбросов, для чего создаются и внедряются соответствующие технологии фильтрации контента.

История развития и философская парадигма «гигантского муравейника» в Китае богата масштабными воплощениями. Достаточно вспомнить такой продукт, как Великая Китайская стена, которая видна даже с космической орбиты. Гигантомания, свойственная китайцам, нашла свое воплощение и в информационном пространстве в виде проекта «Золотой щит». Фактически это уже вторая великая стена, возведенная в Китае, только теперь она защищает уже не от орд кочевников, а от нашествия западных контент-вредоносов. Поэтому ее по праву можно называть Великая Китайская информационная стена, которая также как и первая стена, решает задачу изоляции, но не физической, а информационной.

Реальный практический интерес представляет анализ китайского проекта «Золотой щит», как пример национальной Интернет-фильтрации. С помощью него власти КНР осуществляют контроль за своим населением и защищают свое информационное пространство от проникновения деструктивного контента извне.

Предпосылки для создания «Великого китайского файрвола» возникли уже в 1994 году, когда в КНР впервые ввели ответственность за посягательства на компьютерную безопасность, которая была установлена Постановлением Государственного Совета Китайской Народной Республики от 18 февраля 1994 года «О компьютерной безопасности информационных систем» [18].

В 1998 году началась разработка «Золотого щита». В 2003 году он начал использоваться на территории страны и уже к 2006 году охватил почти 100% Интернет-пространства Китая, на его разработку ушло 800 миллионов долларов [19]. В 2000 году проект впервые получил огласку во время торговой выставки в Пекине. Грэг Уолтон из Международного центра по правам человека и демократическому развитию на выставке SecurityChina 2000, на которой собрались более 300 компаний из 16 стран мира, описал «Золотой щит» как инструмент, который направлен на внедрение передовых информационных и коммуникационных технологий в целях укрепления контроля за населением, а также для снижения преступности и предупреждения различных преступлений [20].

«Золотой щит» на первом этапе своей работы представлял многоуровневую систему баз данных. С помощью нее в течение первых лет эксплуатации проекта Департамент общественной безопасности упорядочил информацию о большей части жителей Китая. Одна из подсистем «Золотого щита» в последствии получила название «Великий файрвол». Она отвечала и продолжает отвечать за фильтрацию сетевого контента в соответствии с законодательством страны [21].

На первый взгляд может показаться, что «Золотой щит» – это просто технология поиска и блокировки нежелательных Интернет-ресурсов, но на самом деле это более совершенный фильтр. «Золотой щит» имеет три составляющие, на которых он базируется, – это технологии: DeepPacketInspection (DPI), Connectionprobe и Supportvectormachines (SVM).

DPI – технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. Коренное отличие от уже всем привычных файрволов в том, что DPI анализирует не столько заголовки пакетов, сколько зарывается в содержимое транзитного трафика на уровнях модели OSI со второго и выше. Всё это делается в режиме реального времени и с точки зрения внешнего наблюдателя никаких задержек или манипуляций с трафиком практически не заметно. DPI потребляет очень много ресурсов, так как все многочисленные операции, производимые им (например, дефрагментация пакетов, их распаковка, распознавание типов данных и протоколов, сканирование содержимого, многочисленные эвристики и многое-многое другое), должны происходить в режиме реального времени.

Поэтому главный критерий степени серьёзности DPI, это глубина анализа транзитного трафика, который может позволить себе эта система, чтобы при этом сохранять приемлемый уровень латентности. Даже если технические возможности и ресурсы позволяют трассировать код до бесконечности, погружаясь во всё новые ветвления и процедуры, общие требования к латентности системы всегда имеют волне конкретные ограничения, поэтому глубина погружения всегда ограничена. Часто в этой ситуации применяются технологические или оптимизирующие ноу-хау, но можно пойти

иначе – просто многократно увеличить вычислительную мощность.

Говоря о китайском DPI, нужно понимать, что это именно второе решение – это датацентр размером с самый настоящий районный центр, который применяет SwarmIntelligence (роевой интеллект) для управления балансировкой и обработкой данных между его бесчисленными частями-узлами [22].

Многие мировые провайдеры применяют его для контроля и балансировки своего трафика. Мобильные операторы с его помощью собирают подробную статистику для каждого отдельного пользователя. Также эта технология даёт возможность адаптивно управлять скоростью передачи отдельных пакетов (QoS) и многое другое. В целом, DPI обеспечивает огромное количество уникальных возможностей в широком спектре, от высококачественного шейпинга до создания продвинутых шпионских систем типа PRISM (ProgramforRobotics, IntelligentsSensingandMechatronics) – государственная программа США, которая включает в себя комплекс мероприятий, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи, принятая американским Агентством национальной безопасности в 2007 году.

Connectionprobe – это дальнейшая эволюция DPI – сращивание прокси-сервера и низкоуровневого фильтрующего механизма. В этом случае при попытке подключения к любому сервису за пределами национального сетевого шлюза сначала происходит «заморозка» такого запроса с последующим опережающим подключением по целевому адресу уже от имени DPI. Это, так сказать, проактивная система тестирования и идентификации типа запрашиваемых во внешнем «Интернете» сервисов.

SVM (метод опорных векторов) – это интеллектуальная насадка на DPI. Особым свойством метода опорных векторов является непрерывное уменьшение эмпирической ошибки классификации и увеличение зазора, поэтому метод также известен как метод классификатора с максимальным зазором. Вспомним, что DPI – это фильтрующая машина, вычленяющая некие данные в потоке согласно статическим правилам или сигнатурам. В противоположность к этому SVM даёт возможность сканировать Интернет-поток на основе статистического анализа без жесткого набора правил. Например, проводить анализ частоты определённых символов, длин пакетов, анализа подозрительной активности с заданных адресов, замечать различные диспропорции и сетевые аномалии, выявляя скрытые закономерности. Алгоритмы естественно засекречены и об их содержании остается только догадываться, но уже сейчас достоверно можно утверждать, что фильтрация контентов становится всё более интеллектуальной.

«Золотой щит» является эффективным инструментом борьбы с терроризмом и кибертерроризмом. Под кибертерроризмом понимается использование сети Интернет, как средства и способа совершения «теракта», а также вербовка новых членов в террористическую организацию или организация связи между существующими группами [23]. Благодаря развитой системе распознавания контекста сообщений и оперативной работе служащих, занимающихся работой с шифрами, а также благодаря фильтрации всего Интернет-трафика для выявления подозрительного контента, удалось выслеживать террористические ячейки раньше, чем они начинают действовать. Конечно, полной безопасности данная система не обеспечивает, но по сравнению с другими странами азиатского региона, такими как Филиппины и Индонезия, Китай более стабилен и число террористических актов в стране заметно меньше. После событий 11 сентября 2001 года Китай, как и многие другие страны, ужесточил антитеррористическое законодательство. В результате были изменены некоторые существующие пункты уголовного кодекса КНР, а также добавлены новые. Теперь признавалось преступным распространение средств совершения теракта и финансирование преступных организаций.

Вместе с тем в контексте обеспечения региональной безопасности ужесточилось отношение к сепаратистам Уйгурского района и Тибета.

К ним широко стали применять термин «террористы», в частности, террористической организацией признано «Исламское движение Восточного Туркменистана», требующая создания исламского государства и обращения всех жителей Китая в ислам.

«Великий китайский файрвол» наглядно показывал, как закрытый «Интернет» способствует внутренней стабилизации и государственной безопасности. Системы Интернет-слежения помогают

правоохранителям вычислять злоумышленников, а китайские суды – жестоко карают любого, кто посмеет посягнуть на безопасность КНР и ее граждан.

Все это доказывает, что исполнительный аппарат обеспечения безопасности сети «Интернет» достаточно успешно проводит работу по контролю информационного обмена и пресечению незаконной деятельности в китайском сегменте сети.

Менталитет китайца прежде всего заточен на служение родине, жесткое повиновение вышестоящим и осуждение инакомыслящих. Поэтому информационная изоляция от деструктивных внешних воздействий непротестно воспринимается большинством населения Китая, а проект «Золотой щит» если и вызывал нарекания, то только на Западе. При этом главным выгодополучателем от внедрения «Золотого щита» является не столько простой житель Китая, сколько его правительство, которое ввело не только инструмент защиты, но и инструмент контроля. С 2017 года на территории Китая отсутствует анонимость в Интернет-пространстве, поэтому все пользователи должны указывать свои настоящие имена [24], что упрощает правительству Китая наблюдение за поисковыми запросами жителей Китая.

При этом в Интернет-пространстве находятся различные неофициальные сообщения про обход данной системы. Во-первых, в Гонконге и Макао имеются свободные зоны, т.е. «Золотой щит» не распространяет свое влияние в этих городах. Во-вторых, по словам наших соотечественников, которые проживают на территории КНР, те, кому нужны такие сети как Facebook, YouTube, Instagram, Google, просто скачивают бесплатные приложения для использования VPN, но некоторые для большей вероятности покупают платные VPN. За VPN у лидеров рынка стандартная цена – 60 долларов за полгода [25]. Пути обхода «Золотого щита» китайцы будут изыскивать и далее, ибо этого требует психология личности, нуждающейся в полноценном информационном обмене.

Функционал информационной изоляции реализуется не только за счет «Золотого щита». В Китае запрещены и не функционируют такие социальные сети как Facebook, Twitter др. Их замещение осуществлено китайскими аналогами, которые в полной мере соответствуют принятой национальной парадигме и обеспечивают доминирование конфуцианской философии и исторически сложившихся народных традиций.

Исторически сложившаяся в Китае и активно поддерживаемая его руководством модель «гигантского муравейника» объективно требует поддержания соответствующей дисциплины в обществе. Причем, чем крупнее система, тем жестче должен быть режим контроля за ее элементами. В этом контексте гиперразмерность китайского общества требует едва ли не тотального отслеживания функционирования каждого «муравья». Даже с учетом традиционной дисциплинированности китайцев столь масштабный контроль в принципе не возможен без его автоматизации.

Развернувшееся сегодня глобальное информационное противоборство отчетливо выставило перед этой гиперразмерной нацией угрозы обеспечения управляемости миллиардным населением. В этой связи в июне 2014 года Правительством КНР был опубликован план реализации системы социального кредита, внедрение которой было аргументировано необходимостью поддержания и распространения идеи культуры искренности и повышения честного менталитета во всех сферах государства и общества, а также существенного повышения уровня рыночной и социальной удовлетворенности. Система должна быть полностью внедрена к 2020 году и хоть на данный момент она функционирует не в полную силу, но уже можно многое о ней сказать.

Несмотря на то, что внедрение системы социального кредита в стране правительством было аргументировано необходимостью поддержания и распространения идеи культуры искренности и повышения уровня честности в государственной и общественной жизни, рассмотрение реализации проекта дает понять, что истинная цель его внедрения совсем иная – автоматизация давно существовавшей в КНР системы dang'an, то есть системы публичных записей, в которых собрана вся информация о населении КНР. Личные дела граждан содержат такую информацию, как: фотография, физические характеристики и др., также дела содержат оценки со стороны руководителей и сверстников, отчеты об успеваемости в учебных заведениях, любые отметки о правонарушениях, факты членства в клубах/обществах и т.д., dang'an также использовалась, как средство оценки граждан при приеме на

работу.

Чтобы посмотреть, как система социального кредита влияет на целое общество, достаточно переместиться на запад КНР в Сыньцзян-Уйгурский. Автономный район, населенный преимущественно уйгурами после начала действия системы социального кредита стал центром проведения партией репрессивной политики в отношении населения. С началом действия системы социального кредита в регионе количество арестованных выросло в три раза, а расходы региона на внутреннюю безопасность стремительно выросли. Задержанных власти держали в центрах предварительного заключения, тюрьмах, а также в лагерях политически-трудового образования. Властями были выделены огромные средства на постройку в регионе контрольно-пропускных пунктов, полицейских участков, исправительных учреждений. Для составления базы данных населения в регионе, полицией вызывались в участки граждане, лица которых сканировались специальными системами распознавания внешности [26]. Также под предлогом проведения бесплатного медицинского осмотра у населения брали образцы ДНК, а позже процедура сдачи образцов ДНК и вовсе стала обязательной для получения паспорта. Власти пытаются оправдать жестокое обращение необходимостью поддержания стабильности и безопасности в Синьцзяне и «наносить удары» по тем, кого считают террористами и экстремистами. Синьцзянские чиновники утверждают, что корень этих проблем – «проблемные идеи» тюркских мусульман, которые власти описывают как экстремальные религиозные догмы.

В целях обеспечения региональной безопасности жители мятежной провинции обязаны устанавливать в телефоны приложения, отслеживающие все перемещения и контакты. Видеонаблюдение с элементами искусственного интеллекта умеет распознавать их подозрительные передвижения и встречи. Полицейские оснащены VR-очками, распознающими лица, а также устройствами, с помощью которых полицейский легко определяет в смартфоне гражданина запрещенный контент, при наличии которого обладатель телефона может попасть в исправительный лагерь. Все это признаки наличия тотального информационного контроля на основе выявления деструктивного контента и подозрительных, с точки зрения власти, действий.

Для управления населением используются следующие технические методики: устранение анонимности, персонификация граждан, оценка поведения граждан, фильтрация информационного потока и цензура. В частности, анонимность в Интернет-пространстве КНР была объявлена вне закона ещё в 2017 году. По вступившим в силу правилам пользования сетью Интернет все её пользователи обязаны верифицировать свои реальные имена. Это правило позволяет властям без лишних поисков определять авторов всех постов и публикаций во всей сети Интернет в КНР, а также собирать информацию о действиях граждан. Невозможность остаться анонимным при выражении своего мнения существенно, однако не полностью, отбивает желание у населения КНР открыто говорить о ситуации в стране. Вне Интернет-пространства анонимность граждан устраняется путем повсеместного использования технологий распознавания биометрических данных.

Оценка населения КНР производится на основе анализа собранных о нем данных, после обработки которых повышается или понижается коэффициент благонадежности субъекта оценки. Значение коэффициента благонадежности определяет уровень привилегированности субъекта в глазах правительства и объем получаемых субъектом поощрений в случае высокого значения коэффициента благонадежности и наказаний в обратном случае. Поощрение является способом воздействия на объект управления, т.е. на население, для побуждения к проявлению дальнейших успехов [27]. Наказание же запугивает население и также побуждает к совершению «хороших» действий. Устранение анонимности в реальной жизни выполняется благодаря высокотехнологичным устройствам распознавания индивидуальных физических данных граждан. Реализуется это благодаря масштабной сети камер видеофиксации, которых в городах КНР уже установлено около двухсот миллионов. К 2020/2021 году власти собираются увеличить эту цифру втрое. Но упор будет сделан не только на количественное изменение, сами камеры претерпят серьезные технические улучшения. На сегодняшний день камеры способны распознавать лица, сканировать все тело тех, кто попадает в их поле зрения. Сеть камер видеонаблюдения уже показала свою эффективность: в сентябре 2017 года полиция с помощью камер на пивном фестивале арестовала 25 человек, находящихся в розыске. Но не только стационарные уличные камеры используют систему распознавания лиц: данная технология используется в

общественных туалетах Пекина - для исключения кражи, камеры с системой распознавания лиц контролируют выдачу бумажных полотенец и бумаги, а китайская полиция снабжена смарт-очками, оборудованными камерой и имеющими связь с базой данных правоохранительных органов, с помощью очков полицейский, находящийся на расстоянии не более 5 метров от субъекта проверки личности, сможет получить данные о совпадении с внешностью субъекта в базе данных за 2-3 минуты.

В интернет-пространстве анонимность устраняется благодаря тотальному контролю партии за сетью интернет. Интернет-провайдеров обязали верифицировать реальные персональные данные пользователей (имя, фамилия, адрес проживания и т.д.) [28]. Продумано было и использование виртуальных частных сетей (VPN), которые могут использоваться пользователями для сокрытия своего IP-адреса: на законодательном уровне гражданам КНР было запрещено использование VPN. Ежедневно огромные объемы информации различных видов: видеозаписи, аудиозаписи, геометки, посты в социальных сетях, чеки из онлайн-магазинов, попадают в систему хранения данных BigData, где сортируются и готовятся к анализу специальным алгоритмом. Результат работы алгоритма подскажет правительству ответы на те вопросы о субъекте анализа, на которые сам субъект не знает ответ. Поступки, влияющие на изменение значения коэффициента благонадежности, можно разделить на 3 группы учета: государственный учет, общественный учет, онлайн-учет. В категорию государственного учета попадают такие действия граждан как оплата подоходного налога, погашение кредитов, оплата счетов за коммунальные услуги, выплаты по постановлению суда. Общественный учет включает в себя соблюдение правил дорожного движения, соблюдение норм рождаемости, оплата проезда на общественном транспорте, общественная деятельность и т.д. Онлайн-учет включает в себя покупательские привычки субъекта, надежность и достоверность информации, публикуемой в сети интернет, взаимодействия с онлайн-пользователями [29].

В 2020 году система «социального кредита», уже апробированная в ряде провинций КНР, будет внедрена по всей стране. При этом повсеместно установят до полумиллиарда видеокамер. У каждого гражданина появится рейтинг с кредитами в тысячу баллов. По данным видеонаблюдения и другим зафиксированным фактам о личности эта цифра будет автоматически меняться со временем. Появятся несколько категорий граждан. Одни своей законопослушностью и лояльностью власти нарастят кредитные баллы и получат приоритеты в государственном обслуживании. Другие, незначительно потерявшие баллы, оставят за собой права на скидки по коммунальному и банковскому обслуживанию. Существенно растратившие кредитные баллы китайцы попадут под подозрение и не смогут работать в государственных и муниципальных органах. Потерявшие треть баллов граждане будут ограничены в правах на получение работы, кредита, билетов на транспорт и т.п. Общение с такими изгоями чревата для граждан высших категорий стремительным падением их рейтинга.

Именно с введением в эксплуатацию системы социального кредита, благодаря вычислительным мощностям составляющих, которые обеспечивают ее функционирование, стало возможно оценивать граждан в балльной системе и ввести систему поощрений и наказаний, как физически осязаемую интерпретацию баллов. В финансовом плане правительство поощряет граждан с высоким уровнем социального кредита следующими способами: скидки на оплату тарифов ЖКХ, меньшие процентные ставки в банках. Тех же граждан, которые обладают низким уровням социального кредита в качестве наказания от правительства ждет следующее: запрет на работу в управленческой и банковской сфере, отстранение от поступления в высшие учебные заведения и высшие школы, публичное порицание, ограничение перемещения по территории Китая на высокоскоростных поездах и самолетах.

Наработки КНР по тотальному мониторингу информационного пространства оказались самоокупаемыми. По просочившимся в прессу данным продукты, обеспечивающие слежку за гражданами, оказались востребованными в Венесуэле, Зимбабве, Монголии, Малайзии, Эквадоре, Сингапуре, Анголе, Эфиопии, Перу, Лаосе, Мьянме, Бразилии, Боливии, Уганде. Фактически подконтрольные правительству Китая фирмы продают информационные технологии управления населением страны. Характерно заметить, что покупателями в данном случае являются режимы, испытывающие внешнее давление и (или) необходимость оперативного демпфирования внутренней социальной напряженности. Собственно, и сам Китай пошел на столь жесткие информационные меры под угрозой западной экспансии, грозящей развалом страны изнутри.

Таким образом, руководство КНР весьма основательно подготовилось к решающей схватке со своим главным геополитическим конкурентом – США, которые во многом потеряли надежду на выигрыш информационной войны с Китаем и обостряют сейчас экономическое противоборства с ним. Философия конфуцианства, исторически нашедшая широчайшее распространение в китайском обществе, очевидно, значительно способствует внедрению в провинциях КНР системы социального кредита (контроля).

Согласно учению Конфуция веками китайцы неутомимо и ответственно трудились прежде всего на благо государства. Их трудоспособность и сплоченность в этом вопросе вызывает удивление даже у азиатов. Честь отчизны и ее руководства они готовы массово отстаивать и в информационном пространстве. Не случайно самая крупная армия троллей, работающая в интересах государства, функционирует именно в Китае.

Итернет-троллинг как психологический и социальный феномен зародился в 1990-х годах. Феноменом троллей в последнее время интересуются все больше специалистов. Большинство из них считают, что профессиональные тролли могут совершить настоящую революцию в социальных сетях и на тематических площадках, которая позже может вылиться в народные акции протестов в реальном мире. В результате троллинг, как информационная технология влияния на сознание Интернет-пользователей, был взят на вооружение стратегами гибридной войны, как активный элемент пропаганды и контрпропаганды в области внутренней и внешней политики государств, а также экономической борьбы за рынки сбыта [30].

С начала XXI века Интернет-тролли стали образовывать собственные сетевые сообщества и организации, делясь опытом по наиболее эффективному разжиганию конфликтов. Сейчас любой популярный форум, новостная группа и кики-проект рано или поздно сталкивается с троллями и троллингом. Как это ни парадоксально, иногда обсуждение проблемы троллинга перерастает в собственно троллинг, или оно им изначально и являлось благодаря усилиям троллей [31]. Информационные риски Интернет-троллинга, особенно возросли при его реализации «Фабриками и армиями троллей» [32].

Способов и видов «троллинга» довольно много, но стоит обратить внимание на самые популярные из них:

1. Самый примитивный вид - это распространение неверной информации, вредоносных ссылок и слухов.

2. Варианты для развлечений могут включать изменение своего пола на сайтах знакомств, выдача себя за иностранца или знаменитость.

3. Одним из самых жестоких проявлений троллинга считается доведение до нервного срыва человека с неустойчивой психикой.

4. Политический троллинг стоит отдельным видом, он используется как для разжигания конфликтов, так и для привлечения внимания избирателей к нужной проблеме. Он может использоваться с целью диагностики необходимой группы или реакции личности. Суть его сводится к заявлению провокационного утверждения и эскалации конфликта на последние острые политические события. Точно так же, вызываются споры о политике и вкусах, причем это обычно касается тех тем, где априори не может быть однозначного мнения.

5. Групповой троллинг существенно отличается от личного. Тут действует группа людей, имеющих одну общую цель. Чаще всего в подобных сообществах разработаны собственные правила достижения целей, имеется определенный язык. Такие компании включают либо специалистов пиара и политики, либо самостоятельно заинтересованных людей (например, команда по онлайн - игре, таким образом, может рассорить своих конкурентов) [33].

В Китае существование армии проправительственных блогеров, известной под названием Умаодан или «Партия 50 центов», в Китае ни для кого не секрет, ибо невозможно тайно нанять до двух миллионов человек. Шесть лет назад издание GlobalTimes даже опубликовало одобрительную статью, в которой рассказало, что ячейка партии в городе Чанша еще в 2004 году платила команде комментаторов по 600

юаней в месяц, плюс половина юаня за каждый новый пост.

Именно отсюда якобы и происходит странное название организации. С тех пор оплата труда марионеток, готовых хвалить работу партии в сети Интернет, стала столь же обычной статьей расходов для местных органов власти в Китае, как и зарплата для инспекторов дорожного движения. Недавнее исследование Гарвардского университета показало, что китайские власти размещают 448 млн. фальшивых комментариев в интернете каждый год. Проанализировав 43,8 тыс. провластных комментариев, исследователи пришли к выводу, что 99,3% из них были сделаны государственными служащими различных ведомств. Как правило, такие комментарии появлялись разом и помногу в особенно напряженные моменты, например, во время протестов или партийных собраний. Интересно отметить, что некоторые из таких комментариев подходят под определение троллинга (в самом строгом смысле этого слова). Вместо того, чтобы напрямую атаковать своих противников, государственные тролли забивают скептиков потоком флуда или умело отвлекают разговор. Численность этой армии троллей: от 300 тыс. до 2 миллионов человек, где многие на неполной занятости [34].

Вышеизложенное позволяет рассматривать Интернет-троллинг как эффективное информационное оружие, которое активно используется и другими развитыми странами. Фактически государственный троллинг – это средство активного влияния на общественное мнение через травлю политических оппонентов в социо-информационном пространстве. Подобная деятельность органично дополняет фильтрацию контентов и кибер-слежку за гражданами в ходе информационного противоборства.

История Китая и философия Конфуцианства сформировали ментальность, для которой сейчас нисколько не зазорно за пол юаня написать пост в поддержку власти или в осуждение ее оппонентов.

IV. РЕЗУЛЬТАТЫ

Бурное развитие новых ИКТ расширяет поле деятельности средств массовой информации и коммуникации. Китай не является исключением. Китайские власти видят в Интернете и современных ИКТ не только средство сдерживания государств-оппонентов, но и большие возможности для формирования позитивного имиджа страны на международной арене. При Информационном агентстве Государственного совета КНР было создано специальное Административное бюро по пропаганде в Интернете, направляющее и координирующее государственную пропаганду в Сети. Большинство существовавших в стране печатных и электронных СМИ не имели собственных сайтов в Интернете и не были представлены широкой аудитории. Ситуация начала меняться в начале прошлого десятилетия, когда Госсовет КНР осознал, что Интернет — это действенный инструмент реализации конкретных политических и социальных программ. Началось широкое инвестирование не только в масс-медиа на китайском языке, но и в расширение китайских иноязычных СМИ.

Интернет дает беспрецедентную возможность открытого доступа к информации и позволяет диссидентским организациям легко 282 Секция 2 • История, экономика, международные отношения распространять свои идеи. Поэтому правительство КНР активно противодействует подобным негативным последствиям с помощью создания эффективной сетевой цензуры.

В Китае используется две стратегии в осуществлении веб-цензуры: фильтрация запросов и контента и поощрение самоцензуры, что во внешнем Китаю мире получило название «Великая китайская веб-стена». В число сайтов, подвергающихся цензуре, входит большинство западных СМИ, социальные сети и блоги.

В последние годы КНР переходит от оборонительной к наступательной стратегии применения ИКТ в отношении внешнеполитических оппонентов. В 2003 г. Центральный военный совет и Компартия Китая ввели «концепцию трех войн», включающую в себя психологическую войну, медиавойну и правовую войну. В концепции говорится о необходимости опережающих действий в киберпространстве и нанесении Китаем такого рода удара первым. Важным уровнем присутствия Китая в глобальном информационном пространстве является стремительно развивающаяся развлекательная индустрия:

СМИ, шоу-бизнес, компьютерные игры, реклама.

Растущее значение в Китае придается экспорту культурной продукции за рубеж. Кроме того, продвижение китайской культуры и языка осуществляется посредством распространения образовательных школ и классов. Так, в 2010 г. в 96 странах мира действовало 322 института и 369 классов Конфуция.

V. ЗАКЛЮЧЕНИЕ

1. Через фильтр «Золотой щит» КНР удалось обеспечить значительную изоляцию информационного пространства страны от внешнего проникновения нежелательного (по мнению правительства) контента. Эта мера позволила оградить общество КНР от многих негативов Запада (цветные революции, терроризм и др.) и тем самым обеспечить его монолитность в условиях противодействия многочисленным угрозам со стороны США. Однако государственный заказ на критерии селекции скорее будет отвечать запросам правящей элиты, чем потребностям широких слоев населения Китая. Просчет в таком вопросе чреват стратегическими последствиями для развития нации, так как фильтрация контента касается всех китайцев одновременно и действия эти сугубо ограничительные, которые с точки зрения психологии личности (тем более в информации) вызывают внутренний протест у человека, даже если он относится к столь покорной нации, которая проживает в Поднебесной. В этом случае «гигантский муравейник» превращается в кипящий котел без клапана с высокими рисками социального взрыва. При этом жесткие информационные ограничения (особенно, в пользовании столь популярными сейчас глобальными социальными сетями) отгораживает Китай от мировой цивилизации, нарушая сообщения, столь необходимые для обмена достижениями и роста. Обвинения в несанкционированном заимствовании идей и технологий в отношении Китая отнюдь не беспочвенны, но достигать вершин прогресса таким способом становится все труднее, поэтому придется организовывать полноценную диффузию контента даже с риском проникновения его деструктивных разновидностей в информационное пространство Китая. Конечно, свои первичные задачи «Золотой щит» во многом уже выполнил, так как в период мировой экспансии «цветных революций» он обеспечил стабилизацию общества, сохранение его в традициях конфуцианства, однако завещанные Конфуцием китайцам стремление к просветлению вряд ли будет исполняться в круговой информационной обороне. Поэтому в стратегической перспективе «Золотой щит» должен быть значительно более прозрачным, а Китай станет более информационно-интегрированным в мировое сообщество, перед которым сегодня встали такие цивилизационные вызовы, которые усилиями одной страны (даже такой многочисленной, как Китай) преодолеть не предоставляется возможным.

2. Глобальная цифровизация жизнедеятельности граждан развитых стран естественно открывает сетевым администраторам широчайшие возможности для контроля над своими пользователями. Мультисетевое хозяйство современных мегаполисов позволяет организовать едва ли не тотальное отслеживание своих жителей на улице, работе, в доме, банке, торгово-развлекательных комплексах и других объектах. Интеграция таких сетей с технологиями больших данных дает возможность концентрировать и анализировать сведения почти о каждом человеке, попавшем в поле зрения вышеуказанной информационной паутины.

Применение средств искусственного интеллекта усиливает тотальность наблюдения. Ярким примером тому может служить китайская система социального кредита, благозвучное название которой фактически не скрывает сущности реализуемого ей функционала, позволяющего наладить цифровое слежение практически за каждым жителем КНР. Подобное ограничение свобод населения в некоторой степени оправдано для КНР. Вызовы, с которыми приходится сталкиваться этому государству, весьма масштабны. Жесткая геополитическая конкуренция с США при гигантском и довольно разношерстном населении Поднебесной вынуждают правительство КНР прибегать к радикальным средствам защиты своего суверенитета. Поэтому контроль над населением будет тотальным, что, собственно, и обеспечивает система социального кредита.

Вряд ли это будет способствовать творческому развитию личности, так как поведенческая скованность в условиях тотального наблюдения явно не благоприятствует полету мысли. При всей традиционной склонности китайцев к повиновению власти, нагрузка вышеупомянутой системы на психику личности сохраняется постоянно. Этот психологический груз «неусыпного ока» объективно давит на каждого жителя, порождая в нем страхи и внутренний протест. Подобные глубинные процессы нередко находят выход в различных проявлениях агрессии и нигилизма. Группой риска для таковых действий можно считать низкорейтинговую категорию людей. Выставляя баллы и категории гражданам, система не столько объединяет, сколько разобщает китайцев. В случае образования критической массы изгоев вполне возможны социальные протесты. Поэтому сбалансированная (по интересам личности и общества) критериальная основа рейтинговых оценок системы очень важна, ибо перегибы в ходе реализации системы могут обойтись очень дорого с точки зрения обеспечения национальной безопасности. Внешне кажущийся абсолютным монолитом китайский социум может в одночасье разлететься на осколки, если масштабно сработает механизм отчуждения личности от государственных институтов, подавляющих ее свободу, в том числе, через цифровое неусыпное наблюдение.

3. Сегодня троллинг превратился в индустрию межгосударственного информационного противоборства в сети «Интернет». Победить троллинг можно только значительно повысив интеллектуальный и духовно-нравственный потенциал нации, образованность ее молодого поколения. Базовым препятствием в ликвидации троллинга, как и многих других негативов сети Интернет, следует считать высокую степень ее анонимности. Банальная блокировка уже не дает желаемых результатов в такой тонкой материи как информационное противоборство. Поэтому атакующим троллям следует противопоставлять современный арсенал контрмер и средств, адаптированных к специфике регионального менталитета.

СПИСОК ЛИТЕРАТУРЫ

Абудусаламу Н., Ершов Б.А. Китай во Второй мировой войне В сборнике: Ратные страницы истории Великой Отечественной войны (к 70-летию Победы советского народа в Великой Отечественной войне) Труды Международной конференции. 2015. С. 121-124.

Аль Ш. А. А., Чекменёва Т.Г. Политика СССР в отношении войны в Персидском заливе в 90-е гг. XX в. // Войны и революции в новейшей истории России Труды Международной научной конференции. Воронеж: ВГТУ, 2017. С. 36-41.

Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. - 2013. - № 6. - С. 39—54.

Ашмаров И.А. Электронная коммерция в Китае как источник роста страны // Вестник Воронежского института экономики и социального управления. 2019. № 1. С. 21-27.

Бондарева Т.А., Чекменёва Т.Г. Информационные войны в эпоху глобализации // Россия и мир на новом этапе глобальной конкуренции: материалы Международной научно-практической студенческой конференции. Воронеж: ВГТУ, 2013. С. 101-106.

Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика и право. 2014. № 1. С. 27—314.

Великий брандмауэр Китая: история проекта «Золотой щит // URL: https://www.molodostivivat.ru/mnenie/velikij-brandmauer-kitaya-istoriya-proekta-zolotoj-shhit.html

Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива // URL: https://www.liveinternet.ru/users/2483533/post98061428/

Дремлюга Р.И. Интернет как способ и средство совершения преступления // Информационное право. - 2008. - №4. - С. 27-31.

Ершов Б.А. Семейные основы жизни священнослужителей в губерниях Центрального Черноземья в XIX веке Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2011. № 2-2 (8). С. 68-71.

Ершов Б.А., Онищенко Л.С. Национальный вопрос в странах Западной Европы Проблемы социальных и гуманитарных наук. 2018. № 2 (15). С. 30-38.

Запад официально признал создание армии Интернет - троллей // [Электронный ресурс] - URL: http: //www.politonline.ru/ interview/ 22880294.html

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

Как работают армии троллей по всему миру // [Электронный ресурс]-URL: https://ru.ihodl.com/analytics/2016-11-13/kak-rabotayut-armii-trollej-po-vsemu-miru/

Кошурникова Н.А. Особенности информационной политики современного Китая // Китай: история и современность: материалы IX Международной научно-практической конференции. Ответственный редактор С. В. Смирнов. - Екатеринбург: Издательство: Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, 2016. - 279-284.

Краткая история ИБ в Китае: как возводили Великий китайский файрвол // URL: http://orion-int.ru/kratkaya-istoriya-ib-v-kitae-kak-vozvodili-velikij-kitajskij-fajrvol/

Панарин И.Н. Информационная война и мир / И.Н. Панарин, Л.Г. Панарина.- М: ОЛМА-ПРЕСС, 2003. - 366 с.

Понятие и виды методов государственного управления // BzBook. [Электронный ресурс] – URL: https://bzbook.ru/Administrativnoe-33pravo-1.109.html

Попов И.М. Война будущего: взгляд из-за океана. – М.: Издательский дом: "АСТ-Астрель", 2004. – 444 с.

Почему в Китае запрещены VPN-сервисы // VPNmentor. [Электронный ресурс] – URL: https://ru.vpnmentor.com/blog/почему-в-китае-запрещены-vpn-сервисы/

Прибытков А.А., Чекменёва Т.Г. О взглядах выдающегося мыслителя Конфуция на государственное устройство / // Россия и Китай: история и перспективы сотрудничества: Материалы IV международной научно-практической конференции. Благовещенск-Хэйхэ-Харбин: Благовещенский государственный педагогический университет, 2014. С. 274 - 278.

Разумов Е. А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. № 4 (98). – 156 – 170.

Романова Е.В., Перевозчикова Л.С., Ершов Б.А. The lifestyle of the human being in the information society В книге: 3rd International Conference on Advances in Education and Social Sciences Proceedings of ADVED 2017. 2017. С. 950-954.

Сеть через прицел DPI: анатомия китайского Интернета // URL: http://blogerator.org/page/dpi-anatomija-kitajskogo-interneta-cenzura-filtracija

Суянг Ш., Ершов Б.А. Китайский фронт во время Второй мировой войны В сборнике: Ратные страницы истории Великой Отечественной войны (к 70-летию Победы советского народа в Великой Отечественной войне) Труды Международной конференции. 2015. С. 124-128.

Троллинг в интернете, что это такое, причины и виды // [Электронный ресурс] - URL: https://psihomed.com/trolling/

Трубицын С.Д., Остапенко А.А., Чекменёва Т.Г. Особенности информационной политики и способы обеспечения информационной безопасности Китая: исторический и философский аспекты // Проблемы социальных и гуманитарных наук. - 2020. - Выпуск № 1 (22). С. 222 – 234.

Цензура в Китае: Золотой щит, или «Великий китайский файрвол // URL: https://enterchina.ru/blog/cenzura-v-kitae-zolotoy-schit-ili-velikiy-kitayskiy-fayrvol/

Цифровая диктатура: как в Китае вводят систему социального рейтинга // РБК. [Электронный ресурс]–URL: https://www.rbc.ru/business/11/12/2016/584953bb9a79477c8a7c08a7

Чекменёва Т.Г. Проблемы обеспечения информационной безопасности студенческой молодежи в образовательном процессе: опыт Воронежской области // Философия и культура информационного общества: Тезисы докладов. СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2018. С. 271 – 274.

Чекменёва Т.Г., Прибытков А.А. Историческая память и национально-гражданская идентичность россиян как объекты информационно-психологических атак // Информационные войны как борьба геополитических противников, цивилизаций и различных этосов: Сборник Сборник трудов Всероссийской научной конференции /Под ред. В.Ш. Сабирова. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2018. - С. 734-750.

Чекменёва Т.Г., Прибытков А.А. Проблемы обеспечения информационной безопасности молодежи в современной России: психологический аспект // Психологическое благополучие современного человека: Материалы Международной заочной научно-практической конференции. Екатеринбург, Уральский государственный педагогический университет, Отв. ред. С. А. Водяха. 2018. С. 121-128.

Чекменёва Т.Г., Прибытков А.А. Россия в сфере информационного противоборства: проблемы и перспективы // Конфликты в современном мире: международное, государственное и межличностное измерение: Материалы V Международной научной конференции. Саратов: Издательство "Перо", 2016. - С. 218-223.

Что такое троллинг в Интернете и для каких целей его применяют? // [Электронный ресурс] - URL: https://livesurf.ru/zhurnal/5525-troll-chto-yeto-za-zver-i-kak-s-nim-borotsya.html/

Шерман А. Информационный войны (кибер-войны) // URL: https://gazeta.lenta.ru/dossier/06-08-1999_infowar.htm

CHINA'S INFORMATION SECURITY STRATEGY: POLITICAL AND TECHNICAL ASPECTS

Chekmeneva, Tatyana Gennadievna[1], Ershov, Bogdan Anatolyevich[2], Trubitsyn, Sergey Dmitrievich[3], Ostapenko, Alexander Alekseevich[4]

[1]Candidate of Political Sciences, Associate Professor, Voronezh State Technical University, 20 years of October street, 84, Voronezh, Russia, E-mail: politehist@mail.ru

[2]Doctor of historical sciences, professor, Academician of RAE, Voronezh State Technical University, 20 years of October street, 84, Voronezh, Russia, E-mail: bogdan.ershov@yandex.ru

[3]Bachelor, Voronezh State Technical University, 20 years of October street, 84, Voronezh, Russia, E-mail: k-medov@mail.ru

[4]Bachelor, Voronezh State Technical University, 20 years of October street, 84, Voronezh, Russia, E-mail: k-medov@mail.ru

Abstract

The growing role of information technology poses new challenges for the modern state, which include attempts by foreign agents to conduct cyber espionage against government agencies, companies and citizens, as well as the desire of the warring party to undermine important information infrastructure. The relevance of this topic is due to the increasing activity of the People's Republic of China in the global information space, as well as the actions of Chinese government services to ensure internal information security and the organization of cyber attacks on the information infrastructure.

The purpose of this article is to assess the course pursued by China on ensuring information security, as well as to identify trends in the perception of threats to national security in the information sphere among representatives of the Chinese political elite. In this regard, the structures in the state apparatus of China that are in charge of this area are considered. Despite the noticeable actions of the representatives of the “fifth generation” of the leaders of the PRC in the aspect of cybersecurity, a single organization has not been formed in the state structure that would be responsible for developing a political course in the information sphere. In addition to the Central Military Council, the Communist Party of China and the State Council of the PRC are engaged in this. At the same time, the structure of the departments responsible for cybersecurity in the last two bodies copies the corresponding structure in the country's armed forces.

A special place in ensuring China's cyberspace is given to the Central Leading Group on Cybersecurity and Informatization. The main aspects of protection against information and social threats include: The Golden Shield, the cyber security factor, and state Internet trolling. The study considers not only the political aspect of the issue, but also its technical part.

Keywords: China, information technology, information security, the Golden Shield, cyber security factor, social credit, Internet trolling, destructive content.

REFERENCE LIST

Al Sh. A. A., Chekmenyova T. G. (2017) Soviet Policy towards the Gulf war in the 90-ies of XX century War and revolution in the modern history of Russia. *Proceedings of International scientific conference. Voronezh: VSTU.* Pp. 36-41. (in Russ.).

Antipov K. (2013) Cyber conflict in Sino-American relations and the search for dialogue. Problems of the Far East. № 6. Pp. 39-54. (in Russ.).

Ashmarov I.A. (2019). Electronic commerce in China as a source of country growth. Bulletin of the Voronezh Institute of Economics and Social Management. No 1. Pp. 21-27. (In Russ.)

Bondareva T. A., Chekmenyova T. G. (2013) Information wars in the era of globalization. Russia and the world at a new stage of global competition: proceedings of the International scientific and practical student conference. Voronezh: VSTU,. Pp. 101-106. (in Russ.).

Brief history of is in China: how the Great Chinese firewall was built [Electronic resource] URL: http://orion-int.ru/kratkaya-istoriya-ib-v-kitae-kak-vozvodili-velikij-kitajskij-fajrvol/ (in Russ.).

Bulavin A.V. (2014) About the approaches of the USA and China to ensuring cybersecurity. Society: politics, Economics and law. № 1. Pp. 27-314. (in Russ.).

Chekmenyova T. G. (2018) Problems of ensuring information security of students in the educational process: experience of the Voronezh region. Philosophy and culture of information society: Thesis of reports. SPb.: Saint Petersburg state University of aerospace instrumentation. Pp. 271-274. (in Russ.).

Chekmenyova T. G., Pribytkov A. A. (2016) Russia in the sphere of information warfare: problems and prospects // Conflicts in the modern world: international, state and interpersonal dimension: Materials of the V International scientific conference. Saratov: Pero Publishing House. Pp. 218-223. (in Russ.).

Chekmenyova T. G., Pribytkov A. A. (2018) Historical memory and national-civil identity of Russians as objects of information and psychological attacks. Information wars as the struggle of geopolitical opponents, civilizations and various ethos: a Collection Of proceedings of the all-Russian scientific conference / ed. Novosibirsk: Siberian state University of telecommunications and Informatics, Pp. 734-750. (in Russ.).

Chekmenyova T. G., Pribytkov A. A. (2018) Problems of ensuring information security of youth in modern Russia: psychological aspect. Psychological well-being of modern man: Materials of the International correspondence scientific and practical conference. Yekaterinburg, Ural state pedagogical University, Ed. Pp. 121-128. (in Russ.).

Dremlyuga R. I. (2008) Internet as a method and means of committing a crime. Information law. № 4. Pp. 27-31. (in Russ.).

Grinyaev S. N. Information war: history, present day and perspective. [Electronic resource] URL: https://www.liveinternet.ru/users/2483533/post98061428/ (in Russ.).

Abdusalam N., Ershov B. A. (2015) China in the second world war. In the collection: Military pages of the history of the great Patriotic war (to the 70th anniversary of the Victory of the Soviet people in the great Patriotic war) *Proceedings of the International conference.* Pp. 121-124. (in Russ.).

Sang S., Ershov B. A. (2015) Chinese front during the Second world war. In the collection: Military pages of the history of the great Patriotic war (to the 70th anniversary of the Victory of the Soviet people in the great Patriotic war). *Proceedings of the International conference.* Pp. 124-128. (in Russ.).

Ershov B.A. (2011) Family foundations of the life of clergy in the provinces of the Central Chernozem region in the XIX century. *Historical, philosophical, political and legal Sciences, cultural studies and art history. Questions of theory and practice. 2011. № 2-2 (8).* Pp. 68-71. (in Russ.).

Ershov B. A., Onishchenko L. S. (2018) National question in the countries of Western Europe. *Problems of social and humanitarian Sciences. №. 2 (15).* Pp. 30-38. (in Russ.).

Romanova E. V., Perevozchikova L. S., Ershov B. A. (2017) Human Lifestyle in the information society In *the book: 3rd international conference on educational achievements and social Sciences Proceedings of Adved* Pp. 950-954. (in Engl).

How Troll armies work around the world [Electronic resource] URL: https://ru.ihodl.com/analytics/2016-11-13/kak-rabotayut-armii-trollej-po-vsemu-miru /(in Russ.).

Ibragimova G. (2013) China's strategy in cyberspace: issues of Internet governance and information security // Index of safety. № 1 (104). Pp. 169-184. (in Russ.).

Internet Trolling, what it is, causes and types [Electronic resource] URL: https://psihomed.com/trolling/ (in Russ.).

Koshurnikova N. A. (2016) Features of information policy of modern China. China: history and modernity: proceedings of the IX International scientific and practical conference. Responsible editor S. V. Smirnov. - Yekaterinburg: Publishing house: Ural Federal University named after the first President of Russia B. N. Yeltsin. Pp. 279-284. (in Russ.).

Li P. (2010) Order of the People's Republic of China on the Protection of Computer Information System Security Chinese Law&government, vol. 43, iss. 5, pp. 12-16.

Network through the DPI sight: anatomy of the Chinese Internet [Electronic resource] URL: http://blogerator.org/page/dpi-anatomija-kitajskogo-interneta-cenzura-filtracija (in Russ.).

Panarin I. N., Panarina L. G. (2003) Information war and peace. Moscow: OLMA-PRESS. 366 p. (in Russ.).

Popov I. M. (2004) War of the future: a view from across the ocean. Moscow: Publishing house: "AST-Astrel". 444 p. (in Russ.).

Pribytkov A. A., Chekmenyova T. G. (2014) On the views of the outstanding thinker Confucius on the state structure Russia and China: history and prospects of cooperation: Materials of the IV international scientific and practical conference. Blagoveshchensk-Heihe-Harbin: Blagoveshchensk state pedagogical University. Pp. 274-278. (in Russ.).

Razumov E. A. (2017) China's cybersecurity Policy. Russia and the Asia-Pacific region. № 4 (98). Pp. 156 – 170. (in Russ.).

Sherman A. Information wars (cyber wars). [Electronic resource] URL: https://gazeta.lenta.ru/dossier/06-08-1999_infowar.htm (in Russ.).

The Great firewall of China: the history of the Golden shield project [Electronic resource] URL: https://www.molodostivivat.ru/mnenie/velikij-brandmauer-kitaya-istoriya-proekta-zolotoj-shhit.html (in Russ.).

The West has officially recognized the creation of an army of Internet trolls [Electronic resource] - URL: http: //www.politonline.ru/ interview/ 22880294.html (in Russ.).

Trubitsyn S. D., Ostapenko A. A., Chekmenyova T. G. (2020) Features of information policy and ways to ensure information security in China: historical and philosophical aspects. Problems of social and humanitarian Sciences. Issue № 1 (22). Pp. 222 – 234. (in Russ.).

What is Internet trolling and for what purposes is it used? [Electronic resource] URL: https://livesurf.ru/zhurnal/5525-troll-chto-yeto-za-zver-i-kak-s-nim-borotsya.html/ (in Russ.).

Yurchenko G. China's Capabilities for conducting computer network operations and cyber espionage BELVPO.COM: information portal "Military-political review". [Electronic resource] URL: http://www.belvpo.com/9984.htm (in Russ.).