

# Введение

Коммуникация — есть важнейшее свойство живой природы. В ней особое место занимает человек, как единственный вид, способный говорить сквозь время (созвучно религиозным учениям о бессмертии души). Наскальная живопись, дошедшая до нас через тысячелетия, яркий пример того, как художественные символы выступают в качестве послания потомкам. Однако качественный скачок произошел у людей позднее, с появлением языка и письменности (их трансляторами сквозь время выступала церковь). Именно тогда тексты стали первыми средствами вирусной коммуникации, способной заражать сознание людей новыми идеями. Неслучайно Киплинг считал слова самым сильным наркотиком, который изобрело человечество. Понятные и общепризнанные символы, образующие слова, обеспечили широкое распространение идей и доминирование человека как вида среди живых существ. Границы человеческого общения революционно расширились с появлением гаджетов, порожденных симбиозом бинарного языка и цифровой электроники. Благодаря им мы сегодня имеем глобальную коммуникацию, в основе которой лежит словесная конструкция — контент, создающий новую реальность. Видимо именно поэтому возник соблазн контролировать ее, основанный на чрезвычайном любопытстве человека и его значительной зависимости от содержания получаемых контентов. Однако главное достоинство коммуникации заключается не в возможности контролировать реальность, а в способности обрести человеческому виду вечность (за счет генерации и передачи потомкам инновационных знаний и культурно-нравственных ценностей, снижающих риски реализации надвигающихся планетарных вызовов и гарантирующих сохранение и развитие вида).

В этом контексте злоумышленниками следует считать создателей контента, побуждающего личность к деструктивным действиям. Такой (деструктивный) контент оказывает разрушающее воздействие на человека, а глобальная коммуникация открывает злоумышленникам заманчивые перспективы управления массовым сознанием. Отсюда борьба с распространением

деструктивного контента приобретает особую значимость в настоящее время, т.к. он сеет хаос и не должен формировать будущее. Благородство и полезность миссии специалистов в области информационной безопасности, прежде всего, видится именно в этом.

Глобальность обозначенной проблемы требует учета ее геополитической составляющей. И дело здесь в том, что действующая стратегия национальной безопасности США, как лидера западной цивилизации, не оставляет надежд на миролюбивую внешнюю американскую политику в отношении России. С другой стороны, привлекательность для Запада российских природных ресурсов и затруднительность их захвата путем военной агрессии перемещает противоборство в информационное пространство с надеждой для западных глобалистов развалить Российскую Федерацию (РФ) через атаки на ее граждан деструктивным контентом, девальвирующим культурные ценности и традиции, нацеленным на нравственную деградацию и духовное обнищание населения, порождающим национальную и религиозную рознь в обществе. Как следствие, ареной этого ожесточенного противоборства сейчас стали столь популярные социальные сети [160].

Сила и риски России, вытекающие из ее многонациональности и культурного разнообразия, диктуют в ходе вышеупомянутого информационного противоборства необходимость учета регионального аспекта. Природные, этнические и религиозные различия субъектов РФ исторически сформировали весьма пеструю ментальность ее регионов, которая, несомненно, отразилась и на их пользователях интернет-пространства. Информационная модель такого пользователя может существенно розниться для территорий Российской Федерации (свыше 100 народностей, 11 часовых поясов и 8 климатических зон). Очевидным свидетельством этого следует считать региональные паблики. Десятки таких интернет-сообществ функционируют в каждом регионе России, где жители обсуждают темы, насущные для своей территории. Все это перемещает «битву контентов» в республики, края и области РФ. Федеральные обобщения в данном случае будут напоминать поиск «средней температуры по больнице». Поэтому именно модель регионального интернет-пользователя (РИП), отражающая его коммуникационные предпочтения в социальных сетях и сообществах, должна лежать в основе этой битвы, включая процедуры выявления деструктивных контентов, измерения их параметров и оценки

ареала распространения, оперативное противодействие. Уместно здесь отметить тот факт, что практикуемое при противоборстве блокирование источников деструктивных контентов и даже целых интернет-сервисов (Китай) в долгосрочной перспективе малоэффективно [160].

Напротив, сейчас остро необходим инструментарий, который оперативно (по возможности, в реальном масштабе времени) будет отслеживать контент-атаки. В виду обилия и изоциренности последних, осуществлять вышеизложенное только в ручном режиме далее не представляется возможным. Теперь эту процедуру придется автоматизировать, программным путем идентифицируя вредоносы и оценивая их опасность в региональном интернет-пространстве. При этом исключительно организационно-правовое реагирование, глубокая модернизация дает значительное запаздывание в информационной борьбе. Здесь нужна оперативная контрпропаганда в интернет-сообществах (телевидения, которое мало смотрит молодежь, тут явно недостаточно), опирающаяся на предлагаемый риск-мониторинг и систематически актуализируемую модель РИП, в каждом субъекте РФ.

Изложенное выше дает основание утверждать, что проблема повышения защищенности пользователей в онлайн-социальных сетях при распространении в них деструктивных контентов представляется чрезвычайно актуальной, а связанные с этим вопросы создания соответствующего методического обеспечения, его алгоритмизации и программной реализации, включая комплексный риск-анализ наиболее популярных социальных сетей, имеют значительную не только научную, но и практическую ценность.

Указанной проблематике посвящена настоящая монография, авторы которой выражают благодарность Е.А. Шварцкопф, Е.С. Соколовой, Д.А. Савинову, Н.Г. Титову, Е.Н. Телегину, А.А. Гончарову, Д.А. Ишкову, В.В. Филатову, А.В. Ещенко, Ю.О. Гончарову, Е.А. Москалевой за помощь в подготовке рукописи к публикации.

# Мониторинг и управление рисками социоинформационного пространства в целях обеспечения региональной и национальной безопасности

## 1.1. МОТИВАЦИЯ ВВЕДЕНИЯ И РЕАЛИЗАЦИИ ИНФОРМАЦИОННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ОБЩЕСТВОМ

Глобализация представляет собой процесс, целью которого, по большому счету, является достижение мирового доминирования и даже господства отдельной группы государств, создателей финансовых, производственных, торговых и иных сетей мирового масштаба. Высочайшая концентрация ресурсов всего человечества в распоряжении нескольких финансово-промышленных групп открыла им перспективу надгосударственного управления через мультисетевое мироустройство.

Цель «глобальных сетевиков» состоит в том, чтобы через свою паутину превратить население планеты в совокупность потребителей сетевых товаров и услуг, заменив их естественные (этнические, религиозные и др.) связи на виртуальные контакты и обеспечив тем самым тотальный контроль и безусловное управление. Однако государственные институты являются препятствием на пути превращения социумов в глобальное стадо, понукаемое сетевыми модераторами, провайдерами и т.п. Наблюдается тенденция сокращения суверенитета и даже ликвидация государственности ряда наций. При этом встречается деление на «золотой миллиард» и прочих жителей планеты, как бы на «пастухов» и «чрезмерно расплодившееся стадо». Глобальные сети выступают как средство управления и эксплуатации,

включая наказание (санкции и пр.), и даже ликвидацию непокорных «сетевикам» государственных образований (под ложными предложениями защиты демократии и т.п.).

Таким образом, вырисовывается противоречие (пожалуй, самое острое и системное сегодня) между амбициями глобальных сетевиков и интересами суверенных государств или свободной личности. Это эпохальное противоречие современности обусловило нынешние геополитические потрясения (развал СССР, Ливии и др.), вызванные сетевыми конфликтами, разразившимися в финансовых, энергетических, информационных и иных сферах. Колоссальные ущербы, которые уже принесло данное противоборство, и нарастающие его масштабы позволяют рассматривать либеральный глобализм в качестве важнейшей угрозы современности (международный терроризм всего лишь его побочный продукт). Мы стали свидетелями широкомасштабного противостояния в социальных сетях. Непримируемая борьба идет вокруг сетей энергоносителей. Налицо все признаки глобальной сетевой войны. И это не конспирология, а реальность, порожденная вышеуказанным противоречием.

Этот всепоглощающий и антагонистический конфликт сулит в перспективе кардинальное изменение архитектуры мирового сообщества, включая многополярную кооперацию и балансировку сил, а также новейшую регламентацию взаимоотношений наций в условиях современных вызовов.

Таким образом, современное мультисетевое мироустройство представляется весьма несовершенным и неустойчивым. Открывая новые перспективы для глобальных сетевиков, оно порождает значительные риски для наций и человеческой личности. Особенно это касается системообразующего информационного пространства, в котором заложены широчайшие возможности контроля и управления не только гаджетами, но и общества в целом.

Через информационные сети управляются нефте- и газотранспортная инфраструктура, логистика перемещений, хранения и продажи товаров. Производственная инфраструктура, раскинутая по всей планете, также управляется с помощью корпоративных информационных сетей. Финансовые сети во многом перешли на электронные платежи. Многие услуги, оказываемые коммерческими и государственными структурами в различных странах, также переведены в сетевой формат.

Вышеизложенные факты и выводы обусловили необходимость всестороннего и систематического исследования социо-

информационного пространства [87; 99; 169]. Однако, наряду с чисто научным интересом, возникла необходимость в его государственном регулировании [75]. Наиболее благоприятная для этого социальная почва сложилась в Китае, где удалось получить весьма впечатляющие результаты контроля за населением через масштабную фильтрацию контента, оценку благонадежности граждан и даже троллинг [37; 117].

Исторически организационно-управленческая парадигма Китая сводилась к модели «гигантского муравейника». Именно эта модель помогала Поднебесной выстоять на протяжении тысячелетий. Во времена кризиса Китай нередко обращался к другим нациям, что оставило свой культурный след в сфере форм общественных связей и учений. Однако чем сильнее проявлялось влияние извне на традиционные ценности, тем более мощной оказывалась консолидация социальных масс на основе консервативных традиций китайской культуры и основ жизни [133]. Сегодняшняя стратегия развития Китая предусматривает модернизацию политики и духовности в соответствии с идеологией конфуцианства, в основе которого лежат правила поведения для каждого человека, как для личности, так и для гражданина великой державы. Конфуций считал первостепенной задачей воспитание человека в духовном плане. Учение конфуцианства строится на любви, уважении, гуманизме, благородном мышлении, где опорой служит уважение к старшим по положению и возрасту людям.

Конфуций в своем учении реализовывал культ предков. В древности в Китае в каждом доме находился алтарь предков, на котором были таблички с их именами. Понятие «предок» (*цзу*) первоначально записывалось как изображение кланового алтаря — скорее всего, небольшой каменной плиты, положенной горизонтально на каменную подставку. Позже оно стало изображаться в виде небольшой стелы с именем предка. Таким образом, изначально понятие «предок» ассоциировалось не собственно с умершим человеком, а со знаком его сакрального бытия, не зависящего от физического тела [134]. В трудные моменты жизни люди обращались к предкам, чтобы те подарили им свою мудрость и помогли в решении возникшей проблемы.

Китайское осмысление мира вообще корреляционно: человек осмысляет себя как некую точку схождения энергетических потоков от линий предков, т.е. коррелирует свое самосознание не столько с собственными достижениями, сколько с социально-родовыми связями [Там же].

В современном мире данное учение интерпретировано во внутривнутриполитических отношениях. Самым старшим по положению в Китае является власть — элемент, скрепляющий отношения простых жителей КНР. На основе модели «гигантского муравейника» можно предположить, что власть — это королева, которая скрепляет отношения «простых муравьев». Конфуцианство подразумевает не только уважение младших к старшим по возрасту и положению, но и заботу старших о младших. Этим и объясняется такое уважение к власти у жителей Китая. Благодаря такой идеологии правительство может свободно внедрять свои идеи в информационное пространство страны, защищая его от внедрения враждебных влияний извне, в особенности из США.

Еще одним неизменным положением конфуцианства является гуманность, подразумевающая наличие множества качеств: скромности, справедливости, сдержанности, достоинства, любви к людям. Все эти качества закладываются в человека путем воспитания. В современной интерпретации конфуцианства для правительства такие люди очень важны. Опасность представляют люди, не достигшие истинного просветления. Они своими действиями, согласно учению, могут направить себя на путь духовной деградации. Такие люди, не имея стабильного поведения, оказавшись на руководящей должности, могут привести подчиненных к моральному разложению, а также к банальному невыполнению приказов [134].

Психологическая составляющая системы управления населением следует из принятого правительством КНР вектора социалистической модернизации на основе теории социализма с китайской спецификой. На 4-м пленуме 18-й сессии ЦК Коммунистической партии Китая в 2014 г. в целях реализации социализма и управления государством в КНР был выбран правовой путь, который основывается на теории верховенства закона. Китайская специфика социалистической модернизации учитывает историю Китая, его народа, сохраняет создававшиеся тысячелетиями моральные ценности и основывается на таких учениях, как конфуцианство, даосизм и буддизм, основными принципами которых являются стремление к поддержанию порядка, стабильности и мира [214]. Постулат Конфуция о государстве, как об огромной семье, играл и играет важную роль в формировании единства населения КНР. Он подразумевает повиновение власти, необходимость поступаться своими личными интересами ради общих, т.е. государственных целей.

При этом надо понимать, что 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 социоинформационного пространства, заблаговременно внедренные китайским правительством, во многом охладил пыл американцев. Разумеется, использованные Поднебесной в этом отношении технологии заслуживают всестороннего изучения.

В связи с вышесказанным, реальный практический интерес представляет анализ китайского проекта «Золотой щит», как пример национальной интернет-фильтрации. С помощью него власти КНР осуществляют контроль над населением и защищают свое информационное пространство от проникновения деструктивного контента извне [37].

В 1998 г. началась разработка проекта «Золотой щит». В 2003 г. он начал использоваться на территории страны и уже к 2006 г. охватил почти 100% интернет-пространства Китая. На его разработку ушло 800 миллионов долларов [227]. В 2000 г. проект впервые получил огласку во время торговой выставки в Пекине. На выставке Security China 2000, собравшей более 300 компаний из 16 стран мира, Грэг Уолтон из Международного центра по правам человека и демократическому развитию, описал «Золотой щит» как инструмент, направленный на внедрение передовых информационных и коммуникационных технологий в целях укрепления контроля за населением, а также для снижения преступности и предупреждения различных преступлений [92].

«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 отвечает за фильтрацию сетевого контента в соответствии с законодательством страны [128].

На первый взгляд может показаться, что «Золотой щит» является обычной технологией поиска и блокировки нежелательных интернет-ресурсов, но на самом деле это более совершенный фильтр. «Золотой щит» включает три базовые составляющие.



Это технологии Deep Packet Inspection (DPI), Connectionprobe и Supportvectormachines (SVM) [184], алгоритмы которых засекречены и об их содержании остается только догадываться, но уже сейчас достоверно можно утверждать, что фильтрация контентов становится все 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 [108]. Благодаря развитой системе распознавания контекста сообщений и оперативной работе служащих, занимающихся работой с шифрами, а также фильтрации всего интернет-трафика для выявления подозрительного контента, удалось выслеживать террористические ячейки раньше, чем они начинали действовать. Конечно, полной безопасности данная система не обеспечивает, но по сравнению с другими странами азиатского региона, такими как Филиппины и Индонезия [42], Китай более стабилен и число террористических актов в стране заметно меньше. После событий 11 сентября 2001 г. Китай, как и многие другие страны [Там же], ужесточил анти-террористическое законодательство. В результате были изменены некоторые существующие пункты уголовного кодекса КНР, а также добавлены новые, например, признание 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», требующее создания исламского государства и обращения всех жителей Китая в ислам [20].

Менталитет китайца, прежде всего, заточен на служение родине, жесткое повиновение вышестоящим и осуждение инакомыслящих. Поэтому информационная изоляция от деструктивных внешних воздействий воспринимается большинством населения Китая непротестно, а проект «Золотой щит» если и вызывал нарекания, то только на Западе. Однако что бы и кто по этому поводу не говорил, данный фильтр уже второе десятилетие надежно защищает информационное пространство страны от всяческой скверны. 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 г. на территории страны отсутствует анонимность в интернет-пространстве, поэтому все пользователи должны указывать свои настоящие имена [91], что упрощает правительству Китая наблюдение за их поисковыми запросами.

При этом в интернет-пространстве находятся различные неофициальные сообщения об обходе данной системы. Во-первых, в Гонконге и Макао имеются свободные зоны, т.е. «Золотой щит» не распространяет свое влияние на эти регионы. 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. На VPN у лидеров рынка стандартная цена — 60 долларов за полгода [5].

Пути обхода «Золотого щита» китайцы будут изыскивать и далее, ибо этого требует психология личности, нуждающейся в полноценном информационном обмене.

## **1.2. ФАКТЫ ИНФОРМАЦИОННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ОБЩЕСТВОМ**

Развернувшееся сегодня глобальное информационное противоборство отчетливо выставило перед этой гиперразмерной нацией угрозы обеспечения управляемости миллиардным населением. В этой связи в июне 2014 г. Правительством КНР был опубликован план реализации системы социального кредита, внедрение которой 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 [62]. Система должна быть полностью внедрена в 2020 г. И хотя на данный момент она функционирует не в полную силу, но уже можно многое о ней сказать. Так в источниках [28; 30; 126] отражены методы контроля интернет-пространства правительством КНР, в [8] рассмотрены участники реализации системы, в источниках [2; 3; 19; 21] описаны составные части системы социального кредита.

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, т.е. системы публичных записей, в которых собрана вся информация о населении КНР. Личные дела граждан содержат следующую информацию: фотография, физические характеристики и др., характеристики, даваемые руководителями и сверстниками, отчеты об успеваемости в учебных заведениях, любые отметки о правонарушениях, факты членства в клубах/обществах и т.п. Dang'an также использовалась, как средство оценки граждан при приеме на работу [54].

Чтобы посмотреть, как система социального кредита влияет в целом на общество, достаточно переместиться на запад КНР в Синьцзян-Уйгурский автономный район, населенный преимущественно уйгурами. После начала действия системы социального кредита этот район стал центром проведения партией репрессивной политики в отношении населения. С началом действия системы социального кредита количество арестованных в регионе выросло в три раза, а расходы на внутреннюю безопасность стремительно выросли [1; 23].

Для составления базы данных населения, полицией вызывались граждане, лица которых сканировались специальными системами распознавания внешности [8]. Также под предлогом проведения бесплатного медицинского осмотра у населения брали образцы ДНК, а позже эта процедура и вовсе стала обязательной для получения паспорта [22]. Синьцзянские чиновники утверждают, что корень зла — «проблемные идеи» тюркских мусульман, которые власти считают экстремальными религиозными догмами [1].

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