УДК 341.1/8
DOI 10.52452/19931778_2022_1_108

МЕЖДУНАРОДНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ

Е.В. Саунина, И.Д. Бажина

Нижегородский государственный университет им. Н.И. Лобачевского, Н. Новгород

saounina@mail.ru

Поступила в редакцию 30.12.2021

Сформулирована дефиниция и определены две формы информационного терроризма. Проанализирован международный опыт правового регулирования информационного терроризма на примере Китайской Народной Республики и Соединенных Штатов Америки. Обоснован вывод, что КНР был разработан правовой подход, который затрагивает влияние СМИ и технологические проблемы. США придерживаются «либеральной модели», ориентирующейся на наименьшее участие государства в процессе использования информационного пространства.

Ключевые слова: терроризм, информационный терроризм, виды информационного терроризма, международно-правовое противодействие терроризму, Китайская Народная Республика, Соединенные Штаты Америки.

Информационный терроризм известен мировому сообществу еще с XX века, но до настоящего времени нет определенности в представлении его основных признаков и сущности как на доктринальном уровне, так и в законодательстве. Однако в постоянно меняющихся условиях жизни мировое сообщество нуждается в нормативном регулировании информационной сферы, включая защиту информационного пространства. Несанкционированные вмешательства в различные управленческие и контрольные системы, направленные на разрушение, повреждение или полное отключение государственной критической инфраструктуры, могут повлечь за собой последствия, сопоставимые с поджогами или взрывами на физическом уровне. Отсутствие правового регулирования информационного терроризма в международных нормативных документах, а также активное использование террористическими организациями информационного пространства и предопределили актуальность и выбор темы научного исследования.

Анализ научных трудов свидетельствует о различных подходах к проблематике информационного терроризма, что обусловлено его сложной природой.

На наш взгляд, кибертерроризм и психологический терроризм являются видами информационного терроризма, и широкая трактовка этого явления дает возможность охватить весь спектр деятельности террористов в информационном пространстве.

Таким образом, информационный терроризм – это устрашающая население идеологически обоснованная практика воздействия, которая имеет своей целью принятие решения или совершение действия (бездействия) различных субъектов власти в пределах информационного пространства.

Мы соглашаемся с мнениями ряда авторов о том, что разграничение видов является наилучшим методом для подробного исследования. В зависимости от средств воздействия и объектов этого воздействия считаем необходимым выделить информационно-психологический терроризм и информационно-технологический его вид, представляющие повышенную общественную опасность для всего мирового сообщества, которая выражается в легком и анонимном доступе в информационное пространство, характеризуется постоянным расширением ее сферы и ее низкой нормативной защищенностью, чем и обусловлено дальнейшее изучение заявленной темы и рассмотрение различного законодательства стран и способов их борьбы с этим явлением.

Развитые системы мер противодействия информационному терроризму в Китайской Народной Республике и США мы считаем интересными объектами исследования.

Нормативно-правовое обеспечение противодействия информационному терроризму в Китайской Народной Республике

Китайские власти с появлением современных технологий в информационном пространстве проявляли постоянный интерес к его регу-

лированию. До 2015 г. правовой системе КНР было свойственно превалирование подзаконных актов над основными законами, многие из которых не были в открытом доступе как для иностранцев, так и для китайских граждан.

Необходимость мониторинга и регулирования отношений в области информации была обозначена в Постановлении Всекитайского собрания народных представителей от 28 декабря 2000 г. «Об обеспечении безопасности сети Интернет» [1]. Главным исполняющим органом в области информационного пространства является Китайское общество пользователей Интернета, основанное в 2001 году. Общество за 21 год своей работы разработало множество нормативно-правовых документов (например, Правила самодисциплины о запрете на распространение запрещенной информации, Конвенция о бойкотировании вредоносных программ и так далее).

Следующим этапом регулирования информационной сферы стало принятие Государственной стратегии развития информатизации на 2006–2020 годы, где были прописаны основные направления информационных и коммуникативных технологий (далее – ИКТ) [2]. Обеспечением технического функционирования цифровых технологий занимается Министерство промышленности и информатизации, образованное в 2008 году, а регулированием ИКТ в сфере кинематографии, телевидения и радиовещания – Государственное управление, в компетенцию которого также входит блокировка запрещенного контента (New York Times, CNN, Twitter, Facebook, Gmail) [3, с. 86].

Законодателем КНР был разработан особый правовой подход, который затрагивает регулирование как национальных и зарубежных СМИ, так и технологические проблемы, то есть нормативному регулированию подвергается как информационно-психологический, так и информационно-технологический терроризм. «Зеленая дамба» (Green Damba) и «Золотой щит» (The Golden Shield Project) являются примерами цифровых технологий, осуществляющих мониторинг и фильтрацию информации в кибернетическом пространстве [4, с. 141–142].

«Золотой щит» – это единственная мировая система, способная контролировать более четырех миллионов интернет-сайтов, более одного миллиарда пользователей мобильных телефонов в социальных сетях, более тридцати миллиардов сообщений каждый день. «Великий китайский файрвол» использует несколько способов мониторинга: блокирование адресов – URL и IP и соединения VPN, производит фильтрацию DNS-запросов, а также их переадресацию. «Зеленая дамба» – программный комплекс, носящий добровольный характер для клиента и работающий как средство защиты, например, от запрещенного контента для несовершеннолетних. В начале 2010 года китайское правительство хотело провести реформу по установке этой программы для всех персональных компьютеров, однако это вызвало массовые волнения среди правозащитных организаций и компьютерных сборщиков, и проект заморозили. В настоящее время это программное обеспечение установлено во всех общественных местах КНР [5, с. 202].

Китай проводит такую же политику в отношении блогов и различных социальных сетей. Так, блог-хостингам запрещается предоставлять услуги оставившим недостоверные и неполные данные, регистрироваться под псевдонимами, как и оставлять анонимные комментарии в блогосфере [6, с. 927].

Несмотря на существующие технические и правовые меры контроля социальных сетей, китайские граждане находят методы, чтобы обойти их. Во-первых, в Макао и Гонконге есть свободные зоны от «Золотого щита». Во-вторых, для входа Twitter, YouTube, Instagram, Google или Facebook используются различные ресурсы и прокси-серверы, которые позволяют обходить цензуру, покупая бесплатные приложения или для полной уверенности платные. В-третьих, пользователи, обсуждая социально-политические вопросы, используют каламбуры, омонимы, аббревиатуры на английском языке. Так как многие способы общеизвестны, то и цензура может их учитывать, но удалить все комментарии и информацию невозможно. В условиях стремительного развития информационных технологий китайцы постоянно будут изыскивать «трещины в золотой китайской интернет-стене».

Нормативно-законодательная база КНР в сфере информационной безопасности постоянно развивается. Так, основной Закон КНР «О противодействии терроризму» 2015 года включает статьи об организационных и правовых принципах борьбы с терроризмом, международном сотрудничестве Китая с другими государствами, а также положения, запрещающие средствам массовой информации предоставлять подробную информацию о террористических акциях и транслировать «негуманные и жестокие сцены» [7].

Следующим этапом нормативного закрепления мер информационной безопасности в КНР стал закон «О государственной безопасности» от 1 июля 2015 года, в котором предусмотрена возможность государственной системы обеспечения защиты объектов инфраструктуры, данных и важнейших систем [8].

Законодатель КНР не остановился на обозначении направлений работы в сфере безопасности – 7 ноября 2016 года принимается закон «О кибербезопасности», закрепляющий основополагающие понятия: сеть, операторы сети, сетевые данные, сетевая безопасность, личная информация, а также критически важная информационная инфраструктура. Так, под критически важной информационной инфраструктурой понимается область государственных информационных и коммуникационных услуг, нанесение ущерба которым может представлять серьезную угрозу общественным интересам, жизни людей, национальному благополучию и безопасности [9].

Первым документом об участии Китайской Народной Республики в международном обмене и сотрудничестве в кибернетическом пространстве стала Стратегия международного сотрудничества в киберпространстве 2017 года, которая провозглашает суверенное равенство всех стран, вводит понятие «интернет-суверенитет» и включает положения о невмешательстве во внутренние дела государств, а отдельные пункты содержат информацию об угрозах кибертерроризма [10].

Таким образом, опыт превентивных мер Китайской Народной Республики показывает, что необходима дальнейшая разработка и внедрение антитеррористического законодательства. Значимым этапом осуществления стратегических целей является взаимодействие Китая с другими государствами, а также достижение договоренности, сотрудничества и обмена правовым опытом и технологиями в области информации. Китайская Народная Республика осознает необходимость и важность введения системы безопасности государственного информационного пространства не только против информационно-технологического терроризма, но и информационно-психологического терроризма на правовом уровне.

Нормативно-правовое обеспечение противодействия информационному терроризму в Соединенных Штатах Америки

В соответствии со Стратегией национальной безопасности США 2002 года, информационная угроза безопасности страны возникла на стыке радикализма и новейших технологий [11]. Как говорил Джордж Буш-младший, вчера, чтобы представлять угрозу Америке, соперники должны были располагать большой армией и значительным промышленным потенциалом; на сегодняшний день маленькая группа людей может посеять страдания и хаос, не имея денег даже для покупки одного танка [12].

В отличие от Китая, США придерживаются либерального правового подхода к содержанию информационной безопасности. Так, «либеральная модель» ориентируется на наименьшее участие государства в процессе использования сети Интернет. В США не применяются технические способы блокировки контента, а методами фильтрации и мониторинга являются соглашения хостеров и провайдеров об удалении запрещенного контента, самоцензура или выступление частных компаний, общественных групп или организаций за блокирование того или иного информационного ресурса.

Под воздействием политических курсов и стратегических целей стран возникают различия в приоритетных задачах в сфере информационной безопасности. Так, КНР основывается на более широкой трактовке потенциальных угроз, поэтому уделяет наибольшее внимание разработке единой концепции международной деятельности в сфере информации. Соединенные Штаты Америки, заявляя себя как мировой лидер [13], оказывают предпочтение точечным и целенаправленным операциям и совместным действиям с партнерами, постепенно наращивая коллективные усилия по предотвращению роста насильственного терроризма.

Первые стратегические задачи и правовые основы информационной безопасности были сформированы в 1990-х годах. Первые задачи в сфере информационного превосходства путем оборонительных и наступательных операций были определены в 1995 году в период администрации Билла Клинтона в Стратегии национальной безопасности [14]. Директиву Президента № 63 от 1998 года «О защите критической инфраструктуры» [15] и Национальную стратегию безопасности киберпространства [16] кодифицировали в виде Директивы Президента № 7 «Об определении, приоритезации и защите критически важных элементов инфраструктуры» [17], где особое внимание уделялось программам превентивных мер в кибернетическом пространстве.

После теракта в 2001 году американский президент Джордж Буш запретил трансляции, любые напоминания и заявления лидеров «Талибана» и «Аль-Каиды». Многими изданиями это было воспринято как нарушение свободы слова. Многие исследователи в своих работах отмечали умеренность в деятельности государственных и правоохранительных органов в сфере ограничения прав и свобод граждан на информацию. Ученые описывали следующие условия возможных ограничений: общество должно согласиться на определенную степень вторжения в личные права и свободы; угрозы

должны соответствовать такому вмешательству; государство должно действовать в пределах полученных полномочий для защиты граждан, а не для тотального полицейского контроля.

После террористической атаки 11 сентября 2001 года был принят акт «О сплочении и укреплении Америки путём обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» [18], получивший в средствах массовой информации название Акт о патриотизме или Патриотический акт. Акт был принят уже 24 октября 2001 года, 26 октября подписан президентом США. Патриотический акт был определен как временный документ, который подлежал постоянной пролонгации. В течение 2005 – 2007 годов происходили периодические дискуссии о рациональности этого документа, в результате споров в законе были изменены полномочия некоторых спецслужб и возможностей президента США.

Юридические последствия Патриотического акта 2001 года можно представить следующим образом:

– проведена связь между организованной преступностью и террористической деятельностью, что ужесточило ответственность за подготовку теракта и другие составы преступления;

– одним из главных нововведений стало закрепление таких базовых понятий, как «внутренний терроризм» и «международный терроризм», а также «кибертерроризм», к которому причислили общественно-опасные деяния, как хакерство, нанесение ущерба локальным сетям граждан, государственных организаций, работающих в сфере национальной обороны. После принятия Патриотического акта 2001 года в США потенциальные угрозы в кибернетическом пространстве стали сферой интересов и всего мирового сообщества.

Американские эксперты выявили несколько проблемных вопросов по противодействию терроризму: пробелы в законодательстве, технологические трудности, недооценка масштаба последствий, сложность в определении виновных лиц, а также недостаточное международное сотрудничество.

Следует отметить, что следующим этапом стремительного развития в направлении кибербезопасности стал приход администрации Барака Обамы, так как президент США с самого начала определил кибербезопасность одной из самых серьезных проблем страны. Так, после рассмотрения мер по защите информационной инфраструктуры США эксперты представили отчет в виде «Обзора политики в киберпространстве» [19], что обусловило появление Комплексной национальной инициативы по обеспечению кибербезопасности. Она включает несколько основных направлений деятельности США в сфере безопасности: создание узконаправленных киберцентров; формирование общей федеральной корпоративной сети; дальнейшая разработка эффективных планов киберразведки; расширение компетенций правительства в сфере кибербезопасности критической инфраструктуры; внедрение программ в учебные планы университетов; спонсирование научных исследований в сфере информации и другие [20].

Все направления деятельности ведомств США направлены против информационно-технологического терроризма, не затрагивая информационно-психологический вид информационного терроризма, но в истории противодействия информационным угрозам были несколько законодательных инициатив. Так, в 2012 году сенат не принял закон о кибербезопасности, который предусматривал запрет контента в кибернетическом пространстве, связанного с терроризмом. Барак Обама предусмотрел возможность принятия нового законопроекта о взаимодействии частных компаний и федеральных агентств во время расследования в том числе и террористических актов, который также не получил достаточного количества голосов в верхней палате конгресса.

Следует отметить, что последующие изданные стратегии при администрации Дональда Трампа затрагивали кибербезопасность относительно других стран, в числе которых КНР и Россия. Так, в Стратегии национальной безопасности от 19 декабря 2017 года Китай называется одним из главных соперников США. Стратегия подчеркивает необходимость справедливого и равного использования «общих пространств», а именно – Мирового океана, воздушного пространства, космоса и, конечно, кибернетического пространства [21, с. 159–161].

Исходя из описанных выше стратегий можно сделать выводы, что Соединенные Штаты Америки рассматривают больше технологическую сторону информационного терроризма и все усилия направлены на защиту объектов критической инфраструктуры.

Международно-правовые меры противодействия информационному терроризму на универсальном уровне

Информационное пространство требует нормативного регулирования со стороны мирового сообщества, каждое государство становится

потенциальным участником в создании системы обеспечения информационной безопасности. Создавая универсальные нормы, государства встают перед выбором ограничить свободу своих действий в информационном пространстве или использовать возможность оговорок, которые могут привести к высокой вероятности возникновения уязвимостей национальных систем в IT-сфере, поэтому странам необходимо возложить на себя «юридическое бремя».

Появление угроз и вызовов в информационном пространстве обусловливает поиск мер противодействия на глобальном уровне. Работа ООН в области информационной безопасности в настоящее время имеет приоритетный характер, так как многие государственные меры ввиду различных политических, социальных, экономических причин не получают ни юридической обязательной силы, ни дальнейшего практического применения.

Учрежденная в 2014 году Группа правительственных экспертов не раз предоставляла в своих докладах сведения о реальной опасности использования ИКТ террористическими организациями, в том числе для нападения на критическую инфраструктуру, что и обусловливает необходимость решительных мер со стороны государств [22]. Так, ГА ООН была принята Резолюция № 71/28 о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности от 2016 года.

Первым международным договором, который касается компьютерных преступлений, является Конвенция Совета Европы о киберпреступности от 2001 года, или Будапештская конвенция [23], определяющая несколько видов киберпреступлений, например мошенничество, нарушение авторского права или безопасности сетей и другие, но любого вида терроризма среди них не было. Руководство 11 или T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention от 14–15 ноября 2016 года восполнило этот пробел [24].

Будапештская конвенция не стала договором, затрагивающим терроризм. Однако в руководстве особо подчеркивается, что основные преступления, которые подпадают под регулирование Конвенции, могут быть совершены для содействия терроризму (финансирование или участие в его подготовке), а также в виде террористических акций. По этой причине международные и процедурные инструменты совместной правовой помощи, содержащиеся в Конвенции, нужно использовать для судебных преследований и следствия, связанных с терроризмом.

Согласно T-CY Guidance Note #11, пределы и сфера действия Конвенции в отношении кибертерроризма определены статьями 25.1 и 14.2. Статья 14.2 говорит о том, что процедуры и полномочия сторонами применяются в отношении уголовных преступлений (в соответствии со ст. 2–11); других уголовных преступлений, которые совершены с помощью компьютерной системы; сбора доказательств уголовного преступления в электронном виде.

Согласно статье 25.1 «стороны оказывают друг другу взаимную помощь в максимально возможной степени в целях расследования или разбирательства уголовных преступлений, связанных с компьютерными системами и данными, или для сбора доказательств в электронной форме уголовного преступления».

На основании статей 23–35 Конвенции стороны обязаны ускоренно обеспечить сохранение, а также изъятие и поиск компьютерных данных, проводить розыскные операции, судебные расследования в рамках международного сотрудничества в области обеспечения информационной безопасности, связанные с терроризмом.

В 2003 году был принят Дополнительный протокол к Конвенции, согласно которому государства-участники обязаны криминализировать распространение ксенофобных и расистских материалов, включая оскорбления и угрозы в информационном пространстве [25].

На протяжении 2021 года на официальном сайте Совета Европы предоставляются для ознакомления проекты второго Дополнительного Протокола к Конвенции о киберпреступности [26]. Последняя версия протокола была утверждена на 24-м пленарном заседании и содержит пункты о расширенном сотрудничестве в сфере компьютерных технологий и раскрытии электронных доказательств.

Создатели проекта Протокола отмечают, что коммуникационные и информационные технологии стремительно трансформировали общество с открытия подписания Будапештской Конвенции в 2001 году, и киберпреступность рассматривается многими странами как серьезная угроза верховенству права, основополагающим правам человека и функционированию демократического общества в целом. В потенциальные угрозы в информационном пространстве создатели внесли нападения на государственные институты и на критическую инфраструктуру, а также неправомерное использование технологий для террористических целей. В соответствии с проектом Протокола определение чрезвычайной ситуации охватывает время после террористической акции, в которое правоохранительные органы пытаются определить, с кем злоумышленники могли общаться, чтобы

оценить, неизбежны ли дальнейшие атаки или угрозы критической инфраструктуре.

Информационный терроризм, как отмечалось ранее, делится на два основных вида – «технологический» и «психологический». Создание мер по противодействию исследуемому явлению должно работать в двух направлениях, а это возможно при преодолении политической и правовой несогласованности мировых держав.

В настоящий момент разрушающее действие информационного терроризма может превысить уровень поражения всех других видов и форм терроризма, поэтому каждая норма в сфере информационной безопасности выступает как достижение национального и универсального уровней, которые необходимо закреплять и претворять в практическую деятельность каждого государства.

Список литературы

1. **全国人大常委会关于**维护互联网安全的决定 (Quánguó réndà chángwěi huì guānyú wéihù hùliánwǎng ānquán de juédìng; Постановление Всекитайского собрания народных представителей (ВСНП) об обеспечении безопасности в сети интернет). URL: https://wenku.baidu.com/view/a046401b25c52cc58bd6beab.html (дата обращения: 25.05.2021).

2. 2006-2020 **年国家信息化**发展战略 (2006–2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè; Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.). URL: https://baike.baidu.com/item/2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5 (дата обращения: 25.05.2021).

3. Чекменёва Т.Г., Ершов Б.А., Трубицын С.Д., Остапенко А.А. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты // Bulletin Social-Economic and Humanitarian Research. 2020. № 7 (9). С. 78–97.

4. Сидненко Г.Ф. Информационное противодействие терроризму: политологический аспект. М.: Изд-во Триумф, Лучшие книги, 2019. 220 с.

5. Зверянская Л.П. Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики // Труды Института государства и права РАН. 2017. Т. 12. № 5. С. 196–214.

6. Закопаева Д.С. Особенности социальных сетей КНР // Гуманитарное знание и искусственный интеллект: стратегии и инновации: Материалы Международной конференции. Екатеринбург, 2020. С. 926–928.

7. **中华人民共和国反恐怖主义法** (Zhōnghuá rénmín gònghéguó fǎn kǒngbù zhǔyì fǎ; Антитеррористический закон КНР). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95 (Дата обращения: 26.05.2021).

8. **中**华人民共和国国家安全法 (О государственной безопасности). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E6%B3%95?fromtitle=%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E6%B3%95&fromid=830236 (дата обращения: 26.05.2021).

9. **中**华人民共和国网络安全法 (Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ; Закон КНР о кибербезопасности). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin (дата обращения: 26.05.2021).

10. International Strategy of Cooperation on Cyberspace. URL: https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm (дата обращения: 26.05.2021).

11. The National Security Strategy of the United States of America. Washington, D.C.: The White House. September 2002. Introduction. URL: http://www.state.gov/documents/organization/63562.pdf (дата обращения: 27.05.2021).

12. George W. Bush Speech to the National Security Counsil. The White House. September 17, 2002.

13. Стратегия национальной безопасности США (объявлена президентом США Б. Обамой 15 февраля 2015 г.). URL: https://oko-planet.su/politik/politiklist/271399-polnyy-tekst-strategii-nacionalnoy-bezopasnosti-ssha.html html (Дата обращения: 27.05.2021).

14. Clinton William. National Security Strategy. Washington DC: Government Printing Office. February 1995. P. 8.

15. Presidential Decision Directive / NSC-63 / The White House, Washington // The White House. 22.05.1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (дата обращения: 27.05.2021).

16. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 27.05.2021).

17. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection // U.S. Department of Homeland Security. 17.12.2003. URL: https://www.dhs.gov/homeland-security-presidential-directive-7 (дата обращения: 27.05.2021).

18. Act on the «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism». URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата обращения: 27.05.2021).

19. White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (дата обращения: 27.05.2021).

20. The Comprehensive National Cybersecurity Initiative 2009 // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 27.05.2021).

21. Кулешова Г.П., Капитонова Е.А., Романовский Г.Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 156–165.

22. Резолюция 2396 (2017), принятая Советом Безопасности на его 8148-м заседании 21 декабря 2017 г.; Резолюция 2395 (2017), принятая Советом Безопасности на его 8146-м заседании 21 декабря 2017 г. и др. // Система официальной документации ООН. URL: https://documents.un.org (дата обращения: 28.05.2021).

23. Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23 ноября 2001 года. URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения: 21.05.2021).

24. T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention. Adopted by the 16th Plenary of the T-CY. 2016. 14-15 November. URL: https://rm.coe.int/16806bd640 (дата обращения: 28.05.2021).

25. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем ETS N 189 (Страсбург, 28 января 2003). URL: https://base.garant.ru/4084840/ (дата обращения: 1.06.2021).

26. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol version 3 as approved by the T-CY at its 24th Plenary (28 May 2021). URL: https://rm.coe.int/0900001680a2aa1c (дата обращения: 1.06.2021).

INTERNATIONAL EXPERIENCE OF LEGAL REGULATION OF COUNTERING INFORMATION TERRORISM

E.V. Saounina, I.D. Bazhina

The definition and two forms of information terrorism have been formulated. The international experience of legal regulation of information terrorism is analyzed on the example of Republic of China and the United States of America. The conclusion is substantiated that the PR China has developed a legal approach that affects the influence of the media and technological problems. The USA adheres to the "liberal model", focusing on the least participation of the state in the process of using the information space.

Keywords: terrorism, information terrorism, types of information terrorism, international legal counteraction to terrorism, Republic of China, the United States of America.

References

1. 全国人大常委会关于维护互联网安全的决定 (Quánguó réndà chángwěi huì guānyú wéihù hùliánwǎng ānquán de juédìng; Resolution of the National People's Congress (NPC) on ensuring security on the Internet). URL: https://wenku.baidu.com/view/a046401b25c52cc58bd6beab.html (Date of access: 25.05.2021).

2. 2006-2020 年国家信息化发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè; The State strategy for the development of informatization for the period from 2006 to 2020). URL: https://baike.baidu.com/item/2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5 (Date of access: 25.05.2021).

3. Chekmeneva T.G., Ershov B.A., Trubitsyn S.D., Ostapenko A.A. China's strategy for ensuring information security: political and technical aspects // Bulletin Social-Economic and Humanitarian Research. 2020. № 7 (9). P. 78–97.

4. Sidnenko G.F. Informational counteraction to terrorism: a political aspect. M.: Triumph Publishing House, Best books, 2019. 220 p.

5. Zveryanskaya L.P. Organizational and legal support of international and national information security: the experience of the People's Republic of China // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2017. Vol. 12. № 5. P. 196–214.

6. Zakopaeva D.S. Features of social networks of the People's Republic of China // Humanitarian knowledge and artificial intelligence: strategies and innovations: Materials of the International Conference. Yekaterinburg, 2020. P. 926–928.

7. 中华人民共和国反恐怖主义法 (Zhōnghuá rénmín gònghéguó fǎn kǒngbù zhǔyì fǎ; Anti-Terrorism Law of the People's Republic of China). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95 (Date of access: 26.05.2021).

8. 中华人民共和国国家安全法 (About State security). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E6%B3%95?fromtitle=%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E6%B3%95&fromid=830236 (Date of access: 26.05.2021).

9. 中华人民共和国网络安全法 (Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ; China's Cybersecurity Law). URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin (Date of access: 26.05.2021).

10. International Strategy of Cooperation on Cyberspace. URL: https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm (Date of access: 26.05.2021).

11. The National Security Strategy of the United States of America. Washington, D.C.: The White House. September 2002. Introduction. URL: http://www.state.

gov/documents/organization/63562.pdf (Date of access: 27.05.2021).

12. George W. Bush Speech to the National Security Counsil. The White House. September 17, 2002.

13. The US National Security Strategy (announced by US President B. Obama on February 15, 2015). URL: https://oko-planet.su/politik/politiklist/271399-polnyy-tekst-strategii-nacionalnoy-bezopasnosti-ssha.htmlhtml (Date of access: 27.05.2021).

14. Clinton William. National Security Strategy. Washington DC: Government Printing Office. February 1995. P. 8.

15. Presidential Decision Directive / NSC-63 / The White House, Washington // The White House. 22.05.1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (Date of access: 27.05.2021).

16. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/ (Date of access: 27.05.2021).

17. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection // U.S. Department of Homeland Security. 17.12.2003. URL: https://www.dhs.gov/homeland-security-presidential-directive-7 (Date of access: 27.05.2021).

18. Act on the «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism». URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (Date of access: 27.05.2021).

19. White House Cyberspace Policy Review, May 2009 // U.S. Department of Homeland Security. URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (Date of access: 27.05.2021).

20. The Comprehensive National Cybersecurity Initiative 2009 // Obama White House Archives. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (Date of access: 27.05.2021).

21. Kuleshova G.P., Kapitonova E.A., Romanovsky G.B. Legal foundations of countering cyberterrorism in Russia and abroad from the standpoint of the socio-political dimension // All-Russian Journal of Criminology. 2020. Vol. 14. № 1. P. 156–165.

22. European Convention on Cybercrimes (Crimes in Cyberspace). Budapest, November 23, 2001. URL: http://mvd.gov.by/main.aspx?guid=4603 (Date of access: 21.05.2021).

23. T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention. Adopted by the 16th Plenary of the T-CY. 2016. 14-15 November. URL: https://rm.coe.int/16806bd640 (Date of access: 28.05.2021).

24. Additional Protocol to the Convention on Crimes in the Field of Computer Information, on Incriminating Racist Acts and Committed Xenophobe using information systems ETS N 189 (Strasbourg, January 28, 2003). URL: https://base.garant.ru/4084840/ (Date of access: 1.06.2021).

26. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol version 3 as approved by the T-CY at its 24th Plenary (28 May 2021). URL: https://rm.coe.int/0900001680a2aa1c (Date of access: 1.06.2021).