УДК 343.92
DOI 10.17150/2500-4255.2017.11(3).607-614

КИБЕРТЕРРОРИЗМ В КИТАЕ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

Р.И. Дремлюга[1], А.И. Коробеев[1], А.В. Федоров[2]
[1] Дальневосточный федеральный университет, г. Владивосток, Российская Федерация
[2] Следственный комитет Российской Федерации, г. Москва, Российская Федерация

Информация о статье
Дата поступления
2 апреля 2017 г.

Дата принятия в печать
25 июня 2017 г.

Дата онлайн-размещения
29 сентября 2017 г.

Ключевые слова
Киберпреступность; преступность в Интернете; кибертерроризм; преступность в Китае

Аннотация. Статья посвящена проблеме борьбы с проявлениями кибертерроризма в Китае. Так как Китай — мировой лидер по количеству пользователей Интернета, а также единственная страна в мире, где реализована программа широкомасштабного ограничения доступа к деструктивной информации, то его опыт борьбы с кибертерроризмом уникален и может представлять интерес для российских криминологов. В статье акцентируется внимание на том, что терроризм в целом представляет для Китая одну из наиболее актуальных проблем, и контртеррористические меры скорее можно охарактеризовать как настоящую войну. Отмечается, что сеть Интернет используется террористами не только как средство и способ совершения преступления, но и для деятельности, являющейся вспомогательной, например для вербовки новых членов, коммуникации внутри группы, сбора финансовых средств на поддержку террористической деятельности, распространения агитационных и пропагандистских материалов, получения информации о потенциальных целях террористических атак. Несмотря на то что в целом авторы оценивают опыт Китайской Народной Республики как успешный, существуют серьезные вызовы, решения по которым еще не найдены. Это, во-первых, широкая распространенность информации о методах обхода систем ограничения доступа к протеррористической информации; во-вторых, использование теневого Интернета (Dark Net) для получения и распространения деструктивной террористической информации; в-третьих, широкое распространение нелегальных интернет-кафе, количество которых растет год от года, несмотря на активные усилия правоохранительных органов по их закрытию.

CYBERTERRORISM IN CHINA: CRIMINAL LAW AND CRIMINOLOGICAL ASPECTS

Roman I. Dremliuga[1], Aleksandr I. Korobeev[1], Aleksandr V. Fedorov[2]
[1] Far Eastern Federal University, Vladivostok, the Russian Federation
[2] The Investigative Committee of the Russian Federation, Moscow, the Russian Federation

Article info
Received
2017 April 2

Accepted
2017 June 25

Available online
2017 September 29

Keywords
Cybercrime; crime in the Internet; cyberterrorism; crime in China technical-criminalistic methods; tactical-criminal methods

Abstract. The paper discusses cyberterrorism counteraction in China. China has the highest number of Internet users of any country in the world, it is also the only country to implement a large-scale restriction of access to destructive information, which makes its experience in counteracting cyberterrorism unique and valuable for Russian criminologists. The authors stress that terrorism in general is one of the most urgent problems for China and counterterrorism measures can easily be described as a real war. They note that the Internet is used by terrorists not only as a way and method of committing crimes, but also for auxiliary activities, for example, for recruiting new members, communication within a group, fundraising to support terrorist activities, dissemination of propaganda materials, collecting information about potential terrorist attack goals. Although the authors assess the experience of the People's Republic of China as generally positive, the country faces serious challenges that have not been solved yet. They are, firstly, a wide availability of information on bypassing the systems that limit access to pro-terrorist information; secondly, the use of the Dark Net to gain and disseminate destructive terrorist information; thirdly, a wide availability of illegal Internet cafes whose number is growing every year in spite of active efforts by law enforcement agencies to close them.

ISSN 2500-4255

Терроризм включен Организацией Объединенных Наций в список глобальных вызовов человечеству. Несмотря на активные меры, предпринимаемые государствами, террористическая деятельность становится все более распространенной и изощренной, а террористические организации подчиняют себе обширные территории, в связи с чем на состоявшемся в октябре 2016 г. в Пекине форуме «Основные тенденции международного терроризма и меры борьбы с ним» констатировалось возникновение так называемых террористических государств [1]. Появление новых технологий расширяет возможности террористов. В частности, использование Интернета позволяет им, оставаясь анонимными, выбирать цели для террористических актов, согласовывать действия участников терактов в различных регионах мира, готовить широкомасштабные преступления террористического характера.

С увеличением числа подключений к сети Интернет критически важных объектов инфраструктуры, медицинских учреждений, правительственных организаций, правоохранительных структур и органов госбезопасности растет актуальность проблемы кибертерроризма. Большинство авторов рассматривают кибертерроризм как разновидность терроризма, особенность которой заключается в том, что террористическая деятельность осуществляется в киберпространстве [2].

Под кибертерроризмом (терроризмом в Интернете) понимается, во-первых, совершение терактов посредством информационных сетей, когда Интернет выступает как способ и средство совершения преступления [3], и, во-вторых, деятельность, способствующая терроризму, например вербовка в террористические организации, сбор средств для террористов или организация взаимодействия между членами террористических групп. Если совершение террористических актов посредством Интернета и других информационных сетей пока не получило широкого распространения, то использование сети Интернет как вспомогательного средства для совершения преступлений уже давно взято на вооружение террористическими группами.

Из видов кибертеррористических деяний, совершаемых посредством Интернета, на сегодняшний день наиболее распространены следующие:

– использование вредоносных программ, стимулирующих разрушение аппаратных средств, например компьютерного вируса Win32.Stuxnet, вносящего изменения в работу ядерных реакторов;

– широкомасштабное уничтожение или повреждение информационной, программной инфраструктуры, имеющей высокую общественную значимость (финансовые системы, системы социальных платежей, государственные системы учета, системы управления);

– раскрытие и опубликование закрытой информации о функционировании государства, общественно значимых и военных сведений в информационных системах по типу сайта WikiLeaks;

– захват интернет-сайтов с целью распространения дезинформации, слухов, объявления своих требований и т.д. (чаще всего deface — подмена оригинального содержания сайта своим ложным содержимым);

– дестабилизация работы сегментов сети Интернет или отдельных сайтов посредством искусственного создания повышенной нагрузки (Dos Denial of Service — атаки на отказ сервиса).

Зачастую волны кибертеррористических атак порождены крупными политическими конфликтами, такими, например, как конфликт в Южной Осетии 2008 г. или война на территории бывшей Югославии [4].

В качестве вспомогательного средства глобальная сеть обычно используется террористами:

– для связи членов террористической группы или организации;

– вербовки новых членов террористических групп и мобилизации уже принятых членов;

– распространения агитационных и пропагандистских материалов;

– распространения информации по изготовлению средств для совершения терактов (оружия, взрывчатых веществ, компьютерных вирусов);

– сбора средств для финансирования деятельности террористических организаций;

– сбора информации о потенциальных целях (людях, объектах инфраструктуры).

Так, координация терактов в Париже в 2015 г. производилась посредством популярных интернет-сервисов для обмена сообщениями Telegram и WhatsApp с шифрованием, недоступным спецслужбам. Использование этих сервисов также повысило результативность действий по вербовке новых террористов[1].

Согласно исследованиям 2009 г., за 1999–2009 гг. количество интернет-сайтов террористических организаций выросло в 400 раз [5] и продолжает увеличиваться. По мнению многих

[1] URL: http://www.upi.com/Top_News/Voices/2017/01/23/Virtual-planners-of-Islamic-State-on-dark-side-of-the-Internet/1421485199057.

специалистов, преступный мир гораздо быстрее правоохранительных органов внедряет новые технологии в свою деятельность [6]. Это обусловлено тем, что, во-первых, преступники не ограничены бюрократическими процедурами и, во-вторых, преступный мир является крайне конкурентной средой.

Вероятность совершения террористического акта посредством Интернета в тех или иных государствах зависит от степени использования глобальной сети. В Китае на конец 2016 г. глобальной сетью пользовалось 52 % населения (для сравнения: в России — 71,3 %, в США — 88,5 %, в Японии — 91,1 %), что в абсолютном выражении составляет 721 млн чел.[2]

С одной стороны, такое количество пользователей Сети в КНР дает государству большие экономические преимущества, а с другой стороны, создает реальные угрозы для его экономической и политической безопасности, так как Китай лидирует в мире по числу потенциальных киберпреступников и жертв их преступлений. Отметим, что с каждым годом ключевые китайские экономические и социальные институты все больше зависят от глобальной сети, что делает страну более уязвимой к кибератакам. Не вызывает сомнений, что одной из самых потенциально опасных интернет-угроз является кибертерроризм.

При этом опасность совершения актов кибертерроризма исходит как от отдельных физических лиц и их групп, так и от организаций, в связи с чем ряд международных договоров предусматривает необходимость установления уголовной ответственности юридических лиц за преступления террористического характера [7], а в национальных законодательствах многих стран, в том числе Китая, предусмотрена уголовная ответственность юридических лиц за отдельные преступления террористического характера [8].

С этой точки зрения Китай и меры, направленные им на борьбу с террористическими проявлениями в сети Интернет, представляются крайне интересным объектом исследования. Во-первых, это страна номер один по количеству пользователей (физических и юридических лиц) глобальной информационной сети, что делает ее наиболее уязвимой к любым видам киберпреступлений, включая терроризм посредством и с помощью Интернета. Во-вторых, в Китае очень остро стоит проблема терроризма в целом.

[2] URL: http://www.internetlivestats.com/internet-users/china.

С учетом изложенного контртеррористические меры зачастую характеризуются не как составляющие борьбы с терроризмом, а как элементы настоящей войны с ним [9].

Впервые в КНР ответственность за посягательства на компьютерную безопасность была установлена Постановлением Государственного Совета Китайской Народной Республики «О компьютерной безопасности информационных систем» от 18 февраля 1994 г. № 147 [10]. Статья 23 этого нормативного акта предусматривала ответственность за намеренное внедрение и распространение компьютерных вирусов, устанавливая за такого рода деяния наказание в размере до 5,000 китайских юаней для физических лиц и до 15,000 — для юридических, а также конфискацию полученных незаконных доходов в результате распространения компьютерного вируса.

Существенным вкладом в борьбу с киберпреступлениями стало принятие 14 марта 1997 г. на пятой сессии Всекитайского собрания народных представителей новой редакции Уголовного кодекса Китая (УК КНР).

В частности, ст. 285 УК КНР устанавливала ответственность за незаконный доступ к компьютерной информации государственной важности либо связанной с обороноспособностью, а также к данным о прорывных технологиях и научных открытиях. Статья 286 УК КНР устанавливала уголовную ответственность за удаление, искажение, внесение компьютерной информации, вызвавшей нарушение работы и существенные последствия, а также за намеренное создание и распространение компьютерных вирусов. Статья 287 УК КНР признавала преступным использование компьютера для финансового мошенничества, кражи, хищения, присвоения государственных средств, хищения государственной тайны и другие подобные деяния. Стоит отметить, что данные статьи включены в раздел «Преступления против порядка управления» (ст. 277–367). Это свидетельствует о том, что данные статьи были направлены не только на защиту экономических интересов Китая, но и прежде всего на повышение уровня информационной безопасности государства.

В то же время упоминание Интернета и компьютерных технологий есть в ряде статей УК КНР, устанавливающих ответственность за преступления экономической направленности, что присуще и российскому уголовному законодательству [11].

Китай, как и большинство азиатских стран [12], после событий 11 сентября 2001 г. суще-

ственно ужесточил антитеррористическое законодательство. Так, на 25-м заседании Постоянного комитета девятого Всекитайского собрания народных представителей КНР 29 декабря 2001 г. были приняты Поправки № 3 в уголовное законодательство[3]. Как зафиксировано в преамбуле этих поправок, их цель — установить наказуемость террористических преступлений для обеспечения безопасности государства, жизни и имущества людей, а также для поддержания общественного порядка.

Этими поправками изменены ст. 114, 115, 120, 125, 127, 191 УК КНР, а также в кодекс добавлена ст. 120-1, устанавливающая ответственность за финансирование террористических организаций и групп, и ст. 291-1, признающая преступным распространение средств для совершения терактов (взрывчатых, радиоактивных и подобных веществ), а также ложной информации о терроризме[4].

Основываясь на изменениях в УК КНР, китайские власти в настоящее время применяют к сепаратистам Уйгурского района и Тибета термин «террористы». В частности, террористами признаются члены организации «Исламское движение Восточного Туркестана», требующей создания единого исламского государства и обращения в ислам всего китайского населения [9; 13], а сама организация признана террористической.

На сегодняшний день в УК КНР значительное количество статей полностью или частично посвящено киберпреступлениям[5]. Кроме упомянутых выше статей, включенных в УК КНР в 1997 г., изменена ст. 246 кодекса. В ней предусмотрена ответственность за оскорбление посредством информационной сети, приведшее к серьезным последствиям. Новая редакция ст. 287а УК КНР «Пособничество совершению преступлений посредством информационных сетей» криминализирует деяния, выражающиеся в предоставлении доступа, организации платежей, осуществлении коммуникаций. Статья 286 УК КНР, в редакции 1997 г. устанавливавшая уголовную ответственность за искажение информации, нарушение работы компьютерных систем и распространение вирусов, в настоящее время признает преступными действия, нарушающие требования по информационной безопасности, предъявляемые к предоставлению интернет-доступа. Отсылка к информационным сетям появилась и в статьях, устанавливающих уголовную ответственность за террористическую деятельность.

Статья 291 УК КНР в числе других деяний устанавливает ответственность за распространение слухов о радиоактивной, химической или другой угрозе с целью намеренного нарушения общественного порядка, т.е. распространения в Интернете так называемой фальшивой террористической информации.

По опубликованным данным, Китай уже который год входит в тройку самых атакуемых зарубежными киберпреступниками стран [14]. Китайские власти неоднократно подчеркивали высокую виктимизацию страны по причине иностранных кибератак. Они также обеспокоены отсутствием со стороны западных стран интереса к реальному сотрудничеству в борьбе с киберпреступностью, тогда как более 70 % зараженных компьютеров, атакующих сети Китая, расположены за рубежом. Согласно докладу Perception Report Computer Emergency Team, в 2011 г. 8,9 млн китайских компьютеров подверглись нападению с 47 тыс. иностранных интернет-адресов, сделав Китай крупнейшей в мире кибержертвой [15].

Наиболее известной мерой китайского правительства по противодействию распространению деструктивной информации, в том числе террористической, является так называемый Золотой щит (Golden Shield) — общенациональный электронный барьер, фильтрующий и контролирующий информационные потоки таким образом, что все интернет-данные пользователей в Китае проходят через ограниченное число контрольно-пропускных пунктов (шлюзов), управляемых ограниченным числом компаний, предоставляющих доступ в Интернет [16]. Данный проект стартовал в 1998 г., и в 2006 г. весь Интернет попал под контроль названной государственной системы [17]. С этого времени любой интернет-пользователь, находящийся на территории Китая, не может получить доступ к сайтам, распространяющим террористические сведения или призывы, а также к любой другой информации протеррористического толка. Данное техническое средство направлено не только

[3] URL: https://www.loc.gov/law/help/fighting-extremism/china.php.

[4] Уголовный кодекс КНР : принят 14 марта 1997 г. URL: http://www.lehmanlaw.com/resource-centre/laws-and-regulations/general/amendment-3-to-the-criminal-law-of-the-peoples-republic-of-china-2001.html ; URL: http://www.cecc.gov/resources/legal-provisions/third-amendment-to-the-criminal-law-of-the-peoples-republic-of-china.

[5] URL: http://cdjjjc.gov.cn/onews.jsp?id=1063.

на борьбу с терроризмом, но и в целом на ограничение доступа к антиправительственной, аморальной (порнография, насилие) и преступной (пропаганда употребления наркотиков, антисоциального поведения) информации. Такие меры препятствуют формированию антисоциальных установок у пользователей сети Интернет, что может быть полезным и для противодействия использованию в противоправных целях и русскоязычного Интернета [18].

Китай достаточно жестко подходит к регулированию размещения информации в сети Интернет и доступа к ней. В отличие от большинства стран, в КНР компании, предоставляющие доступ в Интернет, или компании, предоставляющие услуги размещения информации на своих сайтах, несут ответственность за размещенную информацию.

Компании, предоставляющие доступ в Интернет, должны обеспечить технические средства контроля и блокирования информации, которую китайское правительство считает нежелательной. Такая запрещенная информация определяется по девяти позициям [17], а именно информация признается запрещенной, если она:

– противоречит основным принципам, которые заложены в Конституции, законах, или правилам управления;

– подрывает правящий режим государства или систему социализма;

– оспаривает государственную власть или саботирует единство государства;

– подстрекает этническую вражду или расовую дискриминацию;

– распространяет слухи, нарушающие общественный порядок;

– распространяет архаичные суеверия, непристойности, порнографию или азартные игры; подстрекает насилие, убийство или террор; подстрекает других к совершению правонарушений;

– публично оскорбляет или порочит других;

– наносит вред репутации или интересам государства;

– имеет содержание, запрещенное законами или административными нормативно-правовыми актами.

Как видно из приведенного перечня, большинство категорий запрещенной информации можно отнести к так называемой протеррористической информации, которая как угрожает государству и принципам, заложенным в Конституции, так и подрывает общественный порядок, подстрекает к насилию и вражде.

Китайское законодательство по запрету на распространение протеррористической и антиправительственной информации часто подвергается критике. Одним из основных критикуемых недостатков является отсутствие строгих правил отнесения информации к той или иной категории. Пользователи Сети не всегда могут предугадать и предсказать отнесение конкретной информации к запрещенной (преступной), так как правила заменены общими принципами достаточно широкого толкования [19].

Оценивать эффективность предпринятых китайским государством мер по противодействию кибертерроризму достаточно сложно, так как официальная статистика по киберпреступлениям и террористическим актам не публикуется. Если взять сведения, которые на протяжении многих лет собираются из общедоступных источников Национальным консорциумом по изучению терроризма и реагирования на терроризм (The National Consortium for the Study of Terrorism and Responses to Terrorism)[6], то максимальное количество терактов в Китае приходится на 1996 г. — более 60 и 2014 г. — 38[7].

Тем не менее, если сравнивать статистику по терактам с данными по другим азиатским странам, в которых существуют очаги сепаратизма, например Индонезии и Филиппинам [12], то Китай существенно выигрывает на их фоне. В то же время имеются нерешенные проблемы по ряду направлений антитеррористической деятельности, в частности в сфере ограничения доступа к распространяемой в террористических целях информации.

Существует много методов обхода китайского общенационального электронного барьера. Статьи на эту тему стали появляться сразу после начала работы «Великого китайского интернет-щита» [20; 21].

Так, несмотря на использование «Великого китайского интернет-щита», Китай лидирует по количеству компьютеров, входящих в хакерские ботнеты, т.е. в сети компьютеров, находящихся под

[6] START (National Consortium for the Study of Terrorism and Responses to Terrorism). URL: http://www.start.umd.edu/gtd/search/Results.aspx?chart=overtime&casualties_type=b&casualtiesmax=&dtp2=all&country=44.

[7] Следует учитывать, что в Китае существенно ограничено размещение информации. Таким образом, есть вероятность, что число произошедших терактов не соответствует их количеству, о котором стало известно из общедоступных источников.

контролем хакеров. Именно компьютеры ботнета могут использоваться для массированных атак на правительственные интернет-сайты и коммуникационные узлы, более того, многие исследователи считают их основным источником широкомасштабных атак в Интернете [22, p. 70–72].

Существенным препятствием на пути борьбы с террористической и иной антиправительственной деятельностью в китайском сегменте сети Интернет является большое количество незарегистрированных интернет-кафе, откуда любой потенциальный киберпреступник может выходить в глобальную сеть анонимно. Несмотря на то что китайские власти неоднократно предпринимали меры по закрытию нелегальных интернет-кафе (в 2002–2003 гг. было закрыто около 43 тыс. таких заведений [17]), проблема остается достаточно насущной. Нелегальные интернет-кафе по-прежнему используются для доступа к запрещенной информации [23]. Каждая новая волна рейдов против неконтролируемого распространения информации и анонимного доступа через интернет-кафе выявляет десятки тысяч вновь открытых нелегальных заведений. Например, в 2014 г. Министерством культуры их было закрыто 14 тыс. [24]. Таким образом, можно констатировать, что предпринимаемые китайским правительством меры в отношении пользователей интернет-кафе еще малоэффективны.

Опыт Китая по противодействию кибертерроризму показывает, что использование Интернета в террористических целях представляет серьезную опасность, и необходимо как дальнейшее развитие антитеррористического законодательства, так и совершенствование антитеррористической практики в указанной сфере, изучение практики использования сети Интернет в террористических целях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Федоров А.В. Основные тенденции международного терроризма и меры борьбы с ним / А.В. Федоров, Д.Н. Сергеев // Российский следователь. — 2016. — № 24. — С. 3–9.

2. Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Т.Л. Тропина // Информационные технологии и безопасность : сб. науч. тр. междунар. конф. — Киев : Нац. акад. наук Украины, 2003. — Вып. 3. — С. 173–181.

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

4. Матвиенко Ю.А. Предупредить — значит вооружить (кибертерроризм вчера, сегодня и завтра) / Ю.А. Матвиенко // Информационные войны. — 2011. — № 2. — С. 60–70.

5. Шивдяков Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма / Л.А. Шивдяков // Защита информации. Инсайд. — 2009. — № 2 (26). — С. 64–72.

6. Goodman M. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World / Marc Goodman. — Doubleday, 2015. — 393 p.

7. Федоров А.В. Международно-правовое регулирование уголовной ответственности юридических лиц в системе мер противодействия терроризму / А.В. Федоров // Вестник Академии Следственного комитета Российской Федерации. — 2016. — № 4. — С. 21–33.

8. Федоров А.В. Уголовная ответственность юридических лиц в Китайской Народной Республике / А.В. Федоров // Правовое поле современной экономики. — 2016. — № 1. — С. 22–28.

9. Martin I. Wayne Inside China's War on Terrorism / I. Martin // Journal of Contemporary China. — 2009. — Vol. 18. — P. 249–261.

10. Li P. Ordinance of the People's Republic of China on the Protection of Computer Information System Security / P. Li // Chinese Law & Government. — 2010. — Vol. 43, iss. 5. — P. 12–16.

11. Korobeev A.I. Comparative analysis of legislation of various countries governing release from criminal liability in cases of crimes in the sphere of economic activity / A.I. Korobeev, A.V. Kuznetcov // Journal of Internet Banking and Commerce. — 2016. — Vol. 21, iss. 3. — P. 1–13.

12. Дремлюга Р.И. Криминологическая характеристика терроризма в Индонезии / Р.И. Дремлюга // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2014. — № 1 (30). — С. 148–166.

13. Лузянин С.Г. Особенности правового регулирования борьбы с преступностью в Китае / С.Г. Лузянин, П.В. Трощинский, Я.А. Суходолов // Всероссийский криминологический журнал. — 2016. — Т. 10, № 4. — С. 812–824. — DOI: 10.17150/2500-4255.2016.10(4).812-824.

14. Kim S.H. A comparative study of cyberattacks / Seung Hyun Kim, Qiu-Hong Wang, Johannes B. Ullrich // Communications of the ACM. — 2012. — Vol. 55, iss. 3. — P. 66–73.

15. Kshetri N. Cyber-victimization and cybersecurity in China: Seeking insights into cyberattacks associated with China / N. Kshetri // Communications of the ACM. — 2013. — Vol. 56, iss. 4. — P. 35–37.

16. Navarria G. China: the Party, the Internet, and power as shared weakness / G. Navarria // Global Change, Peace and Security. — 2016. — Vol. 29. — P. 1–20.

17 . Liang B. Document Internet development, censorship, and Cybercrimes in China / B. Liang, H. Lu // Journal of Contemporary Criminal Justice. — 2010. — Vol. 26. — P. 103–120.

18. Dremliuga R. Subculture of hackers in Russia / R. Dremliuga // Asian Social Science. — 2014. — Vol. 10. — P. 158–162. — DOI: 10.5539/ass.v10n18p158.

19. Xingan Li. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime / Xingan Li // International Journal of Cyber Criminology. — 2015. — Vol. 9, iss. 2. — P. 185–204.

20. Bradbury D. Routing around censorship / D. Bradbury // Network Security. — 2011. — № 5 — P. 5–8.

21. Clayton R. Ignoring the Great Firewall of China / Richard Clayton, Steven J. Murdoch, Robert N.M. Watson // Privacy Enhancing Technologies / eds G. Danezis, P. Goll. — Berlin : Springer Verlag, 2006. — P. 20–35.

22. Handbook of Asian Criminology / eds Jianhong Liu, Bill Hebenton, Susyan Jou. — New York : Springer Science : Springer Business Media, 2013. — 434 p.

23. Hong J. A split and swaying approach to building information society: The case of Internet cafes in China / J. Hong, L. Huang // Telematics and Informatics. — 2005. — Iss. 22. — P. 377–393.

24. Fullerton J. China Has Had Enough of Its Illegal Internet Cafés [Electronic resource] / Jamie Fullerton // Online Journal «Motherboard». — 2015. — 8 Dec. — Mode of access: http://motherboard.vice.com/read/china-has-had-enough-of-its-illegal-internet-cafs.

REFERENCES

1. Fedorov A.V., Sergeev D.N. Major trends of international terrorism and antiterrorism protection. *Rossiiskii sledovatel' = Russian Investigator*, 2016, no. 24, pp. 3–9. (In Russian).

2. Tropina T.L. Cybercrime and cyberterrorism: talking about the conceptual framework. *Informatsionnye tekhnologii i bezopasnost'. Sbornik nauchnykh trudov mezhdunarodnoi konferentsii* [Information Technologies and Security. Collected Research Papers of the International Conference]. Kiev, Ukrainian National Academy of Sciences Publ., 2003, iss. 3, pp. 173–181. (In Russian).

3. Dremliuga R.I. The Internet as a way and a method of committing crimes. *Informatsionnoe pravo = Information Law,* 2008, no. 4, pp. 27–31. (In Russian).

4. Matvienko Yu.A. To forewarn is to forearm (cyberterrorism yesterday, today and tomorrow). *Informatsionnye voiny = Information Wars*, 2011, no. 2, pp. 60–70. (In Russian).

5. Shivdyakov L.A. Cyberterrorism as a new and most dangerous form of terrorism. *Zashchita informatsii. Insaid = Information Protection. Inside,* 2009, no. 2, pp. 64–72. (In Russian).

6. Goodman Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. Doubleday, 2015. 393 p.

7. Fedorov A.V. International legal regulation of criminal liability of juridical persons in the system of counter-terrorism measures. *Vestnik Akademii Sledstvennogo komiteta Rossiiskoi Federatsii = Bulletin of the Academy of the Investigative Committee of the Russian Federation,* 2016, no. 4, pp. 21–33. (In Russian).

8. Fedorov A.V. Criminal liability of legal persons in People's Republic of China. *Pravovoe pole sovremennoi ekonomiki = The Legal Field of Contemporary Economy*, 2016, no. 1, pp. 22–28. (In Russian).

9. Martin I. Wayne Inside China's War on Terrorism. *Journal of Contemporary China*, 2009, vol. 18, pp. 249–261.

10. Li P. Ordinance of the People's Republic of China on the Protection of Computer Information System Security. *Chinese Law & Government*, 2010, vol. 43, iss. 5, pp. 12–16.

11. Korobeev A.I., Kuznetcov A.V. Comparative analysis of legislation of various countries governing release from criminal liability in cases of crimes in the sphere of economic activity. *Joumal of Internet Banking and Commerce*, 2016, vol. 21, iss. 3, pp. 1–13.

12. Dremliuga R.I. The criminological characteristics of terrorism in Indonesia. *Aziatsko-Tikhookeanskii region: ekonomika, politika, pravo = Pacific Rim: Economics, Politics, Law*, 2014, no. 1 (30), pp. 148–166. (In Russian).

13. Luzyanin S.G., Troshchinskiy P.V., Sukhodolov Ya.A. Specific features of legal regulation of crime counteraction in China. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 812–824. DOI: 10.17150/2500-4255.2016.10(4).812-824. (In Russian).

14. Kim Seung Hyun, Wang Qiu-Hong, Ullrich Johannes B. A comparative study of cyberattacks. *Communications of the ACM*, 2012, vol. 55, iss. 3, pp. 66–73.

15. Kshetri N. Cyber-victimization and cybersecurity in China: Seeking insights into cyberattacks associated with China. *Communications of the ACM*, 2013, vol. 56, iss. 4, pp. 35–37.

16. Navarria G. China: the Party, the Internet, and power as shared weakness. *Global Change, Peace and Security*, 2016, vol. 29, pp. 1–20.

17. Liang B., Lu H. Document Internet development, censorship, and Cybercrimes in China. *Journal of Contemporary Criminal Justice*, 2010, vol. 26, pp. 103–120.

18. Dremliuga R. Subculture of hackers in Russia. *Asian Social Science*, 2014, vol. 10, pp. 158–162.

19. Xingan Li. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, 2015, vol. 9, iss. 2, pp. 185–204.

20. Bradbury D. Routing around censorship. *Network Security*, 2011, no. 5, pp. 5–8.

21. Clayton Richard, Murdoch Steven J., Watson Robert N.M. Ignoring the Great Firewall of China. In Danezis G., Goll P. (eds). *Privacy Enhancing Technologies*. Berlin, Springer Verlag, 2006, pp. 20–35.

22. Liu Jianhong, Hebenton Bill, Jou Susyan (eds). *Handbook of Asian Criminology*. New York, Springer Science, Springer Business Media, 2013. 434 p.

23. Hong J., Huang L. A split and swaying approach to building information society: The case of Internet cafes in China. *Telematics and Informatics*, 2005, iss. 22, pp. 377–393.

24. Fullerton Jamie. China Has Had Enough of Its Illegal Internet Cafés. *Online Journal «Motherboard»,* 2015, 8 December. Available at: http://motherboard.vice.com/read/china-has-had-enough-of-its-illegal-internet-cafs.

ISSN 2500-4255

ИНФОРМАЦИЯ ОБ АВТОРАХ

Дремлюга Роман Игоревич — доцент кафедры международного публичного и частного права Юридической школы Дальневосточного федерального университета, кандидат юридических наук, г. Владивосток, Российская Федерация; e-mail: dremliuga.ri@dvfu.ru.

Коробеев Александр Иванович — заведующий кафедрой уголовного права и криминологии Юридической школы Дальневосточного федерального университета, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, г. Владивосток, Российская Федерация; e-mail: akorobeev@rambler.ru.

Федоров Александр Вячеславович — заместитель председателя Следственного комитета Российской Федерации, главный редактор журнала «Наркоконтроль», кандидат юридических наук, профессор, заслуженный юрист Российской Федерации, г. Москва, Российская Федерация; e-mail: 1956af@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Дремлюга Р.И. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты / Р.И. Дремлюга, А.И. Коробеев, А.В. Федоров // Всероссийский криминологический журнал. — 2017. — Т. 11, № 3. — С. 607–614. — DOI: 10.17150/2500-4255.2017.11(3).607-614.

INFORMATION ABOUT THE AUTHORS

Dremliuga, Roman I. — Ass. Professor, Chair of International Public and Private Law, Law School, Far Eastern Federal University, Ph.D. in Law, Vladivostok, the Russian Federation; e-mail: dremliuga.ri@dvfu.ru.

Korobeev, Aleksandr I. — Head, Chair of Criminal Law and Criminology, Law School, Far Eastern Federal University, Doctor of Law, Professor, Honored Researcher of the Russian Federation, Vladivostok, the Russian Federation; e-mail: akorobeev@rambler.ru.

Fedorov, Aleksandr V. — Deputy Chairperson, The Investigative Committee of the Russian Federation, Chief Editor, The Drug Control Journal, Ph.D. in Law, Professor, Honored Lawyer of the Russian Federation, Moscow, the Russian Federation; e-mail: 1956af@mail.ru.

FOR CITATION

Dremliuga R.I., Korobeev A.I., Fedorov A.V. Cyberterrorism in China: criminal law and criminological aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 3, pp. 607–614. DOI: 10.17150/2500-4255.2017.11(3).607-614. (In Russian).