УДК 004.738.5 + 351.751.5 Вестник УрФО № 2(32) / 2019, с. 30–38

Добкач Л. Я., Тарапанова Е. А.

DOI: 10.14529/secur190205

ЗАКОНОДАТЕЛЬНЫЙ МЕХАНИЗМ ОГРАНИЧЕНИЯ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

В настоящее время сеть Интернет является сетевой глобальной автоматизированной информационной системой, которая составляет основу формирования и развития современного общества. Данная система действует в глобальном информационном пространстве и представляет собой средство доступа к огромному объему информации. В ряде стран, включая Российскую Федерацию, существует законодательный механизм ограничения распространения определенной информации. Важно понимать, какая информация является общедоступной, а к какой доступ должен быть ограничен или запрещен. Это позволит специалистам по информационной безопасности эффективнее обеспечивать защиту автоматизированных систем от возможных утечек сведений ограниченного распространения.

Ключевые слова: *Интернет, информация, сети общего пользования, информационная безопасность, кибератака, цензура, Золотой щит.*

Dobkacz L. Ya., Tarapanova E. A.

LEGISLATIVE MECHANISM FOR LIMITATION OF INFORMATION DISSEMINATION IN THE INTERNET

Nowadays the Internet is a global automated information system network which is the basis of formation and development of the modern society. This system acts in global informational space and is a source of access to a huge volume of information. In a number of countries including the Russian Federation there is a legislation regulating the limits of circulation of a definite information. It is important to understand what kind of information is a part of public domain and to which the access must be limited or prohibited. In overall, this will enable specialists in info security provide more efficient protection of automated systems from possible leakage of information containing a restricted data.

Keywords: *Internet, information, public networks, information security, censorship, the Golden Shield.*

Введение

Информационно-телекоммуникационная сеть «Интернет» представляет уникальную совокупность локальных, региональных, национальных и международных компьютерных сетей с универсальной технологией об-

мена информацией между миллионами пользователей, даже сильно географически удаленных друг от друга. Согласно п. 1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — 149-ФЗ) информация — это «сведения (сообщения, данные) независимо от формы их представления» [3]. Информация может быть объектом публичных, гражданских и иных правовых отношений, может свободно использоваться любым лицом по своему усмотрению и передаваться одним лицом другому лицу, если законодательно не установлены ограничения доступа к информации либо какие-либо иные требования к порядку ее предоставления или распространения. Понятия «Интернет» в действующем законодательстве РФ нет, но правовая сущность сети отражена в ряде законов.

Существует информация, доступ к которой должен быть ограничен или запрещён, так как такая информация или ее неконтролируемое распространение потенциально способны нанести вред государству, его национальной безопасности, а также частной жизни его граждан. Такие данные присутствуют в том числе в Интернете, что обуславливает необходимость правового регулирования некоторых групп общественных отношений, связанных с использованием этой сети и, в частности, ограничением доступа к сайтам сети Интернет, содержащим информацию, распространение которой в РФ запрещено.

На основании вышеизложенного очевидно, что важно понимать, какие сведения относятся к общедоступной информации, а к каким доступ должен быть ограничен или запрещен. Знание ответа на поставленный вопрос поможет лучше подойти к проблеме эффективности средств защиты информации, в частности систем обнаружения вторжений, что не дают злоумышленникам получать несанкционированный доступ к защищаемой информации, то есть ограниченного распространения, в основном через Интернет.

Правовое обеспечение информационной безопасности реализуется в результате взаимодействия права и государства и выражается в воздействии правовых механизмов на общественные отношения для осуществления функций государства по противодействию угрозам информационной безопасности.

Конституция обладает высшей юридической силой, является основополагающим нормативным правовым актом, все нижестоящие НПА не должны противоречить ей. Конституция Российской Федерации как, впрочем, и конституции многих других государств, устанавливают свободу слова, мысли и различных видов деятельности в отношении информации, если таковая законна. Кроме того, право на информацию — одно из важнейших конституционных прав и свобод человека и гражданина, согласно ст. 17 Конституции РФ этому праву присущи особые свойства — неотчуждаемость и принадлежность каждому от рождения. Согласно ч. 1 ст. 29, каждому гарантируется свобода мысли и слова. Логичным инструментом представляется цензура, однако, согласно ч. 5 ст. 29 Конституции Российской Федерации, цензура запрещается. При этом гарантируется свобода массовой информации. В развитие указанных норм недопустимость цензуры закрепляет также, в частности, ст. 3 Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» [7].

К большому пласту информации доступ ограничен или запрещён. Подобные действия возможны в соответствии со статьями 55 и 56 всё того же Основного закона РФ, ч. 3 ст. 55 гласит, что права и свободы гражданина могут быть ограничены — федеральным законом, — но лишь на необходимый для благополучия государства и её жителей минимум. А ч. 3 ст. 56 подразумевает, что права и свободы, закреплённые в ст. 29, могут быть ограничены при необходимости (с той лишь оговоркой, что в случае чрезвычайного положения), исходя из списка статей, устанавливающих права и свободы, не подлежащие какому-либо ограничению [1, ст. 55, 56].

Чтобы разобраться, какую информацию можно распространять, а какую — нет, обратимся к № 149-ФЗ. Ст. 5 представляет информацию как объект правовых отношений. В п. 1 ст. 5 закреплено, что федеральные законы могут ограничивать доступ к определённой информации. Далее пункты 2 и 3 ст. 5 в развитие вышеуказанных конституционных норм вводят градацию информации по степени распространяемости, то есть делят её на общедоступную; разрешённую к распространению по договорённости лиц; подлежащую федеральными законами к распространению и ограниченную или запрещённую [3, ст. 5].

В первую очередь к ограниченной информации относятся сведения, составляю-

щие государственную или иную тайну, а также содержащие конфиденциальные сведения [1, ст. 23; 3, ст. 9]. Ст. 23 Конституции Российской Федерации уточняет, что судебным решением можно ограничить право граждан на тайну переписки, телефонных переговоров и разнообразных сообщений.

Если с ограничением информации законодательный механизм более-менее ясен, то с запрещённой информацией несколько сложнее. Нетрудно догадаться, что любая запрещённая информация имеет характер сведений ограниченного доступа, а в обратную сторону это не работает. В 149-ФЗ под запрещённой информацией понимается информация, направленная на пропаганду войны, разжигание розни и т.п., что грозит уголовной или административной ответственностью [3, ст. 10 ч. 6].

Читатели новостей в различных интернет-изданиях, социальных сетях и телеграм-каналах не всегда могут отличить правду от недостоверной информации. Не секрет, что некоторые интернет-издания, специально публикуют сенсационную информацию, далекую от истины, ради трафика и заработка на рекламе. Есть и такие, кто использует сайты в политических целях, способствуя продвижению одних политических деятелей и попутно распространяя недостоверную порочащую информацию о других, возможны призывы к массовым беспорядкам и т.п. Подобного рода информация может ввести в заблуждение даже образованных людей, активных пользователей интернета. 07.03.2019 г. Государственная Дума ФС РФ в третьем, окончательном, чтении приняла законопроекты о наказании за распространение недостоверной информации и неуважение к власти в интернете. Так, Законопроектом № 606594-7 определяется порядок ограничения доступа к информации, выражающей в неприличной форме явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции РФ и органам, осуществляющим государственную власть в Российской Федерации. Генеральный прокурор России и его заместители наделяются полномочиями по обращению в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию (материалы) [10].

Таким образом, если на информационном ресурсе в сети Интернет, который зарегистрирован в соответствии с законом РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», появятся подобного рода материалы, то представители Генпрокуратуры обратятся в Роскомнадзор с требованием заблокировать данный ресурс. Роскомнадзор со своей стороны должен направить в редакцию сетевого издания требование удалить вышеуказанные материалы, исполнить это требование нужно незамедлительно, так как в противном случае сайт этого издания подлежит блокировке.

Законопроект № 606596-7 дополняет ст. 20.1 «Мелкое хулиганство» КоАП РФ нормой, устанавливающей административную ответственность за распространение в сети Интернет вышеуказанной информации [12]. Законопроект № 606593-7 разработан в целях пресечения распространения недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу жизни и (или) здоровью граждан, массового нарушения общественного порядка и (или) общественной безопасности, прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, наступления иных тяжких последствий. Распространение такой информации в СМИ или информационно-телекоммуникационных сетях предлагается признавать злоупотреблением свободой массовой информации [9]. За распространение такого рода информации законопроектом № 606595-7 вводится административная ответственность в виде наложения административного штрафа на граждан в размере от 3000 до 5000 рублей; на должностных лиц — от 30 000 до 50 000 рублей; на юридических лиц — от 400 000 до 1 000 000 рублей с конфискацией предмета административного правонарушения [11]. При этом конкретное определение, что такое «явное неуважение», равно как и «недостоверная информация», законодательно пока не закреплено.

Действующее уголовное законодательство России, единственным источником права которого выступает Уголовный Кодекс Российской Федерации (УК РФ), устанавливает значительное количество норм, в соответствии с которыми деяния, совершенные в ин-

формационной сфере, являются уголовно наказуемыми. В контексте настоящей статьи наибольший интерес здесь представляют нормы, предусматривающие наказание за распространения вирусов и другой компьютерной информации, направленной на вредоносную деятельность, а также умышленного или случайного разглашения сведений, составляющих государственную или иную тайну [2, ст. 138, 155, 183, 272–275, 283, 283.1].

Однако в УК РФ пресекается распространение информации не только и не столько через Интернет, сколько различными способами, поэтому не всегда приведённые статьи будут уместны в рассматриваемом законодательном механизме. Тем не менее, следует отметить, что уголовно-правовая охрана информационной безопасности очень актуальна, с каждым годом тенденция к увеличению количества и появлению новых видов преступлений в этой сфере растет. Например, общий ущерб от вируса Wanna Cry (2017 г.) был оценен в 1 млрд $ (при этом в реальности ущерб, скорее всего, составил гораздо большую сумму, так как преступления в сфере компьютерной информации характеризуются высокой степенью латентности). Следует отметить, что чтобы заразить свой компьютер Wanna Cry пользователю даже не нужно было совершать какую-либо ошибку — кликать на подозрительную ссылку и т.д. Заразиться WannaCry можно было, вообще ничего не делая [18]. Вернее сказать, достаточно иметь открытый RDP-порт (использует протоколы удалённого рабочего стола), через который, просканировав, злодей устанавливает файл-шифровщик и получает доступ ко взломанной сети или отдельно взятому АРМ [19].

Проблема вирусов-вымогателей существует с 1980-х годов (вирус AIDS) и к 2018—2019 гг. стала особенно актуальной. Как правило, злоумышленниками движет стремление заполучить доступ к финансовым активам, причём не только и не столько банковского сектора и государственных компаний, сколько частных лиц. Последние зачастую не понимают, пренебрегают или не имеют достаточно средств для надлежащего уровня ИБ [20, 21]. Только за март 2019 года зафиксировано девять случаев разных вирусов-вымогателей, ориентированных на англоязычных пользователей, но с возможностью заражать АРМ по всему миру [21].

Бывает и так, хакеры действуют и в политических целях (скорее всего, на возмездной основе): например, 07.02.2019 г. кибератакам подверглись сайты как минимум девяти посольств Венесуэлы (и в России, в частности), вследствие чего на интернет-страницах дипломатических представительств появилась информация в поддержку лидера оппозиции Хуана Гуаидо, провозгласившего себя «временным президентом» Боливарианской республики [22].

Скорость развития информационных технологий обуславливает необходимость соответствующих изменений в законодательстве. С 01.01.2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который создал законодательную базу для дальнейших практических действий в этом направлении.

Следует отметить, что законодательно классификация информации, требующей ограничения или запрещения распространения, не очень конкретизируется. Наиболее детализированная классификация представлена в ст. 5 Федерального закона от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее — 436-ФЗ). 436-ФЗ устанавливает запрещённой для детей такую информацию, что может угрожать их физическому или психологическому здоровью, отрицать традиционные семейные ценности, кроме того, ограничению подлежит информация, вызывающая сильные негативные эмоции и т. д. Подобная информация способствует системным деформациям в духовно-нравственной сфере жизни ребенка, наносит вред правовому и нравственному воспитанию молодежи, пропагандирует насилие. Обе части приводимой статьи сходятся на ограничении и запрете демонстрирования межполовых отношений и нецензурной (или подобной ей) брани [5, ст. 5]. 436-ФЗ также содержит статью 12, где вводит возрастной ценз (0+, 6+, 12+, 16+, 18+) для ограничения детей от информации, не приемлемой им по возрасту [5, ст. 12]. Вместе с современным изложением федеральных законов № 126-ФЗ от 7 июля 2003 года «О связи» и 149-ФЗ в области, касающейся именно ограничения распространения информации в информационно-телекоммуникационной сети «Интернет» [3, ст. 2 п. 13–18, 15.1; 4, ст. 46], указанные положения считаются плацдармом для цензуры российского сегмента Интернета, или Рунета.

Существует «Единый реестр доменных имён…», где на основании упомянутых законов и подзаконных актов собраны сайты, IP-адреса и доменные имена, доступ к которым закрывает Интернет-провайдер по решению суда [3, ст. 1 ч. 2, 15.1–3; 4, ст. 46; 8, 13]. Немало внимания уделяется блокировке экстремистских, пиратских и порнографических сайтов [5, ст. 5; 6, ст. 8, 11], в том числе сетевых изданий, относящихся к средствам массовой информации [7; ст. 4, 59]. Однако введение подобного реестра запрещённых сайтов не полностью закрывает доступ к их содержимому, и остаются различные пути обхода существующих запретов, что поначалу делало всё предприятие едва ли не бессмысленным.

Законодательный механизм ограничения распространения информации в сети Интернет реализуется в разных странах по-разному. В США, родоначальнице интернета, также существуют законы об ограничении информации, но касаются они в первую очередь детей [14, 15]. В частности, согласно Закону о защите частной жизни несовершеннолетних, распространение информации частного характера о детях моложе 16 лет возможно лишь с согласия их родителей, кроме того, несовершеннолетние не могут иметь своего интернет-адреса, персонального канала и т. п. [16]. В стране также распространена практика идентифицированного доступа к сети Интернет посредством персонального ключа, позволяющего отслеживать интернет-активность пользователя.

Китайская Народная Республика демонстрирует гораздо более углубленный подход: правовое регулирование Интернета в КНР находится в компетенции сразу нескольких органов: отдела пропаганды Центрального комитета Коммунистической партии Китая (ЦК КПК), Министерства науки и технологий, Министерства общественной безопасности, а Комиссия по управлению киберпространством осуществляет мониторинг Интернета. К 2003 году в КНР была создана и введена в действие на всей территории (кроме специальных административных районов Гонконга и Макао) собственная система фильтрации. Официальное наименование системы — проект «Золотой щит», она же *Great Firewall of China*. Её основная цель — окружить пользователя исключительно идеологически правильной информацией, а также ограничить доступ к ряду иностранных сайтов (например, к международным социальным сетям) [17]. По состоянию на 2019 год в КНР заблокированы следующие ресурсы, популярные во всем мире: WhatsApp, Instagram, Google Search, Facebook, Twitter, The New York Times и т. д. При этом в КНР постепенно создает все свое: от национальных социальных сетей до национальных платежных сервисов.

Ограничение информации — вынужденная плата за обеспечение покоя граждан и безопасности государства. Специалисту по защите информации необходимо руководствоваться законодательством, касающимся ограничений распространения информации, чтобы эффективно применять в своей профессиональной деятельности организационные и технические меры для пресечения незаконного распространения сведений ограниченного характера.

Рассмотренный законодательный механизм направлен на ограничение информации, которая признана ограниченной или запрещённой, в информационно-телекоммуникационной сети «Интернет». Руководствуясь им, специалисты по защите информации могут внедрить нужные средства защиты информации в защищаемую сеть так, чтобы сформировать единый комплекс мер для обеспечения информационной безопасности.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс]: с учётом поправок, внесённых Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ. — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 26.01.2019).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ [Электронный ресурс]: ред. от 27.12.2018 (с изм. и доп., вступ. в силу с 08.01.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 26.01.2019).

3. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федер. закон Рос. Федерации от 27.07.2006 N 149-ФЗ (ред. от 18.12.2018). — Справочно-правовая

система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 26.01.2019).

4. О связи [Электронный ресурс]: федер. закон Рос. Федерации от 07.07.2003 N 126-ФЗ (ред. от 27.12.2018). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_43224/ (дата обращения: 26.01.2019).

5. О защите детей от информации, причиняющей вред их здоровью и развитию [Электронный ресурс]: федер. закон Рос. Федерации от 29.12.2010 N 436-ФЗ (ред. от 01.05.2017). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_ 108808/ (дата обращения: 26.01.2019).

6. О противодействии экстремистской деятельности [Электронный ресурс]: федер. закон Рос. Федерации от 25.07.2002 N 114-ФЗ (ред. от 23.11.2015). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 26.01.2019).

7. О средствах массовой информации [Электронный ресурс]: закон Рос. Федерации от 27.12.1991 N 2124-1 (ред. от 18.04.2018, с изм. от 17.01.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения: 26.01.2019).

8. О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети „Интернет“ и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети „Интернет“, содержащие информацию, распространение которой в Российской Федерации запрещено» [Электронный ресурс]: постановление Правительства Рос. Федерации от 26.10.2012 N 1101 (ред. от 05.06.2018). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/ document/cons_doc_LAW_137077/ (дата обращения: 26.01.2019).

9. О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: проект федер. закона Рос. Федерации N 606593-7 (окончательная ред., принятая ГД ФС РФ 07.03.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi? req=doc;base=PRJ ;n=182225#0809725137804495 (дата обращения: 19.03.2019).

10. О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: проект федер. закона Рос. Федерации N 606594-7 (окончательная ред., принятая ГД ФС РФ 07.03.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ; n=182226#07408838839465 (дата обращения: 19.03.2019).

11. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: проект федер. закона Рос. Федерации N 606595-7 (окончательная ред., принятая ГД ФС РФ 07.03.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=182227#07386656188058517 (дата обращения: 19.03.2019).

12. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: проект федер. закона Рос. Федерации N 606596-7 (окончательная ред., принятая ГД ФС РФ 07.03.2019). — Справочно-правовая система «Консультант Плюс». — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=182228#034604824511561416 (дата обращения: 19.03.2019).

13. Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено [Электронный ресурс]: Роскомнадзор. — Электрон. текстовые дан. — Москва [б.и.], 2018. — Режим доступа: https://eais.rkn.gov.ru/ (дата обращения: 26.01.2019).

14. Children's Online Privacy Protection Rule [Электронный ресурс]: федер. закон США от 21.04.2000 (ред. от 17.01.2013). — Federal Trade Commission. — Режим доступа: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (дата обращения: 26.01.2019).

15. Children's Internet Protection Act [Электронный ресурс]: федер. закон США от 21.12.2000. — Internet Free Expression Alliance. — Режим доступа: http://ifea.net/cipa.pdf (дата обращения: 26.01.2019).

16. Federal Trade Commission Enforcement Policy Statement Regarding the Applicability of the Children's Online Privacy Protection Act Rule to the Collection and Use of Voice Recordings [Электронный ресурс]: заявление о правоприменительной политике США от 20.10.2017. — Federal Trade Commission. — Режим доступа: https://www.ftc.gov/public-statements/2017/10/federal-trade-commission-enforcement-policy-statement-regarding (дата обращения: 17.03.2019).

17. 国网络安全 (О кибербезопасности) [Электронный ресурс]: закон Китайской Народной Республики от 07.11.2016. — The National People's Congress of the People's Republic of China. — Режим доступа: http://www.npc.gov.cn/ npc/xinwen/2016-11/07/content_2001605.htm (дата обращения: 26.01.2019).

18. Блог Лаборатории Касперского [Электронный ресурс]: Эпидемия шифровальщика WannaCry: что произошло и как защититься / А. Перекатин. — Москва, 2017. — Режим доступа: https://www.kaspersky.ru/blog/wannacry-ransomware/16147/ (дата обращения: 28.01.2019).

19. Зотов, С. С. Анализ концепций распространения вирусов-вымогателей / С. С. Зотов, А. С. Лысак // Аллея науки. — 2017. — Т. 1. — № 11. — С. 32–36.

20. Жук, М. А. Анализ масштабности кибератак XXI века и их географическая картина / М. А. Жук, И. П. Миллер // Фундаментальные и прикладные исследования молодых учёных: сборник научных трудов II Международной научно-практической конференции студентов, аспирантов и молодых учёных 08-09 февраля 2018 г. — Омск: СибАДИ, 2018. — С. 491–497.

21. Blogspot [Электронный ресурс]: Шифровальщики-вымогатели / А. Иванов. — Режим доступа: http://id-ransomware.blogspot.com/ (дата обращения: 17.03.2019).

22. РИА Новости [Электронный ресурс]: Сайты посольств Венесуэлы в ряде стран не доступны из-за кибератаки. — Москва, 2019. — Режим доступа: https://ria.ru/20190207/1550563663.html (дата обращения: 17.03.2019).

References

1. Konstitutsiya Rossiyskoy Federatsii (prinyata vsenarodnym golosovaniem 12.12.1993): s uchetom popravok, vnesennykh Zakonami RF o popravkakh k Konstitutsii RF ot 30.12.2008 N 6-FKZ, ot 30.12.2008 N 7-FKZ, ot 05.02.2014 N 2-FKZ, ot 21.07.2014 N 11-FKZ [Constitution of the Russian Federation (passed by referendum at 12.12.1993: as amended by the RF Amendment Acts 6-FCL dd. 30.12.2008, 7-FCL dd. 30.12.2008, 2-FCL dd. 05.02.2014, 11-FCL dd. 21.07.2014]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_ 28399/ (accessed 26 January 2019).

2. Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 N 63-FZ: red. ot 27.12.2018 (s izm. i dop., vstup. v silu s 08.01.2019) [the Criminal Code of the Russian Federation 63-FL dd. 13.06.1996: revised 19.02.2018 as am. eff. of 08.01.2019]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_ 10699/ (accessed 26 January 2019).

3. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: feder. zakon Ros. Federatsii ot 27.07.2006 N 149-FZ (red. ot 18.12.2018) [On Information, Information Technologies and the Protection of Information: feder. law of the Rus. Federation 149-FL dd. 27.07.2006 (revised 18.12.2018)]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61798/ (accessed 26 January 2019).

4. O svyazi: feder. zakon Ros. Federatsii ot 07.07.2003 N 126-FZ (red. ot 27.12.2018) [Concerning Communications: law of the Rus. Fedeation 126-FL dd. 07.07.2003 (revised 27.12.2018)]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_43224/ (accessed 26 January 2019).

5. O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorov'yu i razvitiyu: feder. zakon Ros. Federatsii ot 29.12.2010 N 436-FZ (red. ot 01.05.2017) [On Protection of Children from Information Harmful to Their Health and Development: feder. law of the Rus. Federation 436-FL dd. 29.12.2010 (revised 01.05.2017)]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_ 108808/ (accessed 26 January 2019).

6. O protivodeystvii ekstremistskoy deyatel'nosti: feder. zakon Ros. Federatsii ot 25.07.2002 N 114-FZ (red. ot 23.11.2015) [On Countering Extremist Activities: feder. law of the Rus. Federation 114-FL dd. 25.07.2002 (revised 23.11.2015)]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_ 37867/ (accessed 26 January 2019).

7. O sredstvakh massovoy informatsii: zakon Ros. Federatsii ot 27.12.1991 N 2124-1 (red. ot 18.04.2018, s izm. ot 17.01.2019) [Concerning Mass Media: the Law of Rus. Federation 2124-1 dd. 27.12.1991 (revised 18.04.2018 as am. on 17.01.2019). — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/ cons_doc_LAW_1511/ (accessed 26 January 2019).

8. O edinoy avtomatizirovannoy informatsionnoy sisteme "Edinyy reestr domennykh imen, ukazateley stranits saytov v informatsionno-telekommunikatsionnoy seti 'Internet' i setevykh adresov, pozvolyayushchikh identifitsirovat' sayty v informatsionno-telekommunikatsionnoy seti 'Internet', soderzhashchie informatsiyu, rasprostranenie kotoroy v Rossiyskoy Federatsii zapreshcheno": postanovlenie Pravitel'stva Ros. Federatsii ot 26.10.2012 N 1101 (red. ot 05.06.2018) [On the Unified Automated Information

System "The Unified Register of Domain Names, Uniform Resource Locators Which Allow to Identify Websites Containing Information That Is Prohibited to Be Distributed in the Russian Federation": decree of the Government of the Rus. Federation 1101 dd. 26.10.2012 (revised 05.06.2018)]. — Spravochno-pravovaya sistema "Konsul'tant Plyus" [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/document/cons_doc_LAW_ 137077/ (accessed 26 January 2019).

9. O vnesenii izmenenij v stat'ju 15.3 Federal'nogo zakona Ob informacii, informacionnyh tehnologijah i o zashhite informacii: proekt feder. zakona Ros. Federatsii N 606593-7 (okonchatel'naja red., prinjataja GD FS RF 07.03.2019) [Concerning the Introduction of an Amendment to Article 15.3 of the Federal Law On Information, Information Technologies and the Protection of Information: draft feder. law of the Rus. Federation 606593-7 (final text passed by the State Duma of the RF 07.03.2019)]. — Spravochno-pravovaja sistema «Konsul'tant Pljus» [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/cons/cgi/online.cgi? req=doc;base=PRJ;n=182225#0809725137804495 (accessed 19 March 2019).

10. O vnesenii izmenenija v Federal'nyj zakon Ob informacii, informacionnyh tehnologijah i o zashhite informacii: proekt feder. zakona Ros. Federatsii N 606594-7 (okonchatel'naja red., prinjataja GD FS RF 07.03.2019) [On Amendment Being Made to the Federal Law On Information, Information Technologies and the Protection of Information: draft feder. law of the Rus. Federation 606594-7 (final text passed by the State Duma of the RF 07.03.2019)]. — Spravochno-pravovaja sistema «Konsul'tant Pljus» [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=182226#07408838839465 (accessed 19 March 2019).

11. O vnesenii izmenenij v Kodeks Rossijskoj Federacii ob administrativnyh pravonarushenijah: proekt feder. zakona Ros. Federatsii N 606595-7 (okonchatel'naja red., prinjataja GD FS RF 07.03.2019) [On Amendments Being Made to the Code of the Russian Federation on Administrative Offenses: draft feder. law of the Rus. Federation 606595-7 (final text passed by the State Duma of the RF 07.03.2019)]. — Spravochno-pravovaja sistema «Konsul'tant Pljus» [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base= PRJ;n=182227#07386656188058517 (accessed 19 March 2019).

12. O vnesenii izmenenij v Kodeks Rossijskoj Federacii ob administrativnyh pravonarushenijah: proekt feder. zakona Ros. Federatsii N 606596-7 (okonchatel'naja red., prinjataja GD FS RF 07.03.2019) [On Amendments Being Made to the Code of the Russian Federation on Administrative Offenses: draft feder. law of the Rus. Federation 606596-7 (final text passed by the State Duma of the RF 07.03.2019)]. — Spravochno-pravovaja sistema «Konsul'tant Pljus» [Consultant Plus Legal Reference System]. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base= PRJ;n=182228#034604824511561416 (accessed 19 March 2019).

13. Edinyy reestr domennykh imen, ukazateley stranits saytov v seti "Internet" i setevykh adresov, pozvolyayushchikh identifitsirovat' sayty v seti "Internet", soderzhashchie informatsiyu, rasprostranenie kotoroy v Rossiyskoy Federatsii zapreshcheno: Roskomnadzor [The Unified Register of Domain Names, Uniform Resource Locators Which Allow to Identify Websites Containing Information That Is Prohibited to Be Distributed in the Russian Federation: Roskomnadzor] (2018). Available at: https://eais.rkn.gov.ru/ (accessed 26 January 2019).

14. Children's Online Privacy Protection Rule: US federal act dd. 21.04.2000 (revised 17.01.2013). — Federal Trade Commission (2019). Available at: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/ childrens-online-privacy-protection-rule (accessed 26 January 2019).

15. Children's Internet Protection Act: US federal act dd. 21.12.2000. — Internet Free Expression Alliance (2019). Available at: http://ifea.net/cipa.pdf (accessed 26 January 2019).

16. Federal Trade Commission Enforcement Policy Statement Regarding the Applicability of the Children's Online Privacy Protection Act Rule to the Collection and Use of Voice Recordings dd. 20.10.2017. — Federal Trade Commission (2019). — Available at: https://www.ftc.gov/public-statements/2017/10/federal-trade-commission-enforcement-policy-statement-regarding (accessed 17 March 2019).

17. 国网络安全 [Concerning Cybersecurity]: the law of People's Republic of China dd. 07.11.2016. — The National People's Congress of the People's Republic of China (2019). Available at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (accessed 26 January 2019).

18. Kaspersky Lab Daily: Jepidemija shifroval'shhika WannaCry: chto proizoshlo i kak zashhitit'sja [Epidemic of WannaCry Ransomware: What's Happened And How to Protect Your Assets] (2017) / Alex Perekatin. Available at: https://www.kaspersky.ru/blog/wannacry-ransomware/16147/ (accessed 28 January 2019).

19. Zotov S. S., Lysak A. S. Analiz kontseptsiy rasprostraneniya virusov-vymogateley [Analysis of the concepts of the propagation of ransomware]. Alleya nauki [Alley of Science], 2017, vol. 1, no. 11, pp. 32–36.

20. Zhuk M. A., Miller I. P. Analiz masshtabnosti kiberatak XXI veka i ikh geograficheskaya kartina [Analysis of the scale of cyberattacks in the XXI century and their geographical representation]. Fundamental'nye i prikladnye issledovaniya molodykh uchenykh: sbornik nauchnykh trudov II Mezhdunarodnoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh

[Fundamental and applied research of young scientists: collection of scientific works by the materials of the II International Scientific & Practical Conference of Students, Postgraduates and Young Scientists] 08-09 February 2018, pp. 491–497.

21. Blogspot: Shifroval'shhiki-vymogateli [Cryptoware] / A. Ivanov (2019). — Available at: http://id-ransomware.blogspot.com/ (accessed 17 March 2019).

22. RIA Novosti [RIA News]: Sajty posol'stv Venesujely v rjade stran ne dostupny iz-za kiberataki [The websites of the Venezuelan embassies in some countries are not available due to cyberattacks] (2019). — Available at: https://ria.ru/20190207/1550563663.html (accessed 17 March 2019).

ДОБКАЧ Леонид Яковлевич, студент группы ИУ8-121, кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н.Э. Баумана. 105005, Россия, Москва, 2-я Бауманская ул., д. 5. E-mail: dobkachleo@mail.ru

ТАРАПАНОВА Елена Александровна, доцент кафедры ИУ10 «Защита информации», Московский государственный технический университет им. Н.Э. Баумана, к.ф.н. 105005, Россия, Москва, 2-я Бауманская ул., д. 5. E-mail: tarapanova@bmstu.ru

DOBKACZ Leonid Yakovlevich, student of IU8-121 group, IU8 Information security department, Bauman MSTU. Bld. 5, 2nd Baumanskaya st., Moscow, Russia, 105005. E-mail: dobkachleo@mail.ru

TARAPANOVA Elena Alexandrovna, docent of Bauman MSTU's IU10 Information protection department, Cand. sc. phil. Bld. 5, 2nd Baumanskaya st., Moscow, Russia, 105005. E-mail: tarapanova@bmstu.ru