УДК 341.64

Информационно-коммуникационные технологии в свете казахстанского, российского и международного права

***Сарсембаев Марат Алдангорович,* главный научный исследователь, Институт законодательства и правовой информации Республики Казахстан, доктор юридических наук, профессор**

daneker@mail.ru

Аннотация: Данная статья посвящена анализу ряда аспектов информационно-коммуникационных технологий с точки зрения казахстанского права, российского права и общего для обеих стран международного права. Эта тема автором выбрана потому, что проблемы информационно-коммуникационных технологий являются актуальными и требуют оперативного решения, в том числе с помощью правовых средств. Автор приводит законодательные акты Казахстана и России по теме этих технологий и обосновывает необходимость разработки и принятия новых казахстанских и российских законодательных актов в этой же сфере. Автором данной статьи предпринята попытка предложить к разработке и принятию новых универсальных международных многосторонних конвенций, посредством которых нужно решать проблемы информационно-коммуникационных технологий и связанных с ними прав человека в масштабе мирового сообщества. ***Ключевые слова:*** информационно-коммуникационные технологии, Интернет, смартфон, мобильная связь, волоконно-оптический кабель, средства коммуникаций, информационно-коммуникационное право.

UDC 341.64

Information-communication technologies in the light of Kazakhstan, Russian and international law

Sarsembayev Marat Aldangorovich, ***chief scientific researcher, Institute of Legislation and Legal Information of the Republic of Kazakhstan, doctor of sciences (law), professor***

daneker@mail.ru

Annotation: This article is devoted to the analysis of a number of aspects of information and communication technologies from the point of view of Kazakh law, Russian law and international law common to both countries. This topic was chosen by the author because the problems of information and communication technologies are relevant and require prompt solutions, including through legal means. The author cites the legislative acts of Kazakhstan and Russia on the topic of these technologies and justifies the need to develop and adopt new Kazakh and Russian legislative acts in the same area. The author of this article attempts to propose the development and adoption of new universal international multilateral conventions, through which it is necessary to solve the problems of information and communication technologies and related human rights on the scale of the world community. ***Keywords:*** information and communication technologies, Internet, smartphone, mobile communication, fiber-optic cable, means of communication, information and communication law.

Введение. Вносящих серьезный вклад в развитие трендов информационно-коммуникационных технологий на планете немного: примерно 17–18 стран. Первые места в мировом

ранжированном рейтинге информационных технологий из 176 стран по последним данным 2017 года заняли Исландия, Южная Корея, Швейцария.

Исландии присудили первое место в мировом рейтинге потому, что она обладает превосходным Интернетом. К тому же это островное государство имеет громадное количество волоконно-оптических кабелей на каждую душу исландского населения. 78 процентов исландских домохозяйств входят в сеть Интернет. Каждому исландцу предоставлен доступ к трем сетям высоких технологий. Исландцы так умеют оперативно и грамотно работать с компьютером, что смогли достичь автоматизированных навыков программирования, их знания, умения и навыки в сфере компьютерного дела оценивают как самые высокие в Европе.

Занимающая второе место в мировом рейтинге Южная Корея, представляет собой государство, народ которого в совокупности является чрезвычайно продвинутым в сфере использования Интернета и огромного числа смартфонов. Количество собственников мобильных телефонов составляет 94 процента от всей численности населения данной республики. Интернет в Республике Корея является практически самым быстрым на планете. Более того, телекоммуникационные компании страны планируют еще больше увеличить скорость Интернета.

Третье место в данном мировом рейтинге отведено Швейцарии. Сравнительно недавно коммуникационные компании этой страны заплатили 380 миллионов швейцарских франков за получение доступа к мегагерцовым частотам в целях обеспечения связи в режиме 5G. К тому же в этой стране планируют создать 6G-сети. Это станет рекордным достижением, но предварительно надо исследовать, насколько эти высокие частоты безопасны для населения и окружающей человека среды.

Хотя Япония не входит в состав тройки самых продвинутых стран, тем не менее она входит в десятку лучших государств в мире по вопросам информационно-коммуникационных технологий. В 2019 году было отмечено, что эта страна стала самой ведущей страной в вопросах информационных технологий. По численности интернет-кабелей на душу населения Японии удалось выйти на третье место в мире. Согласно утверждениям экспертов Союза электросвязи, рядовой японец умеет так быстро решать возникающие в мировой Интернет-паутине проблемы, что по этому показателю обходит среднестатистического жителя стран Европы. Кроме того, в программировании японцам практически нет равных, но они несколько уступают жителям Люксембурга и Объединенных Арабских Эмиратов [1].

Нам, конечно, интересно узнать, каковы показатели по исследуемым вопросам у стран СНГ, в том числе России и Казахстана. Среди стран Содружества Россия занимает второе место (в мировом рейтинге — 45 место с 7,07 балла), Казахстан идет на третьем месте (в рейтинге — 52 место с 6,79 балла). Первое место принадлежит Республике Беларусь (в мировом рейтинге ей отвели 32 место, присудив 7,55 балла). Остальные страны СНГ

расположились в следующей последовательности: Молдова — 59 место (6,45 балла), Азербайджан — 65 (6,20), Армения — 75 (5,76), Украина — 79 (5,62), Узбекистан — 95 (4,90), Кыргызстан — 109 место (4,37). Таджикистана и Туркменистана в рейтинге нет. Из всех постсоветских государств лучшим в информационно-коммуникационных технологиях зарекомендовала себя Эстония, которая находится в этом рейтинге на 17 месте сразу после США и которая обошла Сингапур, Австрию, Финляндию, Израиль, Бельгию, Канаду (вот вам якобы медлительные эстонские парни) [2]. Нам, специалистам из стран СНГ, следует поучиться в Эстонии этому делу на всем нам доступном и понятном русском языке.

В настоящее время в мире информационно-коммуникационным технологиям принадлежит весомая роль в развитии экономики, управления, науки, культуры, так как они представляют собой процессы и методы взаимодействия с информацией, которые применяются посредством устройств вычислительной техники, к которым относятся компьютеры, а также средства коммуникаций. Следует отметить, что не менее 40 процентов населения планеты имеют доступ к Интернету как глобальной информационной сети, а каждый 7 из 10 домохозяйств обладает мобильным телефоном с выходом в эту сеть. 4,8 миллиарда человек ежедневно используют Интернет. Не менее 98 процентов людей от всей численности населения Дании, Исландии, Катара и Кувейта имеют Интернет. 306,4 миллиарда электронных писем находят своих адресатов каждый день. Благодаря цифровым информационным технологиям граждане, представители бизнеса получили прямой доступ к государственным услугам, имеют возможность более ускоренного обмена информацией, а также возможность создания новых цифровых информационно-коммуникационных продуктов. Электронные носители информации заменяют бумажный документооборот. Безбумажный документооборот сегодня активно внедрен в образовательной сфере (в том числе вследствие пандемии), в транспортной, таможенной, налоговой и иных сферах.

Аспекты информационно-коммуникационных технологий в казахстанском и российском праве и совершенствование законодательства в обеих странах. В казахстанском законодательстве есть достаточно широкие гарантии доступности граждан к информации. Так, в законе Республики Казахстан от 16 ноября 2015 года «О доступе к информации» содержится норма о транспарентности информации по многим направлениям деятельности как центральных, так и местных государственных органов. Было бы желательно, чтобы казахстанские государственные органы чаще обновляли информацию о своей деятельности на своих интернет-ресурсах. При осуществлении механизмов защиты прав человека особую роль обретают информационные технологии, в том числе онлайн-петиции. Существенный интерес представляет статья 4 Федерального закона России от 9 февраля 2009 года N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», в котором достаточно

четко сформулированы, в частности, такие принципы обеспечения доступа к информации о деятельности государственных органов, как: «открытость и доступность информации о деятельности государственных органов и органов местного самоуправления, за исключением случаев, предусмотренных федеральным законом»; «свобода поиска, получения, передачи и распространения информации о деятельности государственных органов и органов местного самоуправления любым законным способом».

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года, утвержденная распоряжением Правительства Российской Федерации от 1 ноября 2013 года N 2036-р, предусматривая состояние и перспективы направления отраслей информационных технологий, обозначила роль информационных технологий в экономике государства, определила цели, задачи, принципы отрасли информационных технологий, указала направления международного сотрудничества в этой сфере, сформулировала ожидаемые результаты реализации этого стратегического документа [3]. В Казахстане действовала Программа «Информационный Казахстан-2020», которая в целом была реализована, но, к сожалению, не была принята новая программа или стратегия по вопросам развития информационно-коммуникационных технологий на перспективу. Было бы целесообразно разработать новый стратегический документ, в котором могли бы найти отражение идеи тех или иных положений российской Стратегии развития отрасли информационных технологий.

В России предпринята попытка формулирования Концепции развития законодательства в области разработки и применения информационно-коммуникационных технологий в Российской Федерации, в которой определены задачи Концепции, состояние правового регулирования как разработки, так и применения информационно-коммуникационных технологий в России, определены принципы, механизмы правового регулирования, стратегическое направление правового регулирования этих технологий, сформулированы направления совершенствования законодательства в сфере разработки, принятия и применения информационных технологий на всей территории России, приведены названия законодательных и иных нормативных актов, которые необходимо разработать и принять, а также акты об информации и коммуникациях, подлежащие изменению и (или) отмене. Посредством такой Концепции целесообразно разработать и обсудить проекты необходимых законов, нормативных правовых актов, имеющих отношение к информационно-коммуникационным технологиям в целях их принятия российским законодателем [4]. Аналогичную Концепцию по информационно-коммуникационным технологиям могли бы разработать ученые-юристы Казахстана.

Новое образование в наших странах должно быть нацелено на обретение умений и навыков в процессе творческого анализа информации и развития креативного мышления. В частности, следует делать более насыщенным

содержание программ учебных заведений таких учебных предметов, как: *«Основы программирования»*, *«Информатика в профессиональной деятельности»*, *«Информационно-коммуникационные технологии»* по всем специальностям. Причем наши преподаватели должны научить учащихся и студентов автоматическому печатанию на клавиатуре компьютера на русском и английском языках, умению составлять творческие программы, оперативно выявлять и нейтрализовывать электронные «вирусы», быстро блокировать действия хакеров и обнаруживать их, четко лавировать в Интернет-сети, моментально решать возникшие электронно-компьютерные проблемы. Учебные заведения наших стран всем учащимся и студентам должны обеспечивать более широкие информационно-коммуникационные условия для реализации ими своего права на образование. Этому может, в частности, содействовать учебник проф. О. П. Новожилова «Информатика», где четко расписаны понятия компьютерных сетей, программного обеспечения, компьютерного моделирования устройств цифровой обработки информации [5, с. 83, 144, 252–257]. В этой связи необходимо ввести в качестве отдельных разделов *«О совершенствовании качества преподавания предметов по информатике и программированию»* и *«О временном и постоянном дистанционном обучении»* в тексты законов об образовании: в Закон Республики Казахстан от 27 июля 2007 года «Об образовании», в Федеральный закон от 29 декабря 2012 года N 273-ФЗ «Об образовании в Российской Федерации».

Концепция кибербезопасности (Киберщит Казахстана), утвержденная правительственным постановлением Республики Казахстан от 30 июня 2017 года как акт «мягкого права», говорит о необходимости установления и обеспечения реальной кибербезопасности. Под кибербезопасностью понимается совокупность методов и практических мер по защите компьютеров, серверов, мобильных устройств, электронных систем, цифровизированных сетей и различных данных от атак злоумышленников, хакеров, кракеров (взломщиков сайтов). Более подробно о кибербезопасности можно узнать в исследованиях А. А. Внукова [6, с. 20–21], С. Смита [7, p. 71], Д. У. Хаббарда [8, p. 7–9].

Здесь следует подчеркнуть, что ежедневно фиксируются и отражаются миллионы хакерских атак в Интернете. Ежедневному взлому подвергаются не менее 30 тысяч веб-сайтов. В этой связи необходимо осуществление ответных мероприятий в целях обеспечения компьютерной безопасности государственных органов, юридических и физических лиц. В России Концепция стратегии кибербезопасности Российской Федерации существует пока в проектном формате. Желательно как можно скорее обсудить и принять Стратегию кибербезопасности России, что особенно важно в нынешнее время.

В наших странах сравнительно немного вузов, в которых готовят выпускников, которые специализируются в вопросах обеспечения и укрепления компьютерной безопасности. В Казахстане, например, надо создавать дополнительные организационно-правовые и

управленческие механизмы, с помощью которых можно решать проблемы кибербезопасности. Государства для успешной борьбы с преступлениями в Интернете могли бы увеличить количество вузов по подготовке специалистов по кибербезопасности. Каждая страна могла бы формировать высококвалифицированные отряды киберполицейских, которые могли бы отслеживать и привлекать к ответственности хакеров всех мастей, кибермошенников и воров, развратителей, специализирующихся в сфере проституции и порнографии, в том числе детской проституции и порнографии, лиц, совершающих самые разные преступления с помощью информационно-коммуникационных технологий.

В Интернете члены мирового сообщества, в том числе Россия и Казахстан, должны по максимуму создавать и обеспечивать условия людям, гражданам всех стран для реализации их права на свободу слова, свободу выражения мнений, права на распространение практически любой информации. Вместе с тем есть определенные виды информации, которые не могут быть распространены в Интернете: это — пропаганда межличностной ненависти, пропаганда войны, призывы к свержению существующего в стране государственного строя, пропаганда наркотических и психотропных веществ, пропаганда аморальных, преступных действий и некоторые другие категории информации. Поэтому государства должны противостоять таким действиям и пропаганде как внутри страны, так и посредством объединения своих усилий на международном уровне [9; 10, с. 78–80].

Юридической основой имплементации информационных концептуальных и стратегических программ, конституционных положений России и Казахстана по вопросам информационной безопасности и информационно-коммуникационных технологий стали нижеследующие законы: Закон Республики Казахстан от 24 ноября 2015 года *«Об информатизации»*, Федеральный закон Российской Федерации *«Об информации, информационных технологиях и о защите информации»* от 27 июля 2006 года N 149-ФЗ; Закон Республики Казахстан от 7 января 2003 года *«Об электронном документе и электронной цифровой подписи»*, Федеральный закон от 10 января 2002 года N 1-ФЗ *«Об электронной цифровой подписи»*; Закон Республики Казахстан от 21 мая 2013 года *«О персональных данных и их защите»*, Федеральный закон от 27 июля 2006 года N 152-ФЗ *«О персональных данных»*; Закон Республики Казахстан от 16 ноября 2015 года *«О доступе к информации»*, Федеральный закон от 9 февраля 2009 года N 8-ФЗ *«Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»*; Закон Республики Казахстан от 5 июля 2004 года *«О связи»*, Федеральный закон от 7 июля 2003 года N 126-ФЗ *«О связи»*; Закон Республики Казахстан от 6 января 2012 года *«О национальной безопасности Республики Казахстан»*, Федеральный закон от 28 декабря 2010 года N 390-ФЗ *«О безопасности»*; Закон Республики Казахстан от 13 июля 1999 года *«О противодействии терроризму»*, Федеральный закон от 6 марта

2006 года N 35-ФЗ *«О противодействии терроризму»* [11, с. 297–298; 12, с. 31–32, 156, 431]. В России приняты Федеральный закон от 22 декабря 2008 года N 262-ФЗ *«Об обеспечении доступа к информации о деятельности судов в Российской Федерации»*, Федеральный закон от 29 декабря 2010 года N 436-ФЗ *«О защите детей от информации, причиняющей вред их здоровью и развитию»*. Казахстану целесообразно присмотреться к этим российским законам на предмет возможного их заимствования казахстанским законодателем.

Уголовный кодекс Российской Федерации содержит в себе раздел 28 «Преступления в сфере компьютерной информации», в котором предусмотрен целый ряд статей, устанавливающих уголовную ответственность за те или иные виды компьютерных преступлений. В Уголовном кодексе Республики Казахстан есть отдельная глава со статьями о наказании преступлений, которые могут совершаться в сфере информатизации и связи. За совершение виновными лицами десятков преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций предусматривается уголовная ответственность. В Кодексе Республики Казахстан об административных правонарушениях, а также в Кодексе Российской Федерации об административных правонарушениях имеются составы административных правонарушений в связи с нарушением требований по эксплуатации средств защиты электронных информационных ресурсов, невыполнением Единых требований, неосуществлением или ненадлежащим осуществлением собственником или владельцем информационных систем, содержащих персональные данные, нарушением правил защиты информации, незаконной деятельностью в области защиты информации, разглашения информации с ограниченным доступом, неисполнением оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», за совершение которых предусмотрены меры административной ответственности. Благодаря приведенным выше законам и кодексам нашим странам удается в определенной мере урегулировать вопросы и проблемы информационно-коммуникационных технологий. В порядке совершенствования этого законодательства было бы желательно разработать и принять внутри наших стран новые законы на темы: *«Об ответственности за несоблюдение и ненадлежащее соблюдение прав и свобод человека и гражданина, реализуемых в формате офлайн и онлайн»*, *«О соблюдении прав человека, граждан (Республики Казахстан, Российской Федерации) в Интернете, в цифровизированном формате»*, *«О механизме оказания скорой электронной информационно-коммуникационной помощи»*.

Киберпространство — под защиту международного права. В рамках ООН приняты такие международные документы, как: *Глобальная программа кибербезопасности специализированного учреждения ООН* Международного союза электросвязи, *Резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших*

информационных инфраструктур» и другие более 30 резолютивных и организационных документов ООН. В этих документах закреплена необходимость безопасного применения информационно-коммуникационных технологий для обеспечения «неприкосновенности частной жизни, конфиденциальности, целостности и доступности информации в электронной форме», «защиты критической информационно-коммуникационной инфраструктуры, а также Интернета (доступно на: http://iisc.kz). Эти источники имеют рекомендательный характер. Вместе с тем их значимость состоит в том, что они определяют общее международно-политическое направление движения в отношении понимания цифровизированных прав человека, становятся логической основой элементов содержания будущих юридически обязательных международных конвенций, соглашений на эту же тему.

Международно-правовые документы в виде К*онвенции о доступе к информации, участию общественности в процессе принятия решений и доступе к правосудию по вопросам, касающимся окружающей среды*, (Орхусской конвенции) от 25 июня 1998 года (Казахстан ратифицировал эту Конвенцию на основании своего Закона от 23 октября 2000 года), *Конвенции о преступности в сфере компьютерной информации* от 23 ноября 2001 года, *Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных* от 28 января 1981 года (Россия — участница данной Конвенции), *Конвенции об информационном и правовом сотрудничестве, касающемся «услуг информационного общества»* от 4 октября 2001 года, *Конвенции Совета Европы по киберпреступности* от 23 декабря 2001 года, *Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации* от 1 июня 2001 года, *Соглашения между правительствами государств — членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности* от 16 июня 2009 года призваны защищать соответствующие аспекты информационно-цифровизированных прав человека. Аналитическая проработка приведенных источников международного информационно-коммуникационного права дана в научных исследованиях Р. Бахана, Н. Цагоуриса [13], А. А. Данельяна, Е. Е. Гуляева [14, с. 44–45], Т. М. Смысловой [15, с. 20, 23, 45, 50], в работе ООН о киберпреступности [16, с. 4, 16–18], в коллективной монографии ученых Кембриджского университета о кибероперациях в международном праве [17, p. 193–194, 343].

Как видим, Казахстан является официальным участником Орхусской конвенции, Российская Федерация стала участницей Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, и оба наших государства приняли на себя обязательства, вытекающие из Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями

в сфере компьютерной информации и Соглашения ШОС о сотрудничестве в области обеспечения международной информационной безопасности. При этом возникает вопрос, почему Россия и Казахстан не являются участниками других европейских конвенций по информационно-коммуникационным, компьютерным вопросам.

Исходя из положений Окинавской хартии глобального информационного общества 2000 года, Декларации принципов «Построение информационного общества — глобальная задача в новом тысячелетии», а также Совместного заявления стран СНГ по развитию информационного общества (Санкт-Петербургской декларации) 2003 года Россия и Казахстан могли бы решить для себя вопрос о возможном присоединении к Конвенции об информационном и правовом сотрудничестве, касающемся «услуг информационного общества». В русле этой идеи есть смысл поддержать предложение авторов исследования «Международное информационное право»: «Представляется, что в развитие статьи 19 Международного пакта о гражданских и политических правах 1966 года применительно к развитию информационного общества необходимо принять *конвенцию о всеобщем доступе к ИКТ (информационно-коммуникационным технологиям)*. В конвенции следует предусмотреть как общее правило доступа, так и категории бесплатной информации, а также категории социально уязвимых лиц, которым должен предоставляться бесплатный доступ» (доступно на: https://be5.biz).

Российская Федерация решила пока не присоединяться к *Конвенции Совета Европы по киберпреступности* от 23 декабря 2001 года. Она примет решение о присоединении к данной Конвенции, если будут пересмотрены положения пункта «b» статьи 32 данного международно-правового документа. В нынешнем виде эти положения Конвенции «могут причинить ущерб суверенитету и безопасности государств-участников Конвенции и правам их граждан». Из данного пункта вытекает, что «Сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их». А это Россию не устраивает. Нужно исходить из того, что киберпреступления в целом ряде стран наносят ущерб в миллиардах долларов имущественным интересам граждан, корпораций и государств. Поэтому возникшую правовую ситуацию можно разрешить следующим образом. Россия может воспользоваться статьей 42 Конвенции, которая дает ей право на оговорку. С помощью этого международно-правового института Россия могла бы заявить о том, что она оговаривает свое нежелание брать на себя обязательства пункта «b» статьи 32, остальные статьи, считая их правомерными, согласна ратифицировать Конвенцию. Затем, став официальным участником Конвенции, Россия могла бы поставить вопрос о корректировке положений пункта «b» статьи 32 Конвенции. Надо полагать, что эти подходы известны российским юристам: здесь скорее всего примешиваются политические отношения.

Поскольку Казахстан не является членом Совета Европы, ему гораздо сложнее рассчитывать на вхождение в число участников европейских конвенций. В этой связи Казахстан хотел бы надеяться на помощь России в решении вопроса о присоединении к европейским конвенциям, поскольку Россия является официальным членом Совета Европы. Казахстан и Россия могли бы разработать и принять для себя внутренние законы, исходя из тематики и содержания приведенных выше международно-правовых документов.

Если наши малые дети и подростки информационно-коммуникационным технологиям обучаются в учебных заведениях, то все взрослое население должно быть охвачено обучением этим технологиям по месту работы и по месту жительства. В этой связи в каждой стране, в том числе Казахстане, России может быть принят закон «*Об информационно-технологическом, информационно-коммуникационном обучении (ликбезе) всего населения, о доведении компьютерных знаний, умений и навыков до совершенства*», под реализацию которого из государственного бюджета должны выделяться солидные финансовые средства. Это нужно прежде всего для того, чтобы каждый гражданин мог тем самым повышать свой профессионализм на своем рабочем месте, мог бы на равных конкурировать в вопросах компьютерной грамоты с гражданами, предпринимателями развитых государств, сотрудничать с ними, чтобы он не становился жертвой электронных мошенников, чтобы мог грамотно проконтролировать своих детей, защитить их от лиц, подталкивающих их к самоубийству в Интернете, от буллинга (электронной травли) и так далее [18].

Принятие новых универсальных конвенций для решения возникающих проблем информационно-коммуникационных технологий и связанных с ними прав человека. Международно-политическую и международно-правовую основу цифровизированных прав человека составляют следующие две группы источников: а) резолюции органов ООН, документы Венецианской комиссии и б) международно-правовые акты — конвенции и соглашения на тему о цифровизированно-информационной основе прав и свобод человека. К первой группе можно отнести резолюцию Совета ООН по правам человека 2012 года о защите свободы слова во всемирной сети, в которой подчеркивается: *«Те же права, которые человек имеет в офлайновой среде»* на основе статей Международного пакта о гражданских и политических правах и иных актов о правах человека, *«должны также защищаться и в онлайновой среде, в частности, право на свободу выражения мнений»*, «независимо от границ и для любых выбираемых человеком средств массовой информации». В этой связи нужно разработать и принять новый универсальный международно-правовой акт — конвенцию: *«Об обеспечении международной защиты всех прав человека, закрепленных в вошедших в силу письменных международных документах, используемых в Интернете, на иных информационно-коммуникационных носителях»*.

Информация, используемая во благо людей, стран, человечества подлежит распро-

странению, а информация, идущая во вред, должна быть под запретом. Но вредная информация должна быть четко определена и сформулирована как во внутригосударственном законе, так и в международном праве. Международно-правовой механизм может стать таким. Государства в универсальной международной конвенции могли бы прописать и взять на себя обязательства по обеспечению регистрации и лицензирования деятельности всех собственников компьютерных серверов, возложить на них ответственность (вплоть до уголовной) за распространение закрепленной в законе вредоносной информации, за предоставление разрешения на такое распространение, оказывать содействие отечественной и международной полиции при нарушении норм данной конвенции. Можно предложить от имени наших стран, чтобы государства-члены Интерпола могли в порядке дополнения предусмотреть в этой организации еще одну, информационно-коммуникационную, функцию по борьбе с международной преступностью в Интернете. С учетом этих соображений было бы целесообразно разработать и принять новые универсальные международные конвенции под примерно такими названиями, как: *«О привлечении к национальной и международной уголовной ответственности лиц, совершающих преступления в информационно-коммуникационной среде, в Интернете»*, *«О регистрации, лицензировании собственников компьютерных серверов во всех странах, об их ответственности за оказание содействия, за распространение закрепленной в законе вредоносной информации в Интернете»*.

Примеры нарушения свободы слова, свободы выражения мнений, свободы доступа к информации в отношении действовавшего президента США и его многомиллионных сторонников в период избирательной кампании 2020 и начала 2021 года заставляют призадуматься о месте и роли руководителей социальных сетей, в том числе «Твиттер», «Фейсбук», и иных информационно-коммуникационных компаний и объединений. В этой связи на внутригосударственном уровне необходимо установить, усилить ответственность в отношении руководителей информационно-коммуникационных компаний, нарушающих фундаментальные информационные и иные права человека. На международно-правовом уровне название конвенции по данной теме могло бы выглядеть так: *«Об установлении международной правовой, имущественной, финансовой ответственности информационно-коммуникационных корпораций и компаний, их руководителей за нарушение фундаментальных и иных прав человека в онлайн и офлайн режимах»*. В западных странах, как известно, возможно привлечение к уголовной ответственности и юридических лиц.

Все эти предложения могут стать основой как отдельных конвенций, так и разделов, статей конвенций более универсального характера. Кроме того, считаю целесообразным поддержать российский вариант Конвенции об обеспечении международной информационной безопасности, опубликованной 22 сентября 2011 года, а также разработанную в рамках ООН Концепцию конвенции о безопасном функционировании и развитии сети

Интернет, обсудить содержание текстов этих документов на двустороннем и региональном уровнях в целях их возможного совершенствования и принятия в перспективе.

Примечания

1. URL: https://basetop.ru (дата обращения: 24.01.2021).

2. Более подробно см.: Рейтинг стран мира по уровню развития информационно-коммуникационных технологий. URL: https://gtmarket.ru (дата обращения: 25.01.2021).

3. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года. URL: https://digital. gov.ru (дата обращения: 26.01.2021).

4. URL: https://nisse.ru (дата обращения: 26.01.2021).

5. Новожилов О. П. Информатика: учебник в 2 частях. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. Ч. 2. 302 с.; а также: Набиуллина С. Н. Информатика и ИКТ: курс лекций. Москва: Лань, 2019. 72 с.; Астафьева Н. Е. Информатика и ИКТ: практикум для профессий и специальностей технического и социально-экономического профилей. Москва: Academia, 2019. 384 с.

6. Внуков А. А. Основы информационной безопасности: защита информации: учебное пособие. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2020. 240 с.

Notes (transliteration)

1. URL: https://basetop.ru (date of application: 24.01.2021) (in Russ.).

2. URL: https://gtmarket.ru (date of application: 25.01.2021) (in Russ.).

3. URL: https://digital. gov.ru (date of application: 26.01.2021) (in Russ.).

4. URL: https://nisse.ru (date of application: 26.01.2021) (in Russ.).

5. Novozhilov O. P. Informatika. Moscow: *Yurayt*, 2020, part 2, 302 p. (in Russ.); Nabiullina S. N. Informatika i IKT. Moscow: *Lan'*, 2019, 72 p. (in Russ.); Astaf'yeva N. E. Informatika i IKT. Moscow: *Academia*, 2019, 384 p. (in Russ.).

6. Vnukov A. A. Osnovy informatsionnoy bezopasnosti: zashchita informatsii. Moscow: *Yurayt*, 2020, 240 p. (in Russ.).

7. Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. Sebastopol (CA, USA): O'Reilly Media, 2017, 240 p.

8. Hubbard D. W., Geer Jr., Daniel E. Praise for How to Measure Anything in Cybersecurity Risk. Hoboken (NJ, USA): Wiley, 2016, 304 p.

9. URL: https://www.gazeta.ru (date of application: 26.01.2021) (in Russ.).

10. Tendentsii razvitiya interneta v Rossii i zarubezhnykh stranakh / G. I. Abdrakhmanova,

7. Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. Sebastopol (CA, USA): O'Reilly Media, 2017. 240 p.

8. Hubbard D. W., Geer Jr., Daniel E. Praise for How to Measure Anything in Cybersecurity Risk. Hoboken (NJ, USA): Wiley, 2016. 304 p.

9. Герасюкова М. Какие законы об интернете вступят в силу в 2021 году. Социальные сети и блокировка. URL: https://www.gazeta.ru (дата обращения: 26.01.2021).

10. Тенденции развития интернета в России и зарубежных странах: аналитический доклад / Г. И. Абдрахманова, О. Е Баскакова, К. О. Вишневский, Л. М. Гохберг и др.; Координационный центр национального домена сети Интернет, НИУ ВШЭ. Москва: НИУ ВШЭ, 2020. 144 с.

11. Информационно-коммуникационные технологии: учебник. Алматы, 2017. 559 с.

12. Федотов М. А. Информационное право: учебник. Москва: Издательство Юрайт, 2019. 497 с.

13. Buchan R., Tsagourias N. Research Handbook on International Law and Cyberspace. Cheltenham (United Kingdom): Edward Elgar Publishing, 2015. 560 p.

14. Данельян А. А., Гуляева Е. Е. Международно-правовые аспекты кибербезопасности // Московский журнал международного права. 2020. N 1. С. 44–53.

15. Смыслова Т. М. Международное информационное право. Москва, 2002. 192 с.

16. Киберпреступность. Модуль 3. Правовая база и права человека. Вена: Организация Объединенных Наций, 2019. 46 с.

O. E Baskakova, K. O. Vishnevskiy, L. M. Gokhberg et al. Moscow: *NIU VShE*, 2020, 144 p. (in Russ.).

11. Informatsionno-kommunikatsionnyye tekhnologii. Almaty, 2017, 559 p. (in Russ.).

12. Fedotov M. A. Informatsionnoye pravo. Moscow: *Yurayt*, 2019, 497 p. (in Russ.).

13. Buchan R., Tsagourias N. Research Handbook on International Law and Cyberspace. Cheltenham (United Kingdom): Edward Elgar Publishing, 2015, 560 p.

14. Danel'yan A. A., Gulyayeva E. E. *Moskovskiy zhurnal mezhdunarodnogo prava*, 2020, no. 1, pp. 44–53 (in Russ.).

15. Smyslova T. M. Mezhdunarodnoye informatsionnoye pravo. Moscow, 2002, 192 p. (in Russ.).

16. Cybercrime. Module 3. Legal Frameworks and Human Rights. Vienna: United Nations, 2019, 46 p. (in Russ.).

17. Cyber Operations and International Law. Cambridge (United Kingdom): Cambridge University Press, 2020, 522 p.

18. Shmeleva A. G., Ladynin A. I. Informatika. Informatsionnyye tekhnologii v professional'noy deyatel'nosti: Microsoft Word. Microsoft Excel: teoriya i primeneniye dlya resheniya professional'nykh zadach. Moscow, 2020, 304 p. (in Russ.).

17. Cyber Operations and International Law. Cambridge (United Kingdom): Cambridge University Press, 2020. 522 p.

18. Подробнее см.: Шмелева А. Г., Ладынин А. И. Информатика. Информационные технологии в профессиональной деятельности: Microsoft Word. Microsoft Excel: теория и применение для решения профессиональных задач. Москва, 2020. 304 с.