ПРАВО

Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2023. Т. 23, вып. 1. С. 48–59
Izvestiya of Saratov University. Economics. Management. Law, 2023, vol. 23, iss. 1, pp. 48–59
https://eup.sgu.ru https://doi.org/10.18500/1994-2540-2023-23-1-48-59
EDN: DGEDQE

Научная статья
УДК 342.76

Ограничения цифровых прав человека в целях противодействия терроризму

Г. Б. Романовский ✉, **В. Г. Романовский**

Пензенский государственный университет, Россия, 440026, г. Пенза, ул. Красная, д. 40

Романовский Георгий Борисович, доктор юридических наук, профессор, заведующий кафедрой «Уголовное право», vlad93@sura.ru, https://orcid.org/0000-0003-0546-2557

Романовский Владислав Георгиевич, кандидат юридических наук, доцент кафедры «Уголовное право», up406@mail.ru, https://orcid.org/0000-0002-4558-5730

Аннотация. ***Введение.*** Российское гражданское законодательство учитывает инновации в информационном обмене, закрепляя понятие цифровых прав, при этом придавая им исключительно частноправовое понимание. Современная доктрина исходит из того, что развитие цифровых технологий также заметным образом повлияло на концепцию основных прав человека. Продолжением такого видения считается появление цифровых прав в публичной сфере. Это актуализирует анализ их возможных ограничений в целях противодействия терроризму. ***Теоретический анализ.*** Выявлены последствия перевода значительного объема социальных отношений в цифровой формат. При этом пока общий дискурс дискуссий исходит из принципа «нормативной эквивалентности» между «офлайн» и «онлайн» (что не требует кардинальных изменений в праве), но опыт распространения цифровых технологий показывает, что он все чаще дает системные сбои. Обозначены сложности с определением цифровых прав и их нормативным закреплением (на примере нормативных актов Европейского союза). ***Эмпирический анализ.*** На основе выявленных характеристик цифровых коммуникаций были представлены модели противодействия террористическим угрозам, сформированным в современном киберпространстве. Показаны особенности законодательного обеспечения китайской модели «Золотой щит», основанного на принципах цифрового суверенитета (в частности, Закон КНР «О безопасности данных»). Выделены особенности введения ограничений права на цифровое общение для лиц, подозреваемых в причастности к террористической деятельности (в частности, на основании Акта о борьбе с терроризмом и безопасности границ, принятого в 2019 г. в Великобритании). Рассматривается и иной зарубежный опыт противодействия террористическим угрозам в цифровой сфере. ***Результаты.*** Показана необходимость учета технологических особенностей информационного обмена в цифровом пространстве. Это оказывает заметное влияние на появление новых мер противодействия терроризму. Зарубежный опыт свидетельствует о расширении перечня оперативно-розыскных мероприятий, перечня составов преступлений террористической направленности.

Ключевые слова: цифровые права, цифровизация, ограничения, права человека, терроризм, киберпреступление, противодействие

Благодарности: Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 20-011-00096).

Для цитирования: *Романовский Г. Б., Романовский В. Г.* Ограничения цифровых прав человека в целях противодействия терроризму // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2023. Т. 23, вып. 1. С. 48–59. https://doi.org/10.18500/1994-2540-2023-23-1-48-59, EDN: DGEDQE

Статья опубликована на условиях лицензии Creative Commons Attribution 4.0 International (CC-BY 4.0)

© *Романовский Г. Б., Романовский В. Г., 2023*

НАУЧНЫЙ ОТДЕЛ

Article

Restrictions on digital human rights to counter terrorism

G. B. Romanovsky ✉, **V. G. Romanovsky**

Penza State University, 40 Krasnaya St., Penza 440026, Russia

Georgy B. Romanovsky, vlad93@sura.ru, https://orcid.org/0000-0003-0546-2557

Vladislav G. Romanovsky, up406@mail.ru, https://orcid.org/0000-0002-4558-5730

Abstract. ***Introduction.*** Russian civil legislation takes into account innovations in information exchange by fixing the concept of digital rights, while giving them an exclusively private legal understanding. The modern doctrine proceeds from the fact that development of digital technologies has also significantly influenced the concept of fundamental human rights. Continuation of this vision is the emergence of digital rights in the public sphere. This actualizes the analysis of their possible limitations in order to counter terrorism. ***Theoretical analysis.*** The research reveals the consequences of the transfer of a significant amount of social relations to digital format. At the same time, while the general discourse of discussions stems from the principle of "normative equivalence" between "offline" and "online" (which does not require fundamental changes in law), the experience of the spread of digital technologies shows that it increasingly faces systemic failures. The authors indicate the difficulties with the definition of digital rights and their regulatory consolidation (by analyzing the regulations of the European Union). ***Empirical analysis.*** Based on the identified characteristics of digital communications, the paper presents the models for countering terrorist threats in modern cyberspace. The features of the legislative support of the Chinese model of the "Golden Shield", based on the principles of digital sovereignty (in particular, the Law of the People's Republic of China "On Data Security"), are shown. The authors highlight the features of imposing restrictions on the right to digital communication for persons suspected of involvement in terrorist activities (in particular, on the basis of the Anti-Terrorism and Border Security Act adopted in 2019 in the UK) and consider other foreign experience in countering terrorist threats in the digital sphere. ***Results.*** The necessity of taking into account the technological features of information exchange in the digital space is demonstrated. This has a significant impact on the emergence of new measures to counter terrorism. Foreign experience testifies to the expansion of the list of operational and search measures, the list of elements of crimes of a terrorist nature.

Keywords: digital rights, digitalization, restrictions, human rights, terrorism, cybercrime, counteraction

Acknowledgements: This work was supported by the Russian Foundation for Basic Research (project No. 20-011-00096).

For citation: Romanovsky G. B., Romanovsky V. G. Restrictions on digital human rights to counter terrorism. *Izvestiya of Saratov University. Economics. Management. Law*, 2023, vol. 23, iss. 1, pp. 48–59 (in Russian). https://doi.org/10.18500/1994-2540-2023-23-1-48-59, EDN: DGEDQE

This is an open access article distributed under the terms of Creative Commons Attribution 4.0 International License (CC-BY 4.0)

Введение

Цифровизация современного мира затронула практически весь спектр общественных отношений. Происходит трансформация базовых прав человека, а также основ взаимодействия личности и государства. На фоне таких изменений в научный оборот вводится понятие «цифровые права человека».

Данная категория пока не имеет однозначной оценки, можно наблюдать различное толкование самой дефиниции, а также того содержания, которое вкладывается в комплекс цифровых прав. Не добавляют единства в научные дискуссии и некоторые законодательные новеллы, попытавшиеся упорядочить новые аспекты в текущем регулировании. Так, Федеральный закон от 18 марта 2019 г. № 34-ФЗ [1] внес дополнения в Гражданский кодекс РФ, благодаря которым появилась ст. 141.1. «Цифровые права». Знакомство с ее содержанием показывает, что «цифровые права» представлены как «обязательственные и иные права», а значит, как объект гражданских прав, допустимый к обороту и имеющий свою стоимостную оценку. Аналогичная позиция была сохранена в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [2], где практически ставился знак равенства между цифровыми правами и цифровыми финансовыми активами (ст. 1). Недостатки такого подхода обозначались в российской юридической литературе. Л. Г. Ефимова сомневалась в правовой природе указанных цифровых прав, признавая российский опыт «крайне узким и неудачным» [3, 4]. О. А. Городов использует характеристику «размытое» при упоминании понятия цифровых прав [5]. Ю. В. Леднева считает его сложным для восприятия [6].

Е. А. Суханов также скептически отнесся к новеллам гражданского законодательства, дополнив, что примененная логика (указание на цифровой характер) позволяет любое право объявить цифровым. Необходимо отличать форму объекта гражданских прав от юридической природы, которая при смене формы принципиально не меняется [7]. Эту точку зрения поддержал и Н. В. Щербак [8]. В другой своей работе Е. А. Суханов соглашается с опасениями со стороны государства относительно расчетов в криптовалюте, что и порождает не-

обходимость регулирования. Но в этом случае реализуется публично-правовая задача, которая должна решаться «за пределами сферы частного права» [9, с. 11].

В то же время определение цифровых прав, представленное в Гражданском кодексе РФ, носит универсальный характер, что позволяет его расширить на публичную сферу. Е. В. Гриценко прямо указывает, что возможно распространение на «новые цифровые права или цифровые элементы основных прав в публичной сфере» [10, с. 19]. Однако здесь следует сделать ремарку. «Цифровые права», используемые в Гражданском кодексе РФ, не упоминаются как права человека, что является разделительной гранью между частной и публичной сферой использования внешне схожих понятий, но имеющих различную природу, содержание, формы гарантированности и защиты. Не останавливаясь подробно на категории «права человека», укажем лишь, что она носит основополагающий характер, который нашел свое подтверждение на конституционном уровне. В Основах конституционного строя России прямо записано, что человек, его права и свободы – высшая ценность, а их признание и защита – обязанность государства (ст. 2) [11]. Кстати, это практически единственная обязанность государства, предусмотренная Конституцией России. Во всех других положениях предусматриваются обязанности органов государственной власти и местного самоуправления. Иными словами, обратная проекция – с Гражданского кодекса РФ на Конституцию России – весьма непривлекательна.

Теоретический анализ

Методологические разночтения требуют определенного разделения цифровых прав в частной и публичной сферах. Если в частной сфере (как указывалось выше) отношение к цифровым правам далеко не однозначное, то публичная сфера находится под неким «обаянием» нового видения каталога основных прав человека. По-видимому, это связано с быстрым распространением самих цифровых технологий и последствиями такого распространения. При этом зависимость от них наиболее остро проявилась во время пандемийных ограничений, введенных в результате распространения коронавирусной инфекции. С учетом практически тотального перехода на дистанционный формат общения выключенным из социальной жизни оказался тот, кто не имел соответствующих гаджетов и доступа к Интернету. Дискриминационная линия была проведена благодаря киберпространству между теми, кто имеет к нему доступ и соответствующие навыки пользования, и теми, кто лишен того или другого. На тот момент в научной литературе обсуждался вопрос о «выключении» из многих социальных процессов лиц старшего поколения, поскольку некоторым из них с трудом давалось обучение каким-то компьютерным программам и работе с приложениями.

Всеобщий охват цифровизацией создает инфраструктурную основу для реализации властных отношений. Именно поэтому многие государства, первоначально настороженно относившиеся к свободе, пропагандируемой в Интернете, увидели новые перспективы для принуждения и манипулирования. Один из первых шагов – создание технологии Neuro-ID [12], проводящей анализ когнитивных изменений во внешности человека при совершении заданных действий. В частности, одна из перспектив ее развития – выявление реального отношения личности к тому или иному событию, что позволит создать удаленный «детектор лжи», отслеживающий нелояльных граждан во время проведения общественных мероприятий. Нетрудно представить, какие политические режимы проявили заинтересованность к таким экспериментам. Сейчас происходит апробация в кадровых агентствах для подбора кандидатов на определенные должности (пока это подается как «сегментация» – блестящая замена дискредитировавшему себя термину «сегрегация» [13]).

Компания Cognitec [14] продвинулась дальше, предлагая соединить технологию распознавания лиц с выявлением степени взаимодействия в общественном пространстве. Иными словами, благодаря обработке искусственным интеллектом сервис позволяет выявлять лиц, имеющих определенные отношения (вплоть до ранжирования по степени близости), но внешне старающихся это скрыть [15]. Спецслужбы уже высказали перспективы использования изобретения для отслеживания группы террористов, готовящих преступления, идущих к намеченной цели, но находящихся на удалении друг от друга (в частности, при выявлении террористов-смертников, ведомых террористом-контролером).

При таких перспективах (а перечень можно расширить) цифровизация многими рассматривается как одна из угроз системе прав человека. В этой части трудно не согласиться с А. И. Ковлером, прогнозирующим «потерю социального смысла человеческого бытия» и лишение в правах человека их антропологизма [16, с. 148].

Подобный сценарий поддерживается и нейробиологами, где ведущий исследователь Т. Черниговская постоянно указывает на изменения мозга, происходящие из-за отказа от традиционных форм межличностных коммуникаций.

Термин «цифровые права» находятся все больше в центре политических и академических обсуждений, и это характерно практически для всех стран мира. Одно из основных направлений дискуссий – защита цифровых прав – обусловило появление специальных международных площадок, на базе которых вырабатываются различные декларации и программные документы, призванные внедрить принципы прав человека в новое информационное общество. В феврале 2020 г. Европейская комиссия одобрила Цифровую стратегию, где была провозглашена необходимость ориентации цифровых технологий на человека [17]. В ее развитие 15 сентября 2021 г. Европейская комиссия утвердила специальный план цифровой трансформации общества и экономики – «Путь к цифровому десятилетию» [18].

В качестве программных документов необходимо упомянуть Берлинскую декларацию о цифровом обществе и цифровом правительстве, основанных на ценностях [19] (подписана министрами стран Евросоюза). Обращает на себя внимание то, что в документе соединены такие принципы, как «уважение основных прав и демократических ценностей в цифровой сфере», «цифровая грамотность, позволяющая всем гражданам участвовать в цифровой среде», и «цифровой суверенитет».

В 2021 г. инициатива Португалии во время ее председательства в Евросоюзе проявилась в призыве к подписанию Лиссабонской декларации, обращенному ко всем участникам киберпространства (от государств и отдельных органов власти до граждан и неправительственных организаций) [20]. Документ не представляет собой свода обязательств, предусматривая основные направления будущего развития (цифровая идентификация, кибербезопасность, интернет-нейтралитет, свобода слова, цифровые платформы и цифровое образование и др.). Несмотря на такой характер документа, он рассматривается в системе с другими европейскими актами, определяющими общую политику государств в данной сфере.

26 января 2022 г. была опубликована Европейская декларация о цифровых правах и принципах цифрового десятилетия [21]. В преамбуле документа выражена сущность цифровых прав – «человеческое измерение цифровой экосистемы с единым цифровым рынком в качестве ее ядра». Декларация признает, что цифровая трансформация затрагивает все аспекты социальной жизни, улучшает ее качество, но и создает новые проблемы. Исходя из этого, Декларация нацелена на продвижение европейских ценностей в новом цифровом мире. В ней предусматривается набор прав, которые должны обеспечиваться на территории Европейского союза без каких-либо дискриминационных обеспечений. Поскольку это первый официальный каталог цифровых прав, приведем его в полном объеме, но без той детализации, которая представлена в тексте Декларации. Таким образом, каждый имеет право на:

– доступ к недорогому и высокоскоростному цифровому соединению;

– цифровое образование;

– справедливые, здоровые и безопасные условия труда и надлежащую защиту в цифровой среде;

– доступ ко всем ключевым государственным услугам в Интернете по всему Европейскому союзу;

– возможность пользоваться преимуществами искусственного интеллекта, делая свой собственный осознанный выбор в цифровой среде;

– выбор онлайн-сервисов, основываясь на объективной, прозрачной и достоверной информации;

– возможность честно конкурировать и внедрять инновации в цифровой среде;

– доступ к надежной, разнообразной и многоязычной онлайн-среде;

– свободу выражения мнений в онлайн-среде, не опасаясь цензуры или запугивания;

– информацию о владельцах (или осуществляющих контроль) используемых медиа-услуг;

– безопасный, надежный и защищенный доступ к цифровым технологиям, продуктам и услугам;

– защиту своих личных данных в Интернете;

– конфиденциальность своих сообщений и информации на своих электронных устройствах;

– определение своего цифрового наследия.

Отдельными блоками Декларация предусматривает права ребенка в цифровой среде и основы устойчивого развития в цифровой среде.

На уровне ООН разрабатываются базовые документы, которые могут заложить основу возможной будущей конвенции о цифровых правах человека. Однако такое направление развития событий многими оценивается как преждевременное. К тому же международные органы исходят из необходимости защиты универсальных

прав человека как в офлайн-, так и онлайн-пространстве (без введения дополнительных прав человека) [22]. Подобное видение характерно и для юридической науки. Так, В. В. Кресс считает, что цифровизация качественно не изменила право как социальное явление: «Цифровизация не производит революцию в праве, хотя и создает революционную ситуацию в правоприменении, которая по мере накопления количественных характеристик может привести к качественным изменениям» [23, с. 71].

Отчасти соглашаясь с указанным мнением, следует подчеркнуть, что благодаря прорывным технологиям происходит ускорение общественных процессов. И ожидаемый переход «количества в качество» уже намечается в ближайшее время. Формируются предложения о создании «цифровых помощников судьи», превращении электронного правительства в алгоритм, уполномоченный на принятие обязательных решений. Прогнозируемая децентрализация и использование модели сетевого управления приведут не просто к изменениям права, но и к появлению новых источников, которые будут кардинально отличаться от традиционных [24]. Достаточно обратиться к работам ведущих западных футурологов, чтобы увидеть «картину будущего», которая при этом обретает некие черты реальной перспективы. Пока общий дискурс обсуждения исходит из принципа «нормативной эквивалентности» между «офлайн» и «онлайн» (что не требует кардинальных изменений в праве), но опыт распространения цифровых технологий показывает, что он все чаще дает системные сбои. Многие авторы предлагают три этапа реакции мирового сообщества: 1) радикальное переосмысление существующих прав; 2) формирование новых прав; 3) появление новых носителей цифровых прав и обязанностей [25]. Пока человечество находится в начале первого этапа, но надо готовиться к планомерному переходу к двум другим.

Эмпирический анализ

Развитие цифровых технологий также обусловило интерес к ним со стороны деструктивных элементов, что привело к формированию нового явления – киберпреступности. Перевод значительного круга отношений в онлайн-режим не мог не сказаться на росте числа преступлений, совершенных в виртуальном пространстве. Более того, официальная статистика указывает, что именно благодаря кибердействиям возможно нанесение максимального ущерба. Так, Отчет Генеральной прокуратуры Российской Федерации о состоянии преступности в России стабильно показывает, что четверть преступлений совершается в сфере информационно-телекоммуникационных технологий или компьютерной информации [26]. Общий ущерб от киберпреступности в 2021 г. оценивается примерно в 90 млрд руб. (в 2020 г. – около 70 млрд руб.) [27].

Подобное распространение обусловило разработку новой концепции анекселенктотичной (неконтролируемой) технотронной преступности, автором которой выступает К. Н. Евдокимов [28].

Освоение киберпространства со стороны террористических организаций происходило последовательно. Первоначально наблюдались завышенные ожидания от возможного вредоносного воздействия. В конце 1990-х – начале 2000-х гг. некоторую популярность набрал тезис о потенциальном «цифровом Перл-Харборе», при котором террорист-одиночка взламывал критическую инфраструктуру и наносил максимальный вред. Сами террористы подобные планы выстраивали лишь гипотетически. Разведданные мировых спецслужб также подтверждали маловероятность подобного сценария. Между тем апокалипсические предсказания имели свой эффект: были созданы различные компании, занимавшиеся кибербезопасностью. В развитых государствах были освоены значительные ресурсы, нацеленные на создание кибербарьеров и киберзащиты. Это привело к тому, что общий уровень безопасности значительно вырос. В аналитических докладах разведслужб сейчас звучит общий посыл о минимизации компьютерной преступности и создании партнерских отношений правоохранительной системы и интернет-провайдеров, благодаря которым сами операторы берут на себя обязательства по отслеживанию вредоносного трафика и его блокированию [29].

Более значимый эффект от использования цифровых технологий террористическими организациями видится в выстраивании параллельных коммуникаций, с помощью которых возможны: пропаганда и агитация; рекрутирование сторонников; сбор финансовых и материальных ресурсов; обучение навыкам ведения преступной деятельности; запугивание противников. С учетом того, что коммуникации между людьми все больше выстраиваются именно в онлайн, а не офлайн, именно эта сфера наиболее перспективна для оказания соответствующего воздействия.

По каждому из заявленных направлений видна высокая активность наиболее известных в мире террористических организаций. Так, пропаганда преступной идеологии проводится

с помощью различных интернет-ресурсов, где главенствующее место занимают социальные сети. Технологические особенности функционирования социальных сетей строятся на основе мгновенной передачи сообщений, аудио-, фото- и видеоматериалов. Благодаря хэш-тегам происходит быстрое ориентирование в виртуальном мире, когда блокировка одного канала передачи данных практически мгновенно компенсируется построением других. К тому же анонимность, сложность в идентификации реального пользователя и распространителя информации способствует тому, что нахождение реального лица, стоящего за преступным контентом, а затем его привлечение к ответственности – задача весьма затруднительна.

Опыт борьбы с радикальными организациями показывает, что передаваемая информация разделена по аудиториям (для детей, молодежи, лиц более зрелого возраста, учитываются различные факторы, такие как национальность, вероисповедание и др.), по цели ее распространения (агитация, запугивание, оправдание преступных действий и т.д.). Поиск именно запрещенной информации для последующего блокирования осуществляется зачастую самими провайдерами, что отражается в их фактчекинговой политике, обусловливающей блокировку аккаунтов, злоупотребляющих доверием и распространяющим фейковые данные.

Правоохранительные органы также ведут мониторинг онлайн-пространства, что наталкивается на определенные технологические сложности. Даже создание специальных программ, использующих искусственный интеллект и специальные алгоритмы, не справляется с построением системы абсолютного контроля. К тому же пропаганда террористических идей основывается на последовательности, используемой при создании игр с альтернативной реальностью (Alternate Reality Games – ARG), где каждый шаг приводит к переходу на следующий уровень. Это означает, что первоначальный материал, распространяемый в Сети, главная цель которого формирование общего интереса, не содержит прямых агитационных посылов. Чаще всего он относительно нейтрален, чтобы не вызывать подозрений со стороны органов государства. В этом главная задача пошаговой радикализации, именуемой в специальной литературе как путь «от нуля до героя». Ярким примером может служить иллюстрация привлечения внимания немецкой молодежи к салафитскому вероучению и последующему вовлечению в различные экстремистские действия на религиозной основе. Это отражено в специальном докладе за 2018 г. организации «Jugendschutz.net» (создан одноименный сайт, систематизирующий все проявления экстремизма в Интернете против немецкой молодежи) – «Исламизм в сети» [30]. Первичным роликом, возбуждающим интерес, стал видеоролик боя бойцов ММА Конора Макгрегора и Хабиба Нурмагомедова. Сам по себе видеоматериал не содержит какой-то преступной направленности, но при этом в него вложен комментарий, связывающий победу Х. Нурмагомедова с его вероисповеданием, с добавлением, что получение дополнительных знаний возможно на специальных ресурсах. К ролику прилагались интерактивные ссылки на иные сайты. При появлении интереса каждый последующий шаг по интерактивной ссылке создавал «лестницу» уже к тем ресурсам, которые создавали эффект «эхо-камеры» – общение только со сторонниками экстремистской идеологии, где и проходила соответствующая идеологическая обработка [31]. Пропаганда террористических идей в виртуальном мире стала настолько активной, что позволяет некоторым исследователям указывать на новое явление – «электронный джихад» [32].

Цифровые коммуникации имеют ключевые особенности:

– отсутствие территориальных границ, что позволяет выстраивать общение в режиме реального времени между лицами, находящимися за десятки тысяч километров друг от друга;

– невозможность цензурирования и государственного контроля, благодаря чему любая информация может стать общедоступной;

– собственные правила привлекательности и тиражирования, неучет которых приводит к тому, что информационную повестку чаще всего создают не официальные агентства, а индивидуумы, способные генерировать интересный контент, привлекающий массовое внимание;

– превалирование технических правил над юридическими в построении циклической цепочки от создания информации до ее массового распространения, что создает дополнительные сложности в формировании надлежащего правового режима деятельности всех участников онлайн-общения.

Государство в силу определенной инертности не успевает за стремительно меняющейся действительностью. Сейчас можно наблюдать попытки создания регуляционного механизма. Однако пока все это больше напоминает некую гонку противостояния, когда на введение юридического барьера (или дополнительного препятствия для субъекта интернет-активности)

создается технология обхода. Иллюстрацией может служить трехлетнее противостояние (2017–2019 гг.) Роскомнадзора и мессенджера Telegram, созданного выходцами из России братьями Дуровыми. В течение всего это времени попытки блокировать доступ к Telegram так и не увенчались успехом. В настоящее время все официальные претензии к мессенджеру сняты.

Показательно, что Telegram заблокирован в Иране и Китайской Народной Республике, но и там в условиях жесткой системы контроля создать поле вне доступа к указанному мессенджеру так и не стало полностью возможным.

Перевод большинства коммуникаций в цифровое пространство и возможности его использования в противоправных целях обусловили концепцию ограничений цифровых прав. Их полное нивелирование неосуществимо, что находит свое понимание в большинстве правопорядков. Радикальное решение в отключении «заветного рубильника» практически невозможно, даже попытки его реализации могут иметь негативные последствия, которые ни одно государство в современном мире не может себе позволить. Кстати, государства чаще всего при осуществлении таких блокировок напрямую не объявляют о проводимых запретах. К тому же длительное отключение несет как краткосрочные (прямые потери компаний), так и долгосрочные убытки (смена локации предприятия, а значит, уход инновационных проектов).

В августе 2020 г. произошло отключение (на несколько дней) Республики Беларусь от Всемирной паутины. Причины разнятся, по крайней мере, органы государственной власти не взяли на себя ответственность за совершение такого шага. Не вдаваясь в обсуждение поиска виноватых, лишь отметим, что экспертная оценка указывает на ущерб в размере 200–250 млн долл. США за каждый день такого выхода страны из онлайн-пространства [33]. Если брать страну с большим числом интернет-пользователей, то ущерб будет кратно увеличиваться. Таким образом, умаление права на сам доступ к высокоскоростному цифровому соединению (даже если и возникнет такое желание в отдельной стране) является недопустимым и несет большие финансовые потери для государства.

В разных странах вводятся различные правила, пытающиеся распространить национальный правовой режим на киберпространство, где одним из его аспектов выступают ограничения специальных субъективных прав. В этом аспекте, прежде всего, следует упомянуть опыт КНР, основанный на идее цифрового суверенитета. Такая последовательность оправданна, поскольку невозможно ограничение того, что не подлежит национальному регулированию. Если реализация цифровых прав будет зависеть от внешних субъектов – транснациональных корпораций и иных государств, то попытки органов власти без их согласия оказать воздействие только на обладателя цифровых прав будут обречены на провал. В этой части китайская идея «Золотой щит», которая предполагает распространение суверенитета на виртуальное пространство, наиболее последовательна, обусловливая принятие целого комплекса законодательных актов. Это можно наблюдать при анализе правотворческой политики:

– обновление законодательства в сфере государственной тайны (принятие в новой редакции Закона КНР от 5 сентября 1988 г. «Об охране государственной тайны» – Закон от 29 апреля 2010 г. [34]), в рамках которого обязанности по соблюдению государственных секретов были распространены практически на всех субъектов цифрового общения;

– обеспечение суверенитета киберпространства с помощью введения специального правового режима кибербезопасности (итогом стал Закон КНР от 7 ноября 2016 г. «О кибербезопасности» [35]), позволяющего широко трактовать обязанности юзеров;

– суверенизация цифровых данных (Закон КНР от 10 июня 2021 г. «О безопасности данных» [36]), вводящая жесткие ограничения на возможное влияние со стороны иностранных компаний.

Законодательство стран Западной Европы идет иным путем. Введение ограничений цифровых прав в целях противодействия терроризму происходит точечными методами, в совокупности с уточнением уголовного законодательства, где совершение киберпреступлений все чаще рассматривается либо как самостоятельный состав, либо как элемент объективной стороны уже закрепленных преступлений (как правило, как отягчающее вину обстоятельство). В этой части иллюстрацией такого подхода можно считать британский Акт о борьбе с терроризмом и безопасности границ (Counter-Terrorism and Border Security Act, 2019) [37]. Данный закон вызвал определенный шквал критики со стороны правозащитных организаций, поскольку заметно расширил понимание пропаганды терроризма, включив в него широкую формулировку о «безрассудной поддержке». Благодаря этому наказуемым стал просмотр цифрового контента террористической направленности.

Широкие общественные дискуссии, наверное, привели к тому, что в Англии так до сих

пор и не принят Акт о безопасности в Интернете, проект которого был обнародован еще в 2021 г. [38]. Периодически на официальной странице парламента публикуются те или иные документы вокруг заявленного проекта. Объявлялось, что первоначальное голосование пройдет летом 2022 г., но оно так и не состоялось.

Опыт ряда стран показывает, что в отношении лиц, подозреваемых в террористических связях, вводятся ограничения цифровых прав. Так, британский Акт о мерах по предупреждению и расследованию терроризма (Terrorism Prevention and Investigation Measures Act 2011 [39]) предусматривает введение мер административного контроля за любым онлайн-общением лица, в отношении которого есть достаточные основания подозревать его в установлении связей с террористической организацией. Такие меры вводятся на основании судебного ордера и могут включать в себя: ограничения на использование средств электронной связи; подключение любого гаджета только к контролируемой линии соединения; использование только такого электронного устройства, которое не имеет подключения к Интернету. Данный Акт рассматривается как весьма жесткий. Его применение находится под постоянным парламентским контролем. Создана специальная должность Комиссара по обеспечению независимого надзора за использованием следственных полномочий разведывательными органами, полицией и другими государственными органами. Действие Акта 2011 г. неоднократно подтверждалось более поздними законами, хотя его применение в части введения ограничительных мер в области цифрового общения не получило массового характера. Например, в 2017 г. такие запреты были введены только в отношении шести граждан, находящихся на территории Великобритании.

Подобный Закон № 2016-731 «Об усилении борьбы с организованной преступностью, терроризмом и их финансированием, а также о повышении эффективности и гарантий уголовного судопроизводства» принят во Франции 3 июня 2016 г. [40]. Его основное отличие заключается в том, что установлен последующий судебный контроль, сами ограничения устанавливаются административным актом руководителя органа полиции.

Российское законодательство во многом не учитывает зарубежный опыт. Так, антитеррористическое законодательство, представленное Федеральным законом от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», не учитывает глобальные изменения, произошедшие в информационном обмене. Этот упрек, кстати, во многом касается и Уголовно-процессуального кодекса Российской Федерации, и Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Во многих странах уже имеют успешный опыт применения (с их юридическим закреплением) такие мероприятия, как государственное хакерство, взлом электронного устройства, мониторинг интернет-пространства и некоторые другие. По-видимому, в этой части правоохранительной системе следует активнее воспринимать результаты компаративистских исследований, лоббировать их на уровне принятия соответствующих законов.

Выводы

Концепция цифровых прав человека набирает все большую популярность, становясь предметом обсуждений различных политических площадок. Ранее превалировавшая точка зрения о цифровой форме базовых прав человека, но не меняющих их сущность, все чаще критикуется под влиянием последствий технологических изменений. По крайней мере, сейчас можно констатировать устоявшееся мнение о трансформации прав человека. Именно в этом направлении наблюдается основной путь научных исследований. Это приведет к изменениям в российском гражданском законодательстве, где пока цифровые права – объект частной сферы. В последующем возможно расширение субъектного состава цифровых отношений, что, безусловно, приведет к появлению новых нестандартных обладателей прав. Распространение на них действия прав человека – не такая уж и фантасмагория. Сейчас никто не удивляется тому, что некоторые конституционные права человека (если это не меняет их природу) могут принадлежать юридическим лицам. Есть соответствующая практика Конституционного суда Российской Федерации. По-видимому, нечто подобное может быть применено и к иным субъектам.

Террористические организации быстро освоили онлайн-ресурсы и онлайн-возможности для реализации своих преступных целей. При этом наибольшее подспорье оказывают особенности функционирования социальных сетей: их трансграничность, сложности при аутентификации пользователя, быстрота распространения данных. Перевод все большего числа социальных отношений в цифровой формат создает дополнительные трудности правоохранительным органам в процессе создания эффективной системы противодействия террористическим угрозам. Необходим учет технологических особенностей

нового информационного обмена. В настоящее время кибератаки на критические объекты инфраструктуры со стороны террористических организаций маловероятны (тем более с возможным серьезным ущербом). Но это не означает, что иные формы распространения своего влияния могут быть малозначимыми. В цифровом мире основная борьба разворачивается за внимание пользователей и вовлечение в круг влияния как можно большего их числа. Она подчиняется собственным правилам, которые достаточно сложно поменять простым волеизъявлением законодательного органа власти. В ряде стран продвигается идея цифрового суверенитета, которая опосредованно влияет на возможности государства по введению дополнительных ограничений цифровых прав человека. Безопасность и противодействие терроризму – основные легитимные цели введения таких юридических мер.

Необходим также учет новых цифровых реалий в практической деятельности правоохранительных органов, что достигается установлением новых видов оперативно-розыскных мероприятий. В ряде стран закрепляются такие полномочия органов государственной власти, как массовый сбор данных о гражданах, мониторинг онлайн-ресурсов, взлом электронного устройства, государственное хакерство. Это не означает, что подобные меры должны однозначно предусматриваться в российском законодательстве. Они еще должны получить всестороннюю оценку со стороны экспертного сообщества. Однако в этой части российское законодательство заметно отстает от аналогичных зарубежных актов.

Список литературы

1. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации : федер. закон от 18.03.2019 № 34-ФЗ // Собр. законодательства Рос. Федерации. 2019. № 12, ст. 1224.
2. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 31.07.2020 № 259-ФЗ (ред. от 14.07.2022) // Собр. законодательства Рос. Федерации. 2020. № 31 (ч. I), ст. 5018 ; 2022. № 29 (ч. III), ст. 5298.
3. *Ефимова Л. Г.* Альтернативный взгляд на правовое регулирование гражданско-правовых отношений в условиях цифровой экономики // Актуальные проблемы российского права. 2021. Т. 16, № 8. С. 52–62. https://doi.org/10.17803/1994-1471.2021.129.8.052-062
4. *Ефимова Л. Г.* Цифровые активы и права на них в контексте изменения гражданского и банковского законодательства // Банковское право. 2021. № 5. С. 7–20. https://doi.org/10.18572/1812-3945-2021-5-7-20
5. *Городов О. А.* Цифровое право как подотрасль информационного права // Право и цифровая экономика. 2021. № 1. С. 36–43. https://doi.org/10.17803/2618-8198.2021.11.1.036-043
6. *Леднева Ю. В.* Правотворчество в сфере цифровизации публичных финансов // Финансовое право. 2021. № 9. С. 12–16. https://doi.org/10.18572/1813-1220-2021-9-12-16
7. *Суханов Е. А.* Социальное лицо гражданского права (к постановке вопроса) // Гражданское право социального государства : сб. ст., посвященный 90-летию со дня рождения А. Л. Маковского (1930–2020). М. : Статут, 2020. С. 27–28.
8. *Щербак Н. В.* Экзистенциальные особенности гражданско-правового режима объектов авторского права и смежных прав // Вестник гражданского права. 2021. Т. 21, № 6. С. 99–134. https://doi.org/10.24031/1992-2043-2021-21-6-99-134
9. *Суханов Е. А.* О гражданско-правовой природе «цифрового имущества» // Вестник гражданского права. 2021. Т. 21, № 6. С. 7–29. https://doi.org/10.24031/1992-2043-2021-21-6-7-29
10. *Гриценко Е. В.* Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. 2022. № 4. С. 15–36. https://doi.org/10.21128/1812-7126-2022-4-15-36
11. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ) // Собр. законодательства Рос. Федерации. 2014. № 31, ст. 4398 ; 2020. № 11, ст. 1416.
12. Human Analytics for the Digital World. URL: https://www.neuro-id.com (дата обращения: 28.10.2022).
13. *Lee J.* Neuro-ID releases prescriptive analytics solution to assess future risk (2017. 13 June). URL: https://www.biometricupdate.com/201706/neuro-id-releases-prescriptive-analytics-solution-to-assess-future-risk (дата обращения: 28.10.2022).
14. The trusted face recognition company since 2002. URL: https://www.cognitec.com (дата обращения: 28.10.2022).
15. *Hersey F.* Europe heading for ‘open-ended biometric mass surveillance’: report (2021, 9 July). URL: https://www.biometricupdate.com/202107/europe-heading-for-open-ended-biometric-mass-surveillance-report (дата обращения: 28.10.2022).
16. *Ковлер А. И.* Права человека в цифровую эпоху // Бюллетень Европейского суда по правам человека. Российское издание. 2019. № 6. С. 146–150.
17. Europe’s Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983 (дата обращения: 28.10.2022).
18. State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU’s digital transformation by 2030. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630 (дата обращения: 28.10.2022).

19. Berlin Declaration on Digital Society and Value-based Digital Government. URL: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government (дата обращения: 28.10.2022).
20. Lisbon Declaration – Digital Democracy with a Purpose. URL: https://www.lisbondeclaration.eu/ (дата обращения: 28.10.2022).
21. Commission puts forward declaration on digital rights and principles for everyone in the EU. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452 (дата обращения: 28.10.2022).
22. Ensuring the protection of Human Rights. URL: https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Digital_Human_Rights_Summary_PDF.pdf (дата обращения: 28.10.2022).
23. *Кресс В. В.* Цифровые права как объекты гражданских прав: правовое регулирование и перспективы развития в условиях цифровизации гражданского оборота // Журнал российского права. 2022. Т. 26, № 4. С. 67–76. https://doi.org/10.12737/jrl.2022.041
24. *Романовская О. В.* Принцип деконцентрации государственной власти в конституционном праве // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2016. № 2 (38). С. 85–93. https://doi.org/10.21685/2072-3016-2016-2-9
25. *Dror-Shpoliansky D., Shany Y.* It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology // European Journal of International Law. 2021. Vol. 32, iss. 4. P. 1249–1282. https://doi.org/10.1093/ejil/chab087
26. Состояние преступности в России за январь–июль 2022 года. URL: http://crimestat.ru/analytics (дата обращения: 28.10.2022).
27. Оценен ущерб от киберпреступлений в России. URL: https://expert.ru/2021/12/22/otsenen-uscherb-ot-kiberprestupleniy-v-rossii/ (дата обращения: 28.10.2022).
28. *Евдокимов К. Н.* К вопросу о совершенствовании системы противодействия технотронной преступности в Российской Федерации // Российский следователь. 2021. № 10. С. 69–72. https://doi.org/10.18572/1812-3783-2021-10-69-72
29. *Knake R. K.* Cleaning Up U.S. Cyberspace. URL: https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_CyberBrief.pdf (дата обращения: 28.10.2022).
30. 2018 Bericht. Islamismus im Netz. URL: http://www.jugendschutz.net/fileadmin/download/pdf/Bericht_2018_Islamismus_im_Internet.pdf (дата обращения: 28.10.2022).
31. *Silber Mitchell D., Bhatt A.* Radicalization in the West: The Homegrown Threat. 2017. URL: https://info.publicintelligence.net/NYPDradicalization.pdf (дата обращения: 28.10.2022).
32. *Prucha N.* IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram // Perspectives on Terrorism. 2016. Vol. 10, iss. 6. P. 48–58.
33. *Анисимова Н.* Бизнес оценил последствия блокировки интернета в Белоруссии. URL: https://www.rbc.ru/technology_and_media/13/08/2020/5f34d2459a79472c6bac2c32 (дата обращения: 28.10.2022).
34. 中华人民共和国保守国家秘密法 (Закон КНР от 5 сентября 1988 г. «Об охране государственной тайны» (ред. от 29 апреля 2010 г.). URL: http://www.gov.cn/flfg/2010-04/30/content_1596420.htm (дата обращения: 28.10.2022).
35. 中华人民共和国网络安全法 (Закон КНР от 7 ноября 2016 г. «О кибербезопасности»). URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 28.10.2022).
36. 数据安全法 (Закон КНР от 10 июня 2021 г. «О безопасности данных»). URL: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (дата обращения: 28.10.2022).
37. Counter-Terrorism and Border Security Act, 12th February 2019. URL: http://www.legislation.gov.uk/ukpga/2019/3/contents/enacted (дата обращения: 28.10.2022).
38. Draft Online Safety Bill. URL: https://www.gov.uk/government/publications/draft-online-safety-bill (дата обращения: 28.10.2022).
39. Terrorism Prevention and Investigation Measures Act, 2011. URL: http://www.legislation.gov.uk/ukpga/2011/23/pdfs/ukpga_20110023_en.pdf (дата обращения: 28.10.2022).
40. Legifrance – Le service public de l'accès au droit. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id (дата обращения: 28.10.2022).

References

1. On the introduction of amendments to parts one, two and article 1124 of part three of the Civil Code of the Russian Federation. Federal Law 34-FZ of 18.03.2019. *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2019, no. 12, art. 1224 (in Russian).
2. On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation. Federal Law 259-FZ of 31.07.2020 (an edition of 14.07.2022). *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2020, no. 31 (pt. I), art. 5018; 2022, no. 29 (pt. III), art. 5298 (in Russian).
3. Efimova L. G. An alternative view of the legal regulation of civil law relations in the digital economy. *Actual Problems of Russian Law*, 2021, vol. 16, no. 8, pp. 52–62 (in Russian). https://doi.org/10.17803/1994-1471.2021.129.8.052-062
4. Efimova L. G. Digital assets and rights to them within the framework of changes in civil and banking laws. *Bankovskoe pravo* [Banking Law], 2021, no. 5, pp. 7–20 (in Russian). https://doi.org/10.18572/1812-3945-2021-5-7-20

5. Gorodov O. A. Digital law as a sub-branch of information law. *Pravo i tsifrovaia ekonomika* [Law and Digital Economy], 2021, no. 1, pp. 36–43 (in Russian). https://doi.org/10.17803/2618-8198.2021.11.1.036-043
6. Ledneva Yu. V. Law making in the field of digitalization of public finance. *Finansovoe pravo* [Financial Law], 2021, no. 9, pp. 12–16 (in Russian). https://doi.org/10.18572/1813-1220-2021-9-12-16
7. Sukhanov E. A. The social face of civil law (To the formulation of the question). In: *Grazhdanskoye pravo sotsial'nogo gosudarstva: sbornik statey, posvyashchennyi 90-letiyu so dnya rozhdeniya A. L. Makovskogo (1930–2020)* [Civil law of the welfare state: A collection of articles dedicated to the 90th anniversary of the birth of A. L. Makovsky (1930–2020)]. Moscow, Statut Publ., 2020, pp. 27–28 (in Russian).
8. Shcherbak N. V. Existential features of the civil legal regime of objects of copyright and related rights. *Vestnik grazhdanskogo prava* [Civil Law Review], 2021, vol. 21, no. 6, pp. 99–134 (in Russian). https://doi.org/10.24031/1992-2043-2021-21-6-99-134
9. Sukhanov E. A. On the civil legal nature of "digital property". *Vestnik grazhdanskogo prava* [Civil Law Review], 2021, vol. 21, no. 6, pp. 7–29 (in Russian). https://doi.org/10.24031/1992-2043-2021-21-6-7-29
10. Gritsenko E. V. The right to good governance in the digital transformation era. *Sravnitel'noe konstitutsionnoe obozrenie* [Comparative Constitutional Review], 2022, no. 4, pp. 15–36 (in Russian). https://doi.org/10.21128/1812-7126-2022-4-15-36
11. The Constitution of the Russian Federation (adopted by the popular vote of 12.12.1993) (amended by Federal Constitutional Law 6-FKZ of 30.12.2008, Federal Constitutional Law 7-FKZ of 30.12.2008, Federal Constitutional Law 2-FKZ of 05.02.2014, Federal Constitutional Law 11-FKZ of 21.07.2014, Federal Constitutional Law 1-FKZ of 14.03.2020). *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2014, no. 31, art. 4398; 2020, no. 11, art. 1416 (in Russian).
12. *Human Analytics for the Digital World*. Available at: https://www.neuro-id.com (accessed 28 October 2022).
13. Lee J. *Neuro-ID releases prescriptive analytics solution to assess future risk (2017, 13 June)*. Available at: https://www.biometricupdate.com/201706/neuro-id-releases-prescriptive-analytics-solution-to-assess-future-risk (accessed 28 October 2022).
14. *The trusted face recognition company since 2002*. Available at: https://www.cognitec.com (accessed 28 October 2022).
15. Hersey F. *Europe heading for 'open-ended biometric mass surveillance': report (2021, 9 July)*. Available at: https://www.biometricupdate.com/202107/europe-heading-for-open-ended-biometric-mass-surveillance-report (accessed 28 October 2022).
16. Kovler A. I. Human rights in the digital age. *Bulletin of the European Court of Human Rights. Russian Edition*, 2019, no. 6, pp. 146–150 (in Russian).
17. *Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983 (accessed 28 October 2022).
18. *State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU's digital transformation by 2030*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630 (accessed 28 October 2022).
19. *Berlin Declaration on Digital Society and Value-based Digital Government*. Available at: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government (accessed 28 October 2022).
20. *Lisbon Declaration – Digital Democracy with a Purpose*. Available at: https://www.lisbondeclaration.eu/ (accessed 28 October 2022).
21. *Commission puts forward declaration on digital rights and principles for everyone in the EU*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452 (accessed 28 October 2022).
22. *Ensuring the protection of Human Rights*. Available at: https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Digital_Human_Rights_Summary_PDF.pdf (accessed 28 October 2022).
23. Kress V. V. Digital rights as objects of civil rights: legal regulation and development prospects amid the digitalisation of civil commerce. *Journal of Russian Law*, 2022, vol. 26, no. 4, pp. 67–76 (in Russian). https://doi.org/10.12737/jrl.2022.041
24. Romanovskaya O. V. The principle of deconcentration of state power in the constitutional law. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskii region. Obschestvennye nauki* [University proceedings. Volga region. Social sciences], 2016, no. 2 (38), pp. 85–93 (in Russian). https://doi.org/10.21685/2072-3016-2016-2-9
25. Dror-Shpoliansky D., Shany Y. It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology. *European Journal of International Law*, 2021, vol. 32, iss. 4, pp. 1249–1282. https://doi.org/10.1093/ejil/chab087
26. *Sostoyanie prestupnosti v Rossii za yanvar'–iyul' 2022 goda* (The state of crime in Russia for January–July 2022). Available at: http://crimestat.ru/analytics (accessed 28 October 2022) (in Russian).
27. *Otsenen ushcherb ot kiberprestupleniy v Rossii* (Estimated damage from cybercrime in Russia). Available at: https://expert.ru/2021/12/22/otsenen-uscherb-ot-kiberprestupleniy-v-rossii/ (accessed 28 October 2022) (in Russian).
28. Evdokimov K. N. On the improvement of the technetronic crime combating system in the Russian Federation. *Rossiyskiy sledovatel'* (Russian Investigator), 2021, no. 10, pp. 69–72 (in Russian). https://doi.org/10.18572/1812-3783-2021-10-69-72
29. Knake R. K. *Cleaning Up U.S. Cyberspace*. Available at: https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_CyberBrief.pdf (accessed 28 October 2022).

30. *2018 Bericht. Islamismus im Netz*. Available at: http://www.jugendschutz.net/fileadmin/download/pdf/Bericht_2018_Islamismus_im_Internet.pdf (accessed 28 October 2022).
31. Silber Mitchell D., Bhatt A. *Radicalization in the West: The Homegrown Threat. 2017*. Available at: https://info.publicintelligence.net/NYPDradicalization.pdf (accessed 28 October 2022).
32. Prucha N. IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram. *Perspectives on Terrorism*, 2016, vol. 10, iss. 6, pp. 48–58.
33. Anisimova N. *Biznes otsenil posledstviya blokirovki interneta v Belorussii* (Business assessed the consequences of blocking the Internet in Belarus). Available at: https://www.rbc.ru/technology_and_media/13/08/2020/5f34d2459a79472c6bac2c32 (accessed 28 October 2022) (in Russian).
34. *Law of the People's Republic of China of September 5, 1988 "On the Protection of State Secrets" (an edition of April 29, 2010)*. Available at: http://www.gov.cn/flfg/2010-04/30/content_1596420.htm (accessed 28 October 2022) (in China).
35. *Law of the People's Republic of China of November 7, 2016 "On Cyber Security"*. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (accessed 28 October 2022) (in China).
36. *Law of the People's Republic of China of June 10, 2021 "On Data Security"*. Available at: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (accessed 28 October 2022) (in China).
37. *Counter-Terrorism and Border Security Act, 12th February 2019*. Available at: http://www.legislation.gov.uk/ukpga/2019/3/contents/enacted (accessed 28 October 2022).
38. *Draft Online Safety Bill*. Available at: https://www.gov.uk/government/publications/draft-online-safety-bill (accessed 28 October 2022).
39. *Terrorism Prevention and Investigation Measures Act, 2011*. Available at: http://www.legislation.gov.uk/ukpga/2011/23/pdfs/ukpga_20110023_en.pdf (accessed 28 October 2022).
40. *Legifrance – Le service public de l'accès au droit*. Available at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id (accessed 28 October 2022).

Поступила в редакцию 20.11.2022; одобрена после рецензирования 10.12.2022; принята к публикации 12.12.2022
The article was submitted 20.11.2022; approved after reviewing 10.12.2022; accepted for publication 12.12.2022