**Безопасность личности и государства в цифровую эпоху:
политико-правовой аспект***

ОВЧИННИКОВ Алексей Игоревич, заведующий кафедрой теории и истории государства и права Южного федерального университета, доктор юридических наук, профессор
Россия, 344006, г. Ростов-на-Дону, ул. Большая Садовая, 105/42
E-mail: k_fp3@mail.ru

В связи с развитием цифровых технологий государство активно развивает и стимулирует программу цифровизации и технологической модернизации экономики, государственного управления, правового регулирования. Между тем в процессе цифровизации государственного управления следует учитывать некоторые риски и вызовы национальной безопасности, что имеет важное значение для развития законодательства и подзаконного нормотворчества.

Цель статьи — выявление некоторых негативных тенденций цифровизации государства, рассмотренной в контексте цифровой глобализации, обобщение результатов исследования влияния глобальной цифровизации или цифровой глобализации на правовое обеспечение национальной безопасности. Эти тенденции серьезно влияют на реализацию права человека на безопасность, которое становится особенно уязвимым в условиях появления новых субъектов политико-экономических отношений — транснациональных корпораций, сетевых корпораций, блогосферы. Данный анализ позволяет выделить основные направления правового обеспечения национальной безопасности, неотъемлемой частью которой является цифровая или информационная безопасность личности в XXI в. Требуется защиты и право человека на бесцифровую среду, так как необходимо сохранить возможность выбора традиционного образа жизни человека.

Автором выдвинута гипотеза о том, что цифровая глобализация создает новые возможности для экономики, но подвергает безопасность государства, общества и человека ранее неизвестным рискам и вызовам. Применение подходов и методов прогнозирования, социального конструктивизма, философско-правового и системного анализа юридического обеспечения национальной безопасности позволило получить результат, который подтверждает, что цифровизация усугубляет структурные дефекты отечественной системы обеспечения национальной безопасности, изменяет глубинные смыслы и идеи, на которых основано современное государство и общество, трансформирует цели правосудия и поиска справедливости при внедрении искусственного интеллекта в правоприменительную деятельность.

Ключевые слова: национальная безопасность, цифровое общество, цифровое государство, цифровая глобализация, цифровая безопасность, информационная безопасность, искусственный интеллект, правосудие.

Для цитирования: Овчинников А. И. Безопасность личности и государства в цифровую эпоху: политико-правовой аспект // Журнал российского права. 2020. № 6. С. 5—21. DOI: 10.12737/jrl.2020.064

**Individual and State Security in the Digital Age:
Political and Legal Aspect**

A. I. OVCHINNIKOV, Southern Federal University, Rostov-on-Don 344006, Russian Federation
E-mail: k_fp3@mail.ru

* Статья подготовлена при финансовой поддержке гранта РФФИ № 19-011-00820 (а).

In connection with the developing digital technologies, the state is actively developing and stimulating a program of digitalization and technological modernization of the economy, public administration and regulation. Meanwhile, in the process digitalizing public administration, some risks and challenges to national security (of the individual, society and state) should be considered, as this process is important for the development of legislation and by-laws.

The aim of the article is to identify some negative trends in the state digitalization through the digital globalization, to summarize the results of a study of the impact of global digitalization or digital globalization on the legal support of national security. These trends seriously affect the realization of the right to security within human rights. It becomes especially vulnerable in the context of the emergence of new actors in political and economic relations — transnational corporations, network corporations, the blogosphere. This analysis allows us to highlight the main directions of legal support of national security, which integral part is the digital or information security of the individual in the 21st Century.

The result in this study is that a hypothesis is put forward, where digital globalization creates new opportunities for the economy, but exposes risks to the state, social and individual security to previously unknown risks and challenges. The application of approaches and methods of forecasting, social constructivism, philosophical, legal and systematic analysis of legal support of national security allow us to obtain a result that confirms that digitalization exacerbates structural defects of the domestic system of national security, changes the underlying meanings and ideas, on which the modern state and society are based, transforms the goals of justice and the search for justice when introducing artificial intelligence into law enforcement battenning activities.

Keywords: national security, digital society, digital state, digital globalization, digital security, Information Security, artificial intelligence, justice.

For citation: Ovchinnikov A. I. Individual and State Security in the Digital Age: Political and Legal Aspect. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2020, no. 6, pp. 5—21. DOI: 10.12737/jrl.2020.064 (In Russ.)

Введение. Риски и вызовы национальной безопасности в эпоху цифрового мира становятся особенно явными в контексте цифровой глобализации, под которой следует понимать формирование нового миропорядка, конструируемого и управляемого с помощью цифровых технологий в единстве сетевой, коммуникационной и мировоззренческо-смысловой структуры. Представляется правильным говорить в таком случае о цифровой безопасности как важнейшем элементе национальной безопасности, но не в смысле технологической защиты информации. Понятие «цифровая безопасность» значительно шире, чем его часто понимают технические специалисты, определяя ее таким образом: «Цифровая безопасность — это комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства»¹. Представля-

ется, что такой подход не учитывает смену парадигм общественно-политического развития России и мира в целом. Уже в ближайшем будущем понятие «цифровая безопасность» совпадет по смысловому объему с понятием «национальная безопасность» — в этом следует видеть последствия цифровой глобализации, цифровой революции, смены технологических мироукладов, которые могут уничтожить идею национального государства, возникшую в Новое время и пришедшую на смену средневековым теократическим империям. Национальное государство постепенно перестает восприниматься в качестве основного гаранта безопасности человека, большую часть своей жизни проводящего в цифровой реальности, лишенной привычных культурных и территориальных границ, в то время как именно безопасность была идейно-смысловым фундаментом концептуального оформления буржу-

¹ Баранова Н. Что такое цифровая безопасность: термины и технологии. URL:

<https://te-st.ru/2018/05/25/digital-security-terms/>.

азного государства в Новое время в виде доктрины правового государства и общественного договора, заключаемого в целях обеспечения безопасности каждого человека. Например, уже сейчас в международном дискурсе относительно проблем цифровой безопасности конкурируют концепции многосубъектного регулирования и управления рисками (англ. — multi-stakeholder regulation) на основе активного участия негосударственных субъектов-регуляторов, прежде всего граждан, активных пользователей сетей, бизнеса и институтов гражданского общества, и межгосударственного сотрудничества в данной сфере². В цифровом мире нет границ, нет этнической или национальной идентичности — всем этим можно манипулировать по замыслу социальных инженеров-архитекторов нового цифрового мира.

Поэтому пересмотру уже подвергнуты привычные для государства эпохи модерна и даже постмодерна понятия «национальный суверенитет», «государственная валюта», «механизм государства», «национальная идентичность», «идеология» и т. п. Право и его идея также все менее связываются с государством: экстерриториальность становится базовым принципом развития права в информационном пространстве³. Однако самая главная трансформация ожидает идею государства. В эпоху постмодерна постулируются два вектора развития каждого социума (общества, нации, этноса): либо абсолютизация технологического прогресса и крайне рискованный путь в цифровой мир бу-

дущего с его размытыми перспективами в плане семейных ценностей, трансгуманизмом, виртуальной реальностью, ценностным релятивизмом и тотальным прагматизмом, либо иной путь: сохранение национально-культурной идентичности любыми методами, в том числе признавая ее целью и идеологией государства. В некоторых современных странах эта идентичность уже защищается средствами цифрового технологического характера. Примером может служить КНР, где применение искусственного интеллекта и цифровых технологий позволило создать (мягко говоря) цифровую дискриминацию в отношении отдельно взятого этноса в Синьцзяне⁴. Для России этот путь может выглядеть иначе, но только в случае сохранения прав человека в качестве одной из высших ценностей государства.

Национальная безопасность и цифровизация государства. В современной юридической литературе более привычным при обсуждении проблем безопасности человека, общества и государства в контексте цифровизации является термин «информационная безопасность». Однако его возникновение и использование не ассоциируется с формированием совершенно нового цифрового мира и нового человека, не связано с новым мировоззрением. «Информационная безопасность Российской Федерации — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Рос-

² См.: Ефремов А. А. Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве // Информационное право. 2016. № 4. С. 25—28.

³ См.: Овчинников А. И., Самарин А. А. Перспективы развития современного права: экстерриториальность, трансграничность, сетевая множественность // Философия права. 2015. № 3 (70). С. 8—14.

⁴ См.: Саломатин К., Буртин Ш. Заводной мандарин. Узники китайских лагерей рассказывают про общество будущего // Русский репортер. 2019. № 10 (475). С. 34—47.

сийской Федерации, оборона и безопасность государства», говорится в Доктрине информационной безопасности Российской Федерации⁵. Новый технологический уклад ведет к упразднению указанных в данном определении понятий. Суверенитет, территориальная целостность, безопасность государства, понятие «государство» уже подвергнуты пересмотру. Как бы нам того ни хотелось, но эти понятия модерна переживают смысловую трансформацию. Термин «цифровая безопасность» уже прокладывает себе дорогу в отечественной науке в связи с исследованием ранее неизвестных науке цифровых объектов⁶.

В зарубежной научной литературе термин «цифровая безопасность» давно используется для обозначения разнообразных аспектов защищенности в цифровой среде личности и государственных институтов⁷. Рекомендация Организации экономического сотрудничества и развития по управлению рисками цифровой безопасности в целях обеспечения экономического и социального процветания 2015 г. также содержит указание на данное понятие⁸.

Цифровая безопасность представляет собой режим защищенности че-

ловека и общества, а также государства от угроз, возникающих в условиях нового цифрового технологического уклада, в том числе вызванных использованием цифровых технологий в государственном управлении, цифровизацией экономики, образования, медицины и других сфер общественной и частной жизни. Цифровые технологии — это не только сетевые технологии передачи информации, но и развитие искусственного интеллекта, цифровой электроники, биометрии, сотовой связи, телемедицины, смарт-городов, навигации, робототехники и многого другого. Все перечисленное делает понятие цифровой безопасности более объемным и универсально-коннотативным: термин «информационная безопасность» привычно ассоциируется с кибертерроризмом, вирусами, экстремизмом⁹.

Цифровая глобализация: понятие и риски. Прежде всего обратим внимание на то, какие риски для национальной безопасности несет цифровизация в условиях сохраняющегося тренда мирового развития на глобализацию. Думается, речь следует вести уже не просто о глобализации, так как попытки глобализовать мир давно реализуются под разными идейными обоснованиями (например, имперская идея Древнего Рима, миссионерская идея Вселенской Римско-католической церкви, мирового интернационала пролетариата и др.), а о цифровой глобализации, так как в условиях цифровизации общества и государства следует сказать о совершенно новом в истории человечества явлении.

Еще десять лет назад цифровые потоки не оказывали существенного влияния на рост ВВП, в то время как сегодня они влияют на него больше, чем многовековая торговля товарами. Об этом говорится в докладе

⁵ Утв. Указом Президента РФ от 5 декабря 2016 г. № 646.

⁶ См.: Соколов И. А., Куприяновский В. П., Аленков В. В. и др. Цифровая безопасность умных городов // *International Journal of Open Information Technologies*. 2018. No. 1. P. 104—116.

⁷ См.: Ellison D., Venter H. An ontology for digital security and digital forensics investigative techniques (Conference Paper) // *Proceedings of the 11th International Conference on Cyber Warfare and Security (ICWS2016)*. Boston, 2016. P. 120—128.

⁸ См.: Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document. Published on October 1, 2015. URL: <http://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm>.

⁹ См.: Сухаренко А. Н. Законодательное обеспечение информационной безопасности в России // *Российская юстиция*. 2018. № 2. С. 2.

McKinsey Global Institute «Цифровая глобализация: новая эра глобальных потоков», где авторы обращают внимание на то, что этот сдвиг позволяет компаниям выходить на международные рынки с менее капиталоемкими бизнес-моделями, однако он же создает новые риски и политические проблемы¹⁰. Десятки миллионов малых и средних предприятий во всем мире превратились в экспортеров, присоединившись к таким рынкам электронной коммерции, как Alibaba, Amazon, eBay, Flipkart и Rakuten, и уже 12% мировой торговли товарами осуществляется через международную электронную торговлю. Независимо от объема стартового капитала бизнес легко становится глобальным: сотрудничество и торговлю в глобальном масштабе осуществляет 86% технологических стартапов¹¹.

Глобализированное цифровое общество рождает инновационные стратегии управления, сферы и тенденции развития культуры, экономики, права, торговли и даже мышления¹². И не всегда эти стратегии будут приводить к положительным для человека и государства итогам.

Национальное государство в определенной мере базируется на ценностях традиционной национальной культуры, на определен-

ной национально-культурной идентичности, поэтому современные отечественные ученые и публицисты так обеспокоены, в общем-то справедливо, отсутствием в современной России национальной идеи и государственной идеологии. В мировоззренческом смысле цифровая глобализация несет угрозу для государства потери традиционных нравственных ценностей, так как формальный рационализм в условиях цифрового общества становится основным инструментом и критерием правильности принимаемых решений, в то время как традиционные ценности носят иррациональный характер, базируясь на вере в Бога, жертвенности человека личными интересами во имя интересов общества (семьи, Отечества, Родины, блага государства, Церкви, общины, рода, племени и т. п.). Цифровизация несет новые риски и угрозы: дальнейшую индивидуализацию и социальную атомизацию; одиночество и потерю навыков «живой» коммуникации, виртуализацию жизни и отношений, а отсюда рост суицидов и наркологических пристрастий у молодежи; умаление права частной жизни и риск построения цифрового тоталитаризма; архаизацию общества в условиях клипового мышления «цифрового слабоумия», дерефлексивного мышления. По последствиям цифровая революция и искусственный интеллект сравнимы с изобретением парового двигателя, как это верно отмечает С. Холтел: вряд ли кто-то мог предполагать, что это изобретение вызовет огромные последствия: паровой двигатель увеличил промышленное производство, привел к социальным потрясениям, революциям и изменил политический ландшафт на следующие века¹³.

¹⁰ См.: McKinsey Global Institute. Digital Globalization: the new era of global flows. Executive Summary. 2016. March. URL: <http://www.mckinsey.com>.

¹¹ Ibid.

¹² См.: Kadar M., Moise I. A., Colomba C. Innovation Management in the Globalized Digital Society // *Procedia — Social and Behavioral Sciences*. 2014. Vol. 143. P. 1083—1089. URL: <https://doi.org/10.1016/j.sbspro.2014.07.560>; Dufva T., Dufva M. Grasping the future of the digital society // *Futures*. 2019. Vol. 107. P. 17—28. URL: <https://doi.org/10.1016/j.futures.2018.11.001>; Guy J.-S. Digital technology, digital culture and the metric/nonmetric distinction // *Technological Forecasting and Social Change*. 2019. Vol. 145. P. 55—61. URL: <https://doi.org/10.1016/j.techfore.2019.05.005>.

¹³ См.: Holtel S. Artificial Intelligence Creates a Wicked Problem for the Enterprise // *Procedia Computer Science*. 2016. Vol. 99. P. 171. URL: <https://doi.org/10.1016/j.procs.2016.09.109>.

Исследующие данную трансформацию человечества ученые констатируют: «В настоящее время осуществляется переход от логоцентрической к цифроцентрической организации жизни с ее тотальной компьютеризацией и сетевизацией. По сути, это фундаментальный, экзистенциальный процесс в эволюции человеческой культуры»¹⁴. Несомненно, цифровизация сделает мир еще более атомизированным и индивидуализированным, что явно не будет способствовать сохранению национальных суверенитетов и этнокультурных единств. Возможно, цифровизация будет использована для сохранения самобытности национально-государственных укладов, что уже можно увидеть в виртуальных музеях, сетевых формах общения и выставках, но это крайне тяжело осуществлять при господстве цифровых технологий в идейно-ценностных стандартах западноевропейского мира. Пока цифровизация протекает в рамках последнего: именно Запад, являясь лидером в технологическом прогрессе, разрабатывает стандарты цифровой глобализации.

Цифровая глобализация и суверенитет. Государство все больше теряет статус монополиста в привычных сферах: правотворчества, управления, валютного регулирования, правосудия и т. д. Концепция «мягкого права» приходит на смену этатистскому юридическому позитивизму, банки предлагают выдавать паспорта и иные документы, образовательные организации через онлайн-обучение разрушают границы между странами и континентами, валютный рынок с помощью криптовалют пытается жить самостоятельно и т. д. Например, в связи с ростом интернет-торговли возникают и уже функционируют интернет-суды: первый интернет-

суд открылся в китайском городе Ханчжоу, однако сейчас такие суды создаются и в других странах, например в Канаде¹⁵. Президент Центра глобальных интересов (Вашингтон, США) Н. Злобин заявляет: «Суверенные государства теряют свои возможности монопольно управлять главными процессами на собственных территориях. Мировая экономика становится все более глобальной, взаимосвязанной и разветвленной, в ней уже очень трудно, а зачастую невозможно провести границы между различными национальными экономиками. Бизнес стал по природе своей межгосударственным. Как, впрочем, и финансовая система, которая сегодня уже не может быть организована “по национальному признаку”, а функционирует как единый, пусть и не очень здоровый, глобальный механизм»¹⁶.

Среди задач государственным органам на Всемирной встрече на высшем уровне по вопросам информационного общества фигурируют следующие: «...g) органам государственного управления необходимо разработать национальные стратегии, в том числе стратегии электронного государственного управления, с тем чтобы сделать государственное управление более прозрачным, эффективным и демократичным; h) разработать основу для безопасного хранения и архивирования документов и других электронных информационных записей»¹⁷. При этом основными разработчиками тех-

¹⁵ См.: Аббасова Е. В., Васильев В. А. Трудовое право в цифровой реальности: проблемы интеграции // Российская юстиция. 2019. № 4. С. 17.

¹⁶ Злобин Н. Правило «мягкой силы» // Российская газета. 2013. 29 марта.

¹⁷ Документ WSIS-03/GENEVA/DOC/5-R от 12 декабря 2003 г. — Женевский «План действий по построению глобального информационного общества». URL: <https://docplayer.ru/33746414-Dokument-wsis-03-geneva-doc-5-r-12-dekabrya-2003-goda-original-angliyskiy-plan-deystviy.html>.

¹⁴ Лапшин А. О. Глобализация и цифровое общество: заметки на полях // Власть. 2019. № 1. С. 64.

нологий электронного правительства являются транснациональные корпорации со штаб-квартирами в США: Oracle, Microsoft, IBM, Hewlett Packard, Twitter, Mozilla, Intel, Apple, Cisco Systems. Выдающихся успехов в программе импортозамещения в России добилась компания Oracle: объем закупок программного обеспечения, разработанного этой фирмой, госструктурами и госкомпаниями в 2018 г. достиг максимума за последние пять лет — 13,3 млрд руб.¹⁸

Принципы глобального партнерства, а по сути, цифровой глобализации в деле построения цифровой экономики, цифрового образования, правительства и прочего прописаны и в других международных документах. Среди них документы, подписанные на саммитах G20 в Германии в 2017 г.¹⁹ и в Аргентине в 2018 г. На самом высшем уровне регулярно проходят встречи по построению единого глобального цифрового общества на базе Международного телекоммуникационного союза, куда входят 193 государства мира и около 800 частных корпораций. Такой саммит на тему «Информационно-коммуникационные технологии для достижения целей в области устойчивого развития» проходил в Женеве 8—12 апреля 2019 г.²⁰

Эти же идеи культивирует концепция построения «единого наднационального глобального сетевого информационно-сотового общества» будущего, которое в качестве программной цели закрепила Хар-

тия глобального информационного общества, подписанная на Окинаве руководителями государств «Большой восьмерки». Международные встречи в Женеве (2003 г.) и Тунисе (2005 г.), проходившие при участии делегатов из Российской Федерации, подтвердили данный курс развития миросистемы. С той поры на ежегодных встречах делегаты из нашей страны отчитываются о результатах внедрения цифровых технологий в государственное управление и создание электронного правительства на основе выработанных международных стандартов.

Между тем стимулирование цифрового развития в сфере государственного управления должно осуществляться через серьезное обсуждение среди философов, культурологов, правоведов, специалистов в сфере национальной безопасности. Именно зарубежные корпорации занимаются в нашей стране внедрением электронного правительства и его технологических узлов²¹. В 2009 г. Евросоюз выделил 2 млн евро на развитие в Российской Федерации технологий и структур электронного правительства. Осваивать деньги и разрабатывать технологии было поручено корпорации GDSI (Galway Development Services International) из Ирландии, а также немецкой компании Steinbeis GmBH. «Открытому правительству» помогают и ведомства, переводя в формат открытых данных различные сведения. Если добавить к этому создание единой базы данных со всей документацией на каждого гражданина, о которой давно говорят первые лица государства²², то вполне очевидной станет уязвимость государства и его безопасности для внешней агрессии.

¹⁸ См.: *Балашова А.* Oracle установила рекорд продаж в России на фоне импортозамещения софта. Почему госструктуры и госкомпании продолжают закупать американское ПО. URL: https://www.rbc.ru/technology_and_media/29/04/2019/5cc48a549a79475b870c850e?from=newsfeed.

¹⁹ См.: Декларация лидеров «Группы двадцати». URL: <http://www.kremlin.ru/supplement/5373>.

²⁰ См.: Форум ВВУИО 2019 г. URL: <https://www.itu.int/net4/wsis/forum/2019/ru>.

²¹ См.: *Орлов П.* Электронный начальник. URL: <https://rg.ru/2009/12/14/electron-pravitelstvo-site.html>.

²² См.: *Кольдина А.* Свежая голова. URL: <https://rg.ru/2018/02/20/valentina-petrenko-obshchaia-baza-dokumentov-v-razy-uprostit-zhizn.html>.

Процесс цифровизации государственного управления, таким образом, серьезно влияет на прозрачность и доступность его для внешнего контроля. Кроме того, стиль государственного управления, его методы и средства, формы и модели теряют культурные, национально-самобытные корни и особенности. Ранее не было сомнения в том, что государственное управление имеет культурное значение, является и порождением, и генератором национально-культурного творчества народа, населения. Цифровизация стандартизирует, унифицирует стили и формы государственного управления.

«Умный город» (Smart City) и технологическая зависимость. Определенные риски суверенитету государства, безопасности личности, общества и государства возникают и в связи с развитием «умных городов». Большую роль в этом процессе играют Великобритания и США. Разрабатываемые ими унифицированные и стандартизированные шаблоны их моделирования и развития, первоначально возникшие на уровне национальных проектов, постепенно становятся образцами на международном уровне. «Умные города» критически зависят от систем сбора данных, распределения информационных потоков, поступающих с огромного количества датчиков, обрабатываемых с помощью программных алгоритмов искусственного интеллекта, используемых в благих целях обеспечения безопасности граждан, решения и предупреждения экологических, экономических, социальных, инфраструктурных и иных проблем. Стандарты кибербезопасности разрабатываются в Великобритании, ставшей лидером по развитию технологического и нормативного сопровождения умных городов²³. Например, существует специальный

словарь, определяющий термины в системах управления «умным городом», формирующий концептуальные основы, виды данных и многое другое. Кстати, данная система нацеливает на необходимость наличия общегородского хранилища данных о жителях города и информационных объектах из самых различных источников — начиная с медучреждений и заканчивая правоохранительными органами. Данная база данных называется «Открытые данные», и она может быть использована для различных нужд и потребностей²⁴.

Типичный «умный город» состоит из четырех ключевых компонентов: «умные сети», системы автоматизации зданий (BAS), беспилотные летательные аппараты (БЛА), Smart Vehicles (с включением датчиков интернет-вещей (IoT) и облачной платформы)²⁵. Сочетания этих элементов могут порождать абсолютно новые виды преступлений, и обеспечение надежной и сквозной безопасности является непростой задачей. Трудности ожидают и с позиции уязвимости элементов «умных городов» от трансграничных воздействий и кибератак со стороны стран-противников.

Интернет вещей, роботизация. «Интернет-вещи», или «умные вещи», представляют собой высокотехнологичные, интеллектуализированные устройства, подключенные к Интернету, прежде всего промышленные и потребительские товары, бытовую технику, видеонаблюдение и т. п. Одно из определений термина «интернет-вещи» было

²⁴ См.: Куприяновский В. П., Уткин Н. А., Николаев Д. Е. и др. О локализации британских стандартов для Умного Города // International Journal of Open Information Technologies. 2016. Vol. 4. No. 7. P. 14.

²⁵ См.: Baig Z. A., Szweczyk P., Valli C. et al. Future challenges for smart cities: Cybersecurity and digital forensics // Digital Investigation, 22. 2017. P. 3. URL: <https://doi.org/10.1016/j.diin.2017.06.015>.

²³ См.: Соколов И. А., Куприяновский В. П., Аленков В. В. и др. Указ. соч. С. 105.

представлено в п. 3.2.2 Рекомендации Международного союза электросвязи Y.2060 (06/2012): это «глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий»²⁶. Эти устройства легко уязвимы для кибератак, несанкционированного сбора данных для спецслужб зарубежных государств, корпораций, мошенничества и злоупотребления, недобросовестной конкуренции поставщиков товаров и услуг. Например, холодильник с функцией дозаказа продуктов и их покупки в автоматическом режиме может выбирать определенных поставщиков не без помощи удаленного взлома или программирования на этапе производства. При этом программное обеспечение и электронные схемы скрыты от контроля: они защищены как секрет производства (ст. 1465 ГК РФ). По всей видимости, потребуются внесение изменений в федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», от 27 июля 2006 г. № 152-ФЗ «О персональных данных» с целью защитить пользователей интернет-вещей, а также от недобросовестной конкуренции участников рынка. Отметим, что весьма спорной выглядит концепция некоторых авторов, предлагающих строго концептуальное отделение личных (персональных) данных от личной информации и оспарива-

ние применимости концепции собственности к личной информации в контексте интернет-вещей²⁷. Особенно важно определиться с личной информацией в сфере медицинских интернет-вещей: это медицинские изделия, которые с помощью специальных датчиков собирают информацию о пациенте и воздействуют на его здоровье. Это не только фитнес-браслеты, но и устройства, предназначенные для мониторинга, контроля и поддержания состояния здоровья, в том числе инсулиновые и инфузионные помпы, кардиостимуляторы, аппараты искусственного дыхания, электрокардиографы. «Умные устройства данного сегмента позволяют обеспечивать бесперебойный мониторинг уровня кровяного давления, могут в автоматическом режиме вводить необходимые лекарства (в частности, инсулин, химиотерапевтические препараты), снимать кардиограммы и т. д.»²⁸.

Быстрый рост таких устройств, а также роботизированных и алгоритмизированных киберфизических систем в условиях трансграничной торговли, используемой вне доступа государства в сфере частной собственности, может стать большой угрозой личной безопасности. Системы «умного дома», собирающие и хранящие личные данные, обрабатывающие их для обслуживания клиентов с помощью искусственного интеллекта, являются весьма легкими целями для взлома и сбора информации. Законодательно необходимо обязывать производителей защищать эти устройства специальными программами защиты. Кроме

²⁶ Багоян Е. Г. Информационная безопасность и применение технологии блокчейн: зарубежный опыт и необходимость правового регулирования в Российской Федерации // Юрист. 2019. № 3. С. 42. DOI: 10.18572/1812-3929-2019-3-42-49.

²⁷ См.: Janeček V. Ownership of personal data in the Internet of Things // Computer Law & Security Review. 2018. Vol. 34. Iss. 5. P. 1040. URL: <https://doi.org/10.1016/j.clsr.2018.04.007>.

²⁸ Смирнова К. М. Проблема информационной безопасности в контексте использования «Интернета вещей» в медицине // Медицинское право. 2019. № 1. С. 31.

того, следует законодательно определить сферы, в которых применение интернет-вещей и искусственного интеллекта неприемлемо: вызывает опасения тенденция устранения человека из ряда видов деятельности, например образования, медицины, транспорта, связи, правосудия.

Право вполне эффективно может регулировать и определять каналы внедрений технологических инноваций. Опасаться заурегулированности или торможения технологического развития не стоит, как показывает законотворческий опыт других стран, весьма эффективно регулирующих вопросы анонимности в Интернете, идентификации пользователей, взаимодействия спецслужб и разработчиков программного обеспечения, использования роботов в тех сферах, где их применение нежелательно в силу ряда причин, например общественной значимости тех или иных профессий, видов деятельности или технологической безработицы.

Идентификация личности и право на бесцифровую среду. На сегодняшний день идентификация личности осуществляется либо по биометрическим признакам человека, либо с помощью специальных устройств, в том числе имплантируемых. Всеобщий и обязательный для всех сбор биометрических параметров человека для хранения и идентификации недопустим с точки зрения прав человека на частную жизнь: принцип добровольности, точнее принцип «неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия», закрепленный в ст. 3 Федерального закона «Об информации, информационных технологиях и о защите информации», в условиях цифрового общества и государства становится основополагающим с точки зрения воспрепятствования цифровым формам тотальной

диктатуры. «Электронный двойник» физического лица не должен стать отправной точкой в построении цифровой системы государственного управления.

В связи с этим возникает вопрос о перспективах безопасности единой системы цифровой аутентичности и идентичности человека, о доступе к этой системе различных государственных организаций и должностных лиц. Большую опасность вызывает и возможность доступа к этим системам зарубежных государственных организаций и транснациональных корпораций, что в условиях вовлечения банков в процесс биометрической идентификации населения трудно ограничить. Кроме того, данная система является важным узлом внедряемой в России модели электронного правительства, что представляет собой одну из задач в построении единого глобального информационного общества. Решение видится в нормативном ограничении возможности доступа к этим системам различным структурам с установлением уголовной ответственности за нарушение правил работы с ними.

В Великобритании реализация прав человеком не зависит от наличия у него единого документа (паспорта): паспорта граждане этой страны обязаны получать только в случае перемещения за рубеж. В Германии правительство отказалось от идеи концентрации сведений о персональных данных на одном сервере или в одной базе данных из соображений национальной безопасности и безопасности человека, жителей страны: «Федеральный конституционный суд — высший суд ФРГ, следящий за соблюдением Основного закона, еще 30 лет назад постановил: единого средства сохранения всех данных о личности не должно быть. Ведь каждый гражданин по конституции имеет право на информационную тайну, а государство, в свою очередь, неправомочно следить за гражданами, со-

бирать и в централизованном порядке сохранять данные о них». Во Франции также единый электронный документ отказались внедрять, назвав его «тоталитарным и в высшей степени вредным»²⁹. В США паспорта требуются при выезде за границу, нет единого документа, который обязательно выдается каждому гражданину³⁰.

В Стратегии развития электронной промышленности России на период до 2025 г.³¹ фиксируется иной подход — в качестве цели видится единство человека и цифровой реальности: «Внедрение нанотехнологий должно еще больше расширить глубину ее проникновения в повседневную жизнь населения. Должна быть обеспечена постоянная связь каждого индивидуума с глобальными информационно-управляющими сетями типа Internet. Наноэлектроника будет интегрироваться с биообъектами и обеспечивать непрерывный контроль за поддержанием их жизнедеятельности, улучшением качества жизни, и таким образом, сокращать социальные расходы государства». Данная программа развития наряду с созданием единого федерального информационного ресурса, содержащего сведения о населении, порождает новые угрозы и риски в сфере прав человека³². Для России риски тоталитарного контроля неизмеримо

выше в силу ее исторического опыта и привычного пренебрежения правами человека.

Кроме того, имплантация чипов для идентификации человека в целях доступа и платежного средства логически абсурдна: чип должен быть легко подделываемым, так как тогда у злоумышленника меньше стимулов насильно принуждать его носителя к использованию или извлекать его из тел жертв. Но в таком случае смысл его использования в качестве платежного средства пропадает — более безопасным для жизни и здоровья пользователя является привычный способ расчета пластиковыми картами.

В связи с этим большой интерес представляют возможности установления ограничений и запретов использования единого идентификатора, а также хранения единого информационного массива с персональными данными граждан из соображений цифровой безопасности личности, ее конституционных прав и свобод. Недопустима имплантация в тело человека цифровых идентификаторов, кроме медицинских показаний, так как это вызывает изменения в природе человека. Государством, точнее его отдельными ведомствами, часто ведется неконтролируемый гражданами сбор данных, явно избыточных для обеспечения управленческого процесса, особенно в образовательных организациях.

Не следует забывать и о том, что в Стратегии развития информационного общества в Российской Федерации на 2017—2030 гг.³³ к основным задачам применения информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства относят и сохра-

²⁹ См.: Дмитриева О. Без «бумажки» — человек. URL: <https://rg.ru/2011/02/11/dokumenty-site.html>.

³⁰ См.: Купцова М. Права — всем голова. URL: <https://rg.ru/2013/12/02/pasporta.html>.

³¹ Утв. приказом Минпромэнерго РФ от 7 августа 2007 г. № 311.

³² См. распоряжение Правительства РФ от 4 июля 2017 г. № 1418-р «Об утверждении Концепции формирования и ведения единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации» (вместе с «Планом мероприятий (“дорожной картой”) по формированию и ведению единого федерального информационного ресурса, содержа-

щего сведения о населении Российской Федерации»).

³³ Утв. Указом Президента РФ от 9 мая 2017 г. № 203.

нение возможности взаимодействия граждан с государственными и муниципальными организациями без применения информационных технологий.

Искусственный интеллект и правоприменение: риски и ограничения. Следует обратить внимание на угрозы безопасности человека, дегуманизации и технократизации правоприменения, возникающие в связи с внедрением искусственного интеллекта в правоприменительную деятельность. Этот путь развития права и правосудия будет только усугублять недостатки явно ошибочного, логоцентристского, позитивистского восприятия права, формально-догматического правопонимания. И дело здесь не в том, что с точки зрения искусственного интеллекта нормы права в тоталитарном государстве ничем не отличаются от норм, закрепленных в современных социальных государствах, например Дании или Финляндии. Еще в середине XX в. ученые фиксировали кризис права: юридический формализм стал господствовать над содержательной гранью права. Задолго до цифровизации представители западной интеллектуальной элиты фиксировали нарастающий кризис европейской традиции права, вызванный избыточной формальной рациональностью, механистическим мировосприятием права и правосудия, доминированием формальной законности над справедливостью. Известный историк права Г. Дж. Берман отмечает, что человек Запада находится в гуще беспрецедентного кризиса правовых ценностей и правового мышления. Право воспринимается все больше как «мешанина, каша из сиюминутных решений и противоречащих друг другу норм, соединенных только общими “приемами”, “техникой”»³⁴. Право становится все больше политическим и прагматическим, не свя-

зываемым с какими-либо высшими принципами и ценностями, историческими и культурными корнями. Именно поэтому христианский по своему происхождению европейский индивидуализм постепенно трансформируется в социальный атомизм, гуманизм — в трансгуманизм, а либерализм — в социал-дарвинизм.

Расцвет и господство юридического формализма следует рассматривать как процесс отчуждения человека от права. Его также можно считать «перерождением формальной рациональности»: формально-рациональное начало, обязанное своим появлением проблеме поиска справедливости «невзирая на лица» в рамках «здорового» формализма, призванного в качестве средства обеспечить справедливость на началах равенства, обернулось и заняло место цели, т. е. достижения этой справедливости. Говоря коротко: средство (законность) стало самоцелью. Немецкий социолог К. Зейфарт пишет: «Специфически юридическое, то есть формально-рациональное качество права, обязанное своим образованием именно профессионалам-юристам, очень скоро начало доминировать над содержательными (“материальными”) элементами правовой деятельности. В результате собственно творческий аспект деятельности юристов редуцируется и вообще утрачивает свою силу. Происходит эмпирически фиксируемое превращение юридического процесса в нечто “аналогичное производству”, где все сводится к формально-логическому подведению индивидуального под всеобщее»³⁵. Заметим, что речь идет о юристах — людях, способных переживать и сочувствовать, а что можно ожидать от роботов-юристов? Объективность в правоприменении

³⁴ Берман Г. Дж. Западная традиция права: эпоха формирования. М., 1994. С. 13, 50.

³⁵ Цит. по: Гайденок П. П., Давыдов Ю. Н. История и рациональность: Социология М. Вебера и веберовский ренессанс. М., 1991. С. 311.

посредством искусственного интеллекта достигнуть невозможно и не нужно, так как система правовых норм представляет собой прежде всего систему ценностей, защищенных этими нормами. К тому же эта система носит иерархический характер, что предполагает постоянное сопоставление средств и целей, т. е. целеполагание, оценку, субъективность.

Именно достижение объективности предполагается использованием искусственного интеллекта в правоприменительном процессе. Но дело в том, что возможность использования искусственного интеллекта на современном этапе его проектирования, точнее сказать, обоснование этой возможности и пределы его использования должны быть связаны с изучением эпистемологических характеристик правового мышления, логических аспектов правоприменительной деятельности, с логическим анализом правового мышления, правоприменительного познания. Искусственный интеллект не обладает важнейшими предпосылками, свойствами и качествами человеческого интеллекта и сознания, а именно подсознанием, переживанием, страхом смерти и потери близких, состраданием, чувствами, эмоциями, интуициями, словом, всем тем, что лежит в основе человеческого понимания, смыслообразования и творчества. Именно в юриспруденции особенно важными являются творческий компонент мышления, иррациональная основа принятия решений.

Между тем Евросоюз уже принял «Этическую хартию искусственного интеллекта в судебных системах»³⁶. Парадокс в том, что, как выяснилось, искусственные судьи еще более чем люди зависят от различных предустановок, например расовых, социально-экономических, конфес-

сиональных и иных предрассудков, так как прогнозируют поведение человека, исходя из таких фактов, как личный статус, уровень образования, занятость и т. д. Эти предустановки закладываются программистами на этапе формирования алгоритмов. Человеческое мышление оказалось значительно гибче — точнее и глубже определяя правовые выводы.

Внедрение искусственного интеллекта в правосудие влечет дальнейшую дегуманизацию права, увеличивает риски неправосудных и несправедливых решений. Сопереживание и сочувствие играют крайне важную роль в интерпретации оценочных понятий, установлении ответственности казуса и нормы права, а здравый смысл в понимании человеческих поступков и слов неустрашим при юридической квалификации, внешне напоминающей дедуктивный силлогизм, но не являющейся им. С точки зрения эпистемологии сопоставление нормы и казуса выглядит как герменевтический круг: чтобы познать целое, надо знать его части, однако познание части невозможно без знания целого. Это логически противоречивый круг, так как норма (неоконченное множество или целое) и казус (частный случай) обретают соответствие не через логическую процедуру, а посредством интуитивного выбора, интуитивного правочувствия, приходящего с опытом правоприменительной деятельности. Это правочувствие, или желаемое право правоприменителя, возникает в конкретной ситуации в результате деятельности правосознания и правового мышления человека, аккумулирующего не только юридический опыт, но и идеалы, ценности, установки субъекта-интерпретатора, проявляющие себя явно в конкретной ситуации, являясь неосознаваемым контекстом интерпретации социально-правовой реальности. Желаемое право позволяет осуществить правовое суждение, без которого обнаружение справедливости

³⁶ См.: Бекетов А. Искусственный интеллект в суде. URL: <https://ru.euronews.com/2019/01/28/eu-robotjudge-courts>.

в конкретной ситуации невозможно. Способность правового суждения не может быть смоделирована программистами. Это — понимающая способность субъекта, вызванная необходимостью подведения конкретного случая под общее правило и установления их соответствия. Это суждение характеризуется необходимостью творческой активности, в результате которой происходят неосознанное формирование желаемого права в той или иной жизненной ситуации и вхождение в герменевтический круг нормы и казуса.

Таким образом, практически всегда правоприменение сопровождается неосознанным, не видимым поверхностному взору, неявным правотворчеством, которого искусственный интеллект осуществлять не может. Неявное правотворчество требуется в ходе осмысления нормы права в связи с конкретной ситуацией. В данном процессе происходит конкретизация нормы, представляющая собой рождение в правосознании правоприменителя нормы, конкретизирующей норму более высокого порядка, которая имеет общий характер к полностью тождественным и идентичным данному конкретному случаю ситуациям. До тех пор, пока люди не превратятся в полностью идентичных, одинаковых «биороботов», будет сохраняться коллизия между абстрактной нормой и конкретными жизненными обстоятельствами, между типичностью и индивидуальностью. Преодолеть этот разрыв искусственный интеллект и цифровизация правоприменения не смогут ввиду того, что интуиция не программируется.

Заключение. Право на безопасность в условиях цифровой эпохи может исследоваться в двух парадигмах: «безопасности цифры» и «безопасности от цифры». Эти парадигмы тесно связаны, так как ряд угроз и вызовов совпадают или не могут быть устранены без решения одной из этих задач. Однако искусственное стимулирование цифро-

визации увеличивает риски. В качестве примера могут служить системы биометрической идентификации с имплантацией. Необходимо разработать основные параметры права человека на бесцифровую среду обитания, предусмотреть возможность сохранить традиционный, бесцифровой образ жизни.

Возможно, в ближайшее время потребуются пересмотр Доктрины информационной безопасности Российской Федерации и разработка Доктрины цифровой безопасности, которая зафиксирует угрозы и риски цифровизации общественных отношений, поможет определить основные направления государственной политики в сфере обеспечения безопасности личности, общества и государства в условиях цифровизации государственного управления, экономики, права. Она должна координировать деятельность органов государственной власти, местного самоуправления, институтов гражданского общества, субъектов цифрового бизнеса, информационной среды по созданию системы гарантий безопасности в условиях цифровизации общественных отношений, прогнозировать риски и вызовы, определить понятия и механизмы обеспечения цифровой безопасности, особенно в отношении человека, сформулировать принципы применения цифровых технологий в жизни государства и общества. Ограничения и запреты необходимы для обеспечения безопасности личности, общества, государства в условиях всеобщей цифровизации, угрожающей национальному суверенитету, культурной идентичности национального государства, демократии. Государство не должно превращаться в «цифровой концлагерь», общество — в «цифровую колонию», а человек — в «цифровую личность». Эти ограничения должны быть закреплены законом, а также стать наиболее значимым и важным разделом будущего Цифрового кодекса Российской Федерации.

Библиографический список

- Baig Z. A., Szewczyk P., Valli C. et al. Future challenges for smart cities: Cyber-security and digital forensics // *Digital Investigation*, 22. 2017. URL: <https://doi.org/10.1016/j.diin.2017.06.015>.
- Dufva T., Dufva M. Grasping the future of the digital society // *Futures*. 2019. Vol. 107. URL: <https://doi.org/10.1016/j.futures.2018.11.001>.
- Ellison D., Venter H. An ontology for digital security and digital forensics investigative techniques (Conference Paper) // *Proceedings of the 11th International Conference on Cyber Warfare and Security (ICCWS2016)*. Boston, 2016.
- Guy J.-S. Digital technology, digital culture and the metric/nonmetric distinction // *Technological Forecasting and Social Change*. 2019. Vol. 145. URL: <https://doi.org/10.1016/j.techfore.2019.05.005>.
- Holtel S. Artificial Intelligence Creates a Wicked Problem for the Enterprise // *Procedia Computer Science*. 2016. Vol. 99. URL: <https://doi.org/10.1016/j.procs.2016.09.109>.
- Janeček V. Ownership of personal data in the Internet of Things // *Computer Law & Security Review*. 2018. Vol. 34. Iss. 5. URL: <https://doi.org/10.1016/j.clsr.2018.04.007>.
- Kadar M., Moise I. A., Colomba C. Innovation Management in the Globalized Digital Society // *Procedia — Social and Behavioral Sciences*. 2014. Vol. 143. URL: <https://doi.org/10.1016/j.sbspro.2014.07.560>;
- McKinsey Global Institute. Digital Globalization: the new era of global flows. Executive Summary. 2016. March. URL: <http://www.mckinsey.com>.
- Аббасова Е. В., Васильев В. А. Трудовое право в цифровой реальности: проблемы интеграции // *Российская юстиция*. 2019. № 4.
- Багоян Е. Г. Информационная безопасность и применение технологии блокчейн: зарубежный опыт и необходимость правового регулирования в Российской Федерации // *Юрист*. 2019. № 3. DOI: 10.18572/1812-3929-2019-3-42-49.
- Балашова А. Oracle установила рекорд продаж в России на фоне импортозамещения софта. Почему госструктуры и госкомпании продолжают закупать американское ПО. URL: https://www.rbc.ru/technology_and_media/29/04/2019/5cc48a549a79475b870c850e?from=newsfeed.
- Баранова Н. Что такое цифровая безопасность: термины и технологии. URL: <https://te-st.ru/2018/05/25/digital-security-terms/>.
- Бекетов А. Искусственный интеллект в суде. URL: <https://ru.euronews.com/2019/01/28/eu-robojudge-courts>.
- Берман Г. Дж. Западная традиция права: эпоха формирования. М., 1994.
- Гайденок П. П., Давыдов Ю. Н. История и рациональность: Социология М. Вебера и веберовский ренессанс. М., 1991.
- Дмитриева О. Без «бумажки» — человек. URL: <https://rg.ru/2011/02/11/dokumenty-site.html>.
- Ефремов А. А. Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве // *Информационное право*. 2016. № 4.
- Злобин Н. Правило «мягкой силы» // *Российская газета*. 2013. 29 марта.
- Кольдина А. Свежая голова. URL: <https://rg.ru/2018/02/20/valentina-petrenko-obshchaia-baza-dokumentov-v-razy-uprostit-zhizn.html>.
- Куприяновский В. П., Уткин Н. А., Николаев Д. Е. и др. О локализации британских стандартов для Умного Города // *International Journal of Open Information Technologies*. 2016. Vol. 4. No. 7.
- Купцова М. Права — всем голова. URL: <https://rg.ru/2013/12/02/pasporta.html>.
- Лапшин А. О. Глобализация и цифровое общество: заметки на полях // *Власть*. 2019. № 1.
- Овчинников А. И., Самарин А. А. Перспективы развития современного права: экстерриториальность, трансграничность, сетевая множественность // *Философия права*. 2015. № 3 (70).
- Орлов П. Электронный начальник. URL: <https://rg.ru/2009/12/14/electron-pravitelstvo-site.html>.
- Саломатин К., Буртин И. Заводной мандарин. Узники китайских лагерей рассказывают про общество будущего // *Русский репортер*. 2019. № 10 (475).

Смирнова К. М. Проблема информационной безопасности в контексте использования «Интернета вещей» в медицине // Медицинское право. 2019. № 1.

Соколов И. А., Куприяновский В. П., Аленков В. В. и др. Цифровая безопасность умных городов // International Journal of Open Information Technologies. 2018. No. 1.

Сухаренко А. Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2.

References

Abbasova E. V., Vasil'ev V. A. Labor law in digital environment: problems of integration. *Rossiyskaya yustitsiya*, 2019, no. 4, pp. 16—18. (In Russ.)

Bagoyan E. G. Information Security and Application of Blockchain Technologies: Foreign Experience and the Need for Legal Regulation in the Russian Federation. *Yurist*, 2019, no. 3. DOI: 10.18572/1812-3929-2019-3-42-49, pp. 42—49. (In Russ.)

Baig Z. A., Szweczyk P., Valli C. et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 2017, no. 22. Available at: <https://doi.org/10.1016/j.diin.2017.06.015>.

Balashova A. Oracle has set a sales record in Russia amid import substitution software. Why government agencies and state-owned companies continue to purchase American software. Available at: https://www.rbc.ru/technology_and_media/29/04/2019/5cc48a549a79475b870c850e?from=newsfeed. (In Russ.)

Baranova N. What is digital security: terms and technologies. Available at: <https://te-stru/2018/05/25/digital-security-terms/>. (In Russ.)

Beketov A. Artificial intelligence in court. Available at: <https://ru.euronews.com/2019/01/28/eu-robojudge-courts>. (In Russ.)

Berman G. Dzh. Western tradition of law: the era of formation. Moscow, 1994. 590 p. (In Russ.)

Dmitrieva O. Without a piece of paper — a man. Available at: <https://rg.ru/2011/02/11/dokumenty-site.html>. (In Russ.)

Dufva T., Dufva M. Grasping the future of the digital society. *Futures*, 2019, vol. 107. Available at: <https://doi.org/10.1016/j.futures.2018.11.001>.

Efremov A. A. Problems of realization of the conception of Digital Security Risk Management of OECD in Russian legislation. *Informatsionnoe pravo*, 2016, no. 4, pp. 25—28. (In Russ.)

Ellison D., Venter H. An ontology for digital security and digital forensics investigative techniques (Conference Paper). *Proceedings of the 11th International Conference on Cyber Warfare and Security (ICWS2016)*. Boston, 2016.

Gaydenko P. P., Davydov Yu. N. History and Rationality: The Sociology of M. Weber and the Weber Renaissance. Moscow, 1991. 367 p. (In Russ.)

Guy J.-S. Digital technology, digital culture and the metric/nonmetric distinction. *Technological Forecasting and Social Change*, 2019, vol. 145. Available at: <https://doi.org/10.1016/j.techfore.2019.05.005>.

Holtel S. Artificial Intelligence Creates a Wicked Problem for the Enterprise. *Procedia Computer Science*, 2016, vol. 99. Available at: <https://doi.org/10.1016/j.procs.2016.09.109>.

Janeček V. Ownership of personal data in the Internet of Things. *Computer Law & Security Review*, 2018, vol. 34, iss. 5. Available at: <https://doi.org/10.1016/j.clsr.2018.04.007>.

Kadar M., Moise I. A., Colomba C. Innovation Management in the Globalized Digital Society. *Procedia — Social and Behavioral Science*, 2014, vol. 143. Available at: <https://doi.org/10.1016/j.sbspro.2014.07.560>;

Kol'dina A. Fresh head. Available at: <https://rg.ru/2018/02/20/valentina-petrenko-obshchaia-baza-dokumentov-v-razy-uprostit-zhizn.html>. (In Russ.)

Kupriyanovskiy V. P., Utkin N. A., Nikolaev D. E. et al. On Localization of British Standards for Smart Cities. *International Journal of Open Information Technologies*, 2016, vol. 4, no. 7, pp. 13—21. (In Russ.)

Kuptsova M. Rights are the head of all. Available at: <https://rg.ru/2013/12/02/pasporta.html>. (In Russ.)

Lapshin A. O. Globalization and digital society: notes in the margin. *Vlast'*, 2019, no. 1, pp. 63—68. (In Russ.)

McKinsey Global Institute. Digital Globalization: the new era of global flows. Executive Summary. 2016. March. Available at: <http://www.mckinsey.com>.

Orlov P. Electronic boss. Available at: <https://rg.ru/2009/12/14/electron-pravitelstvo-site.html>. (In Russ.)

Ovchinnikov A. I., Samarin A. A. Perspectives of the modern law development: extraterritoriality, transboundary, network plurality. *Filosofiya prava*, 2015, no. 3 (70), pp. 8—14. (In Russ.)

Salomatin K., Burtin Sh. Clockwork Mandarin. Prisoners of Chinese camps talk about the society of the future. *Russkiy reporter*, 2019, no. 10 (475), pp. 13—22 (In Russ.)

Smirnova K. M. The Information Security Issue in View of the Use of the Internet of Things in Medicine. *Meditinskoe pravo*, 2019, no. 1. pp. 31—37. (In Russ.)

Sokolov I. A., Kupriyanovskiy V. P., Alen'kov V. V. et al. On digital security of smart cities. *International Journal of Open Information Technologies*, 2018, no. 1, pp. 104—118. (In Russ.)

Sukharensko A. N. Legislative support for information security in Russia. *Rossiyskaya yustitsiya*, 2018, no. 2, pp. 2—5. (In Russ.)

Zlobin N. Pravilo “myagkoy sily”. *Rossiyskaya gazeta*, 2013, March 29.