Вестник РУДН. Серия: Юридические науки 2023 Т. 27. № 1. 97—116
RUDN JOURNAL OF LAW. ISSN 2313-2337 (print), ISSN 2408-9001 (online) http://journals.rudn.ru/law

ПРАВО И ЦИФРОВЫЕ ТЕХНОЛОГИИ

LAW AND DIGITAL TECHNOLOGY

https://doi.org/10.22363/2313-2337-2023-27-1-97-116

Научная статья / Research Article

Конституционализация информационной безопасности в российском праве: проблема совершенствования теоретической модели

Ю.А. Гаврилова

Волгоградский государственный университет, *г. Волгоград, Российская Федерация*
✉gavrilova_ua@volsu.ru

Аннотация. Анализируется одна из конституционных поправок 2020 года. В соответствии с новой редакцией пункта «м» части 1 статьи 71 Конституции РФ к исключительным полномочиям Российской Федерации отнесены вопросы обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных. Закрепление проблемы информационной безопасности на конституционном уровне определяет необходимость частичной модернизации ее теоретической модели. Модификация и переосмысление некоторых ее составляющих приведет к повышению эффективности конституционной регламентации и улучшению качества применения отраслевого законодательства в области информационных технологий и защиты информации. Цель исследования — изучить основные направления совершенствования теоретической модели информационной безопасности с учетом конституционных изменений. Применены методы: формально-юридический, логический, системный, статистический, структурно-функциональный, моделирование, прогнозирование. Уточнено понятие информационной безопасности, предложено обобщить круг базовых субъектов общественных отношений, связанных с обеспечением информационной безопасности, расширить их права и обязанности, выделить конституционный и отраслевые правовые режимы защиты информации, усилить ответственность за правонарушения в информационной сфере. Выводы. Совершенствование теоретической модели информационной безопасности Российской Федерации следует проводить по следующим ключевым направлениям. Во-первых, развитие целевых ориентиров информационной безопасности, выраженных в стратегических и программных документах государства. Во-вторых, уточнение классификации угроз информационной безопасности. В-третьих, расширение плотности нормативно-правового регулирования. В-четвертых, усиление правообеспечительных механизмов информационной безопасности. В-пятых, установление и поддержание

оптимального баланса между правовым, техническим и этическим регулированием информационных технологий, прежде всего цифровых технологий. В-шестых, определение допустимых и недопустимых границ применения информационных технологий и цифровых данных в жизни людей.

Ключевые слова: личность, общество, государство, безопасность, информационные технологии, цифровые данные, конституционный режим, отраслевые режимы

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Дата поступления в редакцию: 12 марта 2022 г.
Дата принятия к печати: 15 января 2023 г.

Для цитирования:

Гаврилова Ю.А. Конституционализация информационной безопасности в российском праве: проблема совершенствования теоретической модели // RUDN Journal of Law. 2023. Т. 27. № 1. С. 97—116. https://doi.org/10.22363/2313-2337-2023-27-1-97-116

The Constitutionalization of information security in Russian Law: improving the theoretical model

Yulia A. Gavrilova ✉

Volgograd State University, *Volgograd, Russian Federation*
✉gavrilova_ua@volsu.ru

Abstract. Research discusses one of the constitutional amendments of 2020. In accordance with the new version of paragraph “m” of Part 1 of Article 71 of the Constitution of the Russian Federation, the exclusive powers of the Russian Federation include issues of ensuring the security of the individual, society and the state when applying information technologies, and digital data turnover. The consolidation of the problem of information security at the constitutional level determines the need for a partial modernization of its theoretical model. Modification and revision of some of its components will lead to higher effectiveness of constitutional regulation and improve the quality of application of industry legislation in the field of information technology and information protection. The purpose of the research is to investigate the main directions of enhancing the theoretical model of information security in terms of constitutional changes. The employed research methods are formal-legal, logical, system, statistical, structural-functional, modeling, and forecasting. The outcome of the study can be outlined as follows. The research clarifies the concept of information security, proposes to generalize the range of basic subjects of public relations related to information security, expand their rights and obligations, highlight the constitutional and sectoral legal regimes of information protection, and strengthen responsibility for offenses in the information sphere. In conclusion the study argues that updating the theoretical model of information security of the Russian Federation should be carried out in the following key areas: firstly, developing information security targets expressed in strategic and program documents of the state; secondly, clarifying classification of information security threats; thirdly, expanding legal regulation density; fourth, strengthening the law-enforcement mechanisms of information security; fifth, establising and maintening optimal balance between legal, technical and ethical regulation of information technologies, primarily digital technologies; and finally, definiing acceptable and unacceptable boundaries of application of information technology and digital data in people's lives.

Key words: personality, society, state, security, information technology, digital data, constitutional regime, sectoral regimes

Conflicts of interest. The author declares no conflict of interest.

Article received 12rd March 2022
Article accepted 15th January 2023

For citation:

Gavrilova, Yu. A. (2023) The Constitutionalization of information security in Russian Law: improving the theoretical model. *RUDN Journal of Law.* 27 (1), 97—116. (in Russian). https://doi.org/10.22363/2313-2337-2023-27-1-97-116

Введение

В современном обществе проблема информационной безопасности приобрела глобальный масштаб. Благодаря развитию Интернета расширяются человеческие коммуникации по всему миру, возрастают их сложность и многообразие, скорость и прозрачность. Для общения люди используют легкие и доступные цифровые технологии, которые кажутся им прекрасными, увлекательными и интересными. Люди научились с помощью информационных ресурсов и технологий решать множество трудных и ранее неизвестных задач.

Однако параллельно с ростом информационного обмена усиливается неопределенность в понимании сущности и смысла разноплановой информации, разделении информационной «правды» и «лжи», прогнозировании последствий ее использования, поиске инструментов восприятия и обработки информации массовым и индивидуальным сознанием. Информация становится в высшей степени уникальным товаром и ценностью в обществе массовой цифровизации и тотальной информатизации. Информация создает новую реальность, граничащую с подлинной реальностью, а иногда в сознании людей и отождествляемую с этой реальностью.

Значительную сложность представляет определение того, что есть информация, а что — знание? Что является правдой, а что — «неправдой» в информационной сфере? Что есть факт, а что — мнение? и т.п. Отдельные эксперты-аналитики, ученые, политики давно и метафорически называют Интернет «потоком информации», «потоком слов». Поэтому тема информационной безопасности — это во многом вопрос поиска истины в глобальном океане информации, в котором одна сторона претендует на управление и контроль за «потоком информации», а другая сторона стремится противодействовать этим процессам, защитить собственную информацию и сохранить ее безопасность.

Значение информационной безопасности велико и бесценно в современный период с точки зрения генерации и применения инновационных технологий в экономике, науке и образовании. Инновация дает качественно новое знание, обеспечивает его внедрение в производство и быт человека, улучшает качество жизни, ускоряет прогресс. Следовательно, противостояние конкурентной разведке и промышленному шпионажу сохраняет устойчивость, конкурентоспособность граждан и предприятий, обеспечивает их информационную безопасность в хозяйственном и социально-культурном секторах.

Наконец, существенно возросла роль информационной безопасности в интеллектуально-духовной сфере общества. Массовые коммуникации максимально повысили риски ценностного «переформатирования» сознания человека, утраты национальной, этнической, религиозной или профессиональной идентичности, снижения критического мышления, уровня знаний и деградации общей культуры. В связи с этим конституционная регламентация информационной безопасности отвечает задачам стратегического развития Российской Федерации. Конституционализация информационной безопасности в российском праве предопределяет совершенствование ее теоретической модели, уточненные элементы которой могут быть представлены следующим образом:

1) понятие и факторы информационной безопасности;
2) субъектный состав правоотношений;
3) технологии информационной безопасности;
4) правовые режимы.

Понятие информационной безопасности. Угрозы информационной безопасности

В соответствии с подпунктом «в» пункта 2 Доктрины информационной безопасности Российской Федерации, утвержденной указом Президента РФ № 646 от 05.12.2016 (далее — Доктрина), информационная безопасность определена как «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 Российской Федерации, оборона и безопасность государства».

При определении информационной безопасности необходимо рассматривать ее как определенный режим деятельности, направленный на минимизацию информационных рисков, ликвидацию негативных последствий, предотвращение ущерба конституционным правам и свободам личности, охраняемым законом интересам общества и государства в информационной сфере. Именно в результате такого деятельностного подхода может быть достигнуто состояние защищенности жизненно важных интересов.

Информационная безопасность — понятие более широкое, чем только нарушение или опасность нарушения порядка защищенности информации. В рамках онтологического подхода субъект правовых отношений воспринимает информационную безопасность не только через формы негативных проявлений (угроз, рисков, вызовов), но и через позитивные эмоциональные реакции (уверенность, спокойствие, благополучие в обладании или распоряжении необходимой информацией).

Наконец, ключевым выступает структурно-функциональное понимание информационной безопасности через призму объектов, защищаемых от информационных угроз, и выполняемых ими функций. По этому основанию можно выделить компонентный состав информационной безопасности: 1) безопасность

устройств и оборудования; 2) безопасность данных (формализованной информации); 3) безопасность технологий; 4) безопасность сетей связи; 5) безопасность приложений.

Согласно п. 2.4.5 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» безопасность данных — это состояние защищенности данных, при котором обеспечены их конфиденциальность, доступность и целостность. В справочном приложении А к ГОСТУ Р отмечено, что конфиденциальность данных — это передача данных третьим лицам только с согласия обладателя информации и исключение несанкционированного доступа посторонних лиц к этой информации. Доступность информации — это отсутствие препятствий для ее получения. Целостность данных — это их неизменность либо незначительное контролируемое изменение управомоченным лицом (литеры А12, А16 и А17 приложения).

На наш взгляд, важнейшими свойствами безопасных данных выступают достоверность, релевантность и надежность данных. В современных коммуникациях возрастает более всего спрос на достоверные данные, т.е. сведения о фактах и событиях в таком виде, в каком они существуют в действительности.

Какова действительность, в которой мы живем, — это проблема философская. Социальная реальность конструируется нами через взаимное понимание в информационном общении. Часть реальности, о понимании которой мы можем договориться, рассматривается нами как «устоявшаяся» действительность, «правила игры» в информационном пространстве. Мы имеем достаточную определенность и убежденность в существовании этого положения дел.

Другая часть реальности, о понимании которой люди не могут договориться в процессе коммуникаций, интерпретируется как субъективная «правда», и относительно нее в основном и ведутся информационные войны и осуществляется информационно-психологическое воздействие на личность. Чем больше степень согласованности позиций по событиям и явлениям общественной жизни, тем более с высокой вероятностью мы можем судить о них как о «свершившихся» фактах, а не согласные лица высказывают соответственно оценочное мнение либо пытаются исказить картину событий в своих интересах. Существенные и повторяющиеся зависимости между фактами, осмысленные и представленные в абстрактных понятиях и выражениях, теориях, законах позволяют извлечь из информации знание.

Не менее важным является характеристика безопасных данных как релевантных, когда они должны относиться только к определенной предметной области действительности, в познании которой заинтересован субъект. Ошибка в определении предмета коммуникаций дорого обходится участникам информационного пространства, но главное они теряют чувство пригодности обнаруженных данных, если оказывается, что данные не относятся к сути вопроса.

Данные в информационной среде, безусловно, должны быть надежными (Zharova, 2020:55). Безопасность данных ощущается, когда относительно них имеется твердая субъективная уверенность широких социальных групп населения в их безопасных свойствах и возможностях целевого использования.

По изложенным основаниям именно в случае, если информация существует, относится к данной области отношений и совместно оценивается людьми как надежная, по отношению к такой информации можно предусматривать требования конфиденциальности, доступности и целостности.

В тексте действующего Федерального закона «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 (далее — Закон об информации) формулировки о безопасности и обеспечении защиты информации упоминаются в предмете регулирования закона (ст. 1); содержании государственного регулирования (ст. 12); положениях о безопасности персональных данных (ст. 14.1); безопасности использования доменных имен (ст. 14.2) и др. В терминологическом аппарате общее понятие информационной безопасности отсутствует. В этой связи следует дополнить статью 2 Закона об информации пунктом 1.1 следующего содержания: «безопасная информация — информация, которая отвечает требованиям достоверности, релевантности, надежности, конфиденциальности, доступности и целостности».

Требования информационной безопасности устанавливаются и реализуются в зависимости от наличия или отсутствия угроз информационной безопасности. Согласно п. 2.6.1 ГОСТ Р 50922—2006 угроза информационной безопасности — это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Тем не менее, классификация угроз информационной безопасности на внутренние и внешние в Доктрине, конечно же, не исчерпывает полного их деления.

В силу п. 5.1 ГОСТ Р 51275—2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию» по природе возникновения угрозы информационной безопасности могут быть объективные и субъективные.

Объективные угрозы не зависят в процессе возникновения от воли и деятельности человека, либо косвенно зависят от них в конечном итоге: аварийный отказ оборудования, дефекты, природные стихийные явления. Субъективные угрозы являются результатом недостаточной квалификации или небрежности (неосмотрительности) лица в получении доступа и использовании информации (утеря пароля).

В зависимости от формы вины в нарушении требований информационной безопасности угрозы могут подразделяться на преднамеренные и непреднамеренные.

Преднамеренные угрозы возникают при осознанном и целенаправленном неправомерном воздействии управомоченных лиц на информацию: передача информации лицам без права доступа к ней, передача по открытым и незащищенным каналам, сговор с конкурентами и пр. Непреднамеренные угрозы могут быть связаны с несанкционированным доступом к информации третьих лиц, организационными упущениями в системе защиты информации, ошибками персонала.

Можно выделять угрозы информационной безопасности с учетом ценностей, затрагиваемых при предоставлении и распространении информации, что частично нашло отражение в законодательстве. Например, угроза причинения вреда жизни, здоровью и имуществу граждан; угроза массового нарушения общественного порядка или общественной безопасности; угроза приостановления

или прекращения функционирования объектов критической информационной инфраструктуры Российской Федерации (ст. 10.6 Закона об информации).

Мы предлагаем также принять во внимание экстерриториальный характер современного оборота информации. По критерию масштаба действия нужно рассматривать локальные угрозы информационной безопасности (в пределах национальной территории государства); региональные (дисбалансы при налаживании информационного взаимодействия в рамках ЕАЭС); глобальные (деятельность транснациональных цифровых гигантов IT-индустрии). Глобальные вызовы национальной информационной безопасности — отличительная черта актуальной эпохи (Polyakova et al., 2018:32).

И еще один аспект классификации угроз информационной безопасности связан с источниками угроз, где предлагается различать мировоззренческие угрозы, связанные с нарушениями системы ценностей общества; научно-технические, выражающиеся в отсталости науки, зависимости от внешних факторов, низкой эффективности разработки отечественной продукции; социальные угрозы, представленные как ущемление религиозной, этнической принадлежности или нагнетание гражданских конфликтов; экономические угрозы, связанные с деструктивным воздействием на национальную денежную единицу, финансовую систему, конкуренцию и промышленные технологии; геополитические угрозы, проявляющиеся в дестабилизации международного мира, глобальной и региональной информационной безопасности.

Анализ приведенной и уточненной классификации угроз информационной безопасности показывает необходимость более четкого и развернутого закрепления перечня этих угроз в нормативных правовых актах Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (далее — Минцифры России).

Особенность трактовки понятия информационной безопасности заключается в формировании этого понятия на границах технического и правового регулирования. Право — это сильный социальный регулятор, который не должен быть пробельным, но не может быть и агрессивным, избыточным, вторгаться в сферу «юрисдикции» иных социальных норм (Vlasenko, 2018:44—46). Накопившиеся острые социальные проблемы информационной безопасности должны разрешаться правом, в то время как технические алгоритмы и информационные технологии, правила пользования техническими средствами защиты информации относятся к сфере действия технических норм.

Участники правоотношений, связанных с обеспечением информационной безопасности

Закон об информации обозначает большое количество участников информационных отношений, но, к сожалению, не все из них обязаны принимать меры по обеспечению информационной безопасности. К ним относятся обладатель информации; пользователь сети Интернет; владелец сайта в сети Интернет; оператор информационной системы; провайдер хостинга; организатор распространения информации; владелец социальной сети; владелец аудиовизуального

сервиса; оператор связи и т.д. Перечень субъектов общественных отношений при применении информационных технологий и обороте цифровых данных закреплен в ст. 2 Закона об информации, хотя в нем не дается определение всех таких участников.

Данная ситуация порождает дискуссию о субъектном составе участников правоотношений, связанных с обеспечением информационной безопасности. В первую очередь следует обратить внимание на базовых субъектов: обладателей информации и пользователей информацией.

Обладатель информации — это лицо, создавшее информацию или имеющее полномочия в силу закона или договора на разрешение или ограничение доступа к этой информации других лиц. С учетом того, что перечень явлений и процессов, которые не являются объектами авторского права, специально оговорен ст. 1259 ГК РФ, можно исходить из презумпции самостоятельного и творческого характера результата любого интеллектуального труда по поиску и производству информации. Как правило, обладатель информации в информационную эпоху выступает ее правообладателем, если не доказано обратное, поэтому ст. 2 Закона об информации должна быть дополнена после слова «обладатель» словами «(правообладатель) информации (далее, если иное не предусмотрено законом, — обладатель информации)».

Пользователь информации — это физическое или юридическое лицо, заинтересованное в получении и использовании информации для удовлетворения его потребностей и (или) получившее и использующее соответствующую информацию. Данное определение в Законе об информации не дается, поэтому в теоретической модели является общим по отношению к таким его разновидностям, как пользователь сети Интернет, пользователь информационного ресурса, пользователь поисковой системы и др.

Неоднозначно в Законе об информации употребляются такие терминологические константы, как владелец, организатор, оператор. Думается, что в рамках теоретической модели информационной безопасности все названные лица могут быть объединены с помощью конструкции «агент информационной инфраструктуры».

Это можно объяснить тем, что такие лица организуют взаимодействие между обладателями информации и пользователями, а также между пользователями в информационно-телекоммуникационных сетях, в том числе сети Интернет. Деятельность указанных субъектов носит посреднический характер и оформляется как услуги на возмездной основе, за исключением государственных и иных информационных систем, пользование которыми является безвозмездным в соответствии с законодательством. Причем агент информационной инфраструктуры может совмещать функции обладателя информации.

Относительно положений ст. 1253.1 ГК РФ об информационном посреднике следует отметить, что данная статья посвящена нарушению интеллектуальных прав информационным посредником, в то время как в ч. 2 ст. 1 Закона об информации специально оговорено, что эти отношения не входят в предмет регулирования данного закона. Закон об информации направлен преимущественно на защиту прав правообладателей (авторов) в информационном пространстве, а ГК

РФ имеет в виду разграничение ответственности информационного посредника и пользователей информации за нарушение авторских и смежных прав.

Вместе с тем в целях устранения возможных коллизий в ст. 1253.1 ГК РФ необходимо формулировку «информационный посредник» заменить на «агент информационной инфраструктуры (владелец, организатор, оператор и иной информационный посредник)».

Современный уровень проблем информатизации свидетельствует, что Закон об информации следует дополнить новыми субъектами: это эксперты и аудиторы в области информационной безопасности (например, новая статья 16.2).

На наш взгляд, эксперт в области информационной безопасности — это лицо, обладающее специальными знаниями и опытом работы в области информационной безопасности, осуществляющее инженерное проектирование, разработку, тестирование, внедрение и сопровождение информационного продукта на всех стадиях его жизненного цикла. Экспертами могут стать инженеры, программисты, сетевые администраторы, тестовые аналитики и др. Их задача в том, чтобы качественно прогнозировать реализацию и функциональные возможности программно-технических средств и информационных технологий, вводимых на рынок, проводить достоверные измерения параметров, правильно использовать современные методы контроля, своевременно обновлять продукт, достигнуть целевого уровня доверия пользователя к продукту (безопасности). Соответствующие обязанности эксперта могут быть внесены в Закон об информации после дополнительной научной аргументации.

Аудитор в области информационной безопасности — это независимое лицо, самостоятельно проводящее исследование и оценку объекта информатизации на предмет соответствия установленным требованиям к защите информации. Аудитор проверяет фактический уровень доверия пользователя к информации, проводит дополнительное тестирование продукта, измеряет уровень эффективности инструментов контроля и управления продуктом, обеспечивает возможность проверки процедур аудита, объективно сопоставляет полученные результаты и подготавливает аудиторский отчет. Соответствующие обязанности аудитора могут быть также внесены в Закон об информации, а внесение указанных изменений — сопровождаться дополнительной научной экспертизой.

В систему субъектов обеспечения информационной безопасности включены федеральные государственные органы нормотворчества, контроля и надзора в информационной сфере: Правительство Российской Федерации, Минцифры России, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор). Помимо этих органов можно назвать Федеральную службу безопасности Российской Федерации (далее — ФСБ России), Федеральную службу по техническому и экспортному контролю (далее — ФСТЭК России), Центральный Банк Российской Федерации (далее — Банк России) и др. В целом контроль и надзор осуществляются за деятельностью агентов информационной инфраструктуры.

Главное функциональное назначение агентов информационной инфраструктуры — обеспечить безопасное применение информационных технологий.

Информационные технологии и информационная безопасность

В 2019 году Минцифры России приняло дорожные карты развития 7 «сквозных» цифровых технологий будущего: квантовые технологии; новые производственные технологии (промышленный Интернет); технологии беспроводной связи; системы распределенного реестра (блокчейн); компоненты робототехники и сенсорика; нейротехнологии и искусственный интеллект; технологии виртуальной и дополненной реальности.

Наибольшие дискуссии по информационной безопасности в научной литературе вызывают технологии блокчейна, искусственного интеллекта, Интернета вещей, а также всех интересует судьба традиционной централизованной архитектуры доступа к информации «сервер — пользователь» в цифровом обществе.

Согласно Руководящему документу «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий». Часть 1, введенному в действие приказом Гостехкомиссии России от 19.06.2002, безопасность информационной технологии понимается как ее способность решать предписанные задачи по защите информационных ресурсов от угроз при «нулевом» или минимально приемлемом ущербе для пользователей. Критерии оценки безопасности каждой информационной технологии могут не совпадать и сравниваться, так как отличаются задачи и принципы действия этих технологий.

В юридической науке последних лет одной из перспективных безопасных информационных (цифровых) технологий считается блокчейн. В данном случае децентрализованная сеть компьютеров совместно обрабатывает данные в цепочки (блоки) на основе протоколов консенсуса пользователей данной сети. При этом в заголовок нового блока записывается хэш-ключ (шифр) предыдущего блока и хэш-код транзакций текущего блока, а полная актуальная версия базы всех проведенных операций копируется и хранится у каждого пользователя сети на личном компьютере (распределенный реестр), что гарантирует неизменность, неотменяемость принятых решений.

Структура и механизм работы технологии блокчейна делают ее уникальной и предпочтительной для множества социально-экономических проектов. Блокчейн-технология может применяться для ведения различных публичных реестров сделок, прав на имущество, а также для учета цифровых транзакций с объектами авторского и смежного права. Отмечено, что блокчейн имеет высокий потенциал применения в области государственного налогового контроля, поскольку в условиях формирования логистических цепочек прослеживаемости товаров упрощается налоговая отчетность и возможно налаживание автоматического налогообложения совершенных сделок (Lyutova & Fialkovskaya, 2021:707).

Несмотря на очевидные преимущества технологии блокчейна, китайские эксперты выделяют некоторые проблемы безопасности, с которыми столкнулось применение этой технологии: сложность анализа данных по зашифрованным данным блокчейна, плохая масштабируемость, уязвимости программного обеспечения и нехватка соответствующих механизмов стимулирования. Например, пропускная способность канала связи (масштабируемость) зависит от количества транзакций в секунду и предопределяется политикой доступа к сети.

В публичных блокчейнах поддерживается общедоступность и затрачивается больше времени на обработку данных и получение консенсуса. В частных, основанных на ограничении доступа, транзакции и консенсус формируются значительно быстрее; средний вариант функционирования наблюдается в гибридных блокчейнах (Zheng, et al., 2021:6—9).

Для обнаружения неправильного поведения блокчейна и повышения его устойчивости необходим интеллектуальный анализ данных, что логически приводит к задаче сочетания блокчейна и искусственного интеллекта. В то же время блокчейн призван исправить проблемы традиционного системного администрирования, а централизованное управление сетями и приложениями может использовать блокчейн как дополнительный инструмент организации данных.

Например, в случае реализации модели электронного правительства большие данные могут храниться в блокчейне, исходя из недостатков традиционной централизованной архитектуры, основные претензии к которой сводятся к риску утечки конфиденциальности данных при общем пользовании и единой точке отказа серверного оборудования. Использование блокчейна здесь имеет корректирующий характер. Во-первых, повысить уровень аутентификации личности. Во-вторых, определить законного владельца данных при подключении и регулярно отслеживать доступ к данным (Chen, J. et al., 2021:666). В случае же системных сбоев или сетевых атак в одном из технических решений собранные данные о поведении сети сначала целенаправленно записываются в блокчейн, а затем передаются для анализа и оценки администратору сети (Xie, et al., 2021:512).

Искусственный интеллект также относится в научной литературе к числу наиболее упоминаемых решений для обеспечения жизнедеятельности людей. Технология искусственного интеллекта направлена на автоматизацию рутинной или опасной деятельности человека, консультационную поддержку принятия решений и помощь в коммуникации людей, в том числе с участием других систем искусственного интеллекта. Однако при использовании методов машинного и глубокого обучения необходимо безопасное функционирование искусственной интеллектуальной системы. Например, одна из частных проблем — это поиск оптимальной зависимости между размером статистической обучающей выборки и затратами времени на обучение (Chen, et al., 2021:734—736).

Искусственный интеллект позволяет осуществлять мониторинг безопасности сетевого трафика, классифицируя его в виде модели с заданной структурой и функциями элементов по степени их важности (He, et al., 2021:305—310). Кроме того, искусственный интеллект может сокращать сетевой трафик и за счет стабилизации производительности сети поддерживать на должном уровне безопасность передаваемых по сети данных (Cao, et al., 2021:573).

Пожалуй, самый сложный вопрос этой темы — возможность искусственного интеллекта принимать моральные решения и нести за них моральную ответственность наравне с человеком. Теоретически решить эту проблему возможно, обучив искусственный интеллект человеческим ценностям в рамках концепции безопасного его воспитания как «ребенка». В этом случае ценности придется проектировать и обрабатывать как эталонные входные данные, но будут ли они очищены от предвзятости и стереотипов мышления самого разработчика,

уверенно сказать вряд ли возможно. Не решив этот вопрос, мы приходим к тому, что взаимодействие искусственного агента с окружающей средой (искусственная социализация) будет едва ли решающим показателем гуманизма обучения. Поскольку данное обучение основано на примитивных механизмах вознаграждения либо оценки функции полезности, то это является допустимым для информационной безопасности одних лиц и сомнительным для информационной безопасности относительного большинства людей (Bieger, et al., 2015:49).

Искусственный интеллект оказывает серьезное влияние на информационную безопасность личности через призму понятия основных прав человека. Здесь конкурируют между собой два подхода: метафизический и технологический. Метафизический подход рассматривает права человека как этическую основу, очерчивающую границу между человеком и машиной, а технологический — «встраивает» права человека в искусственный интеллект как руководящие инженерные принципы проектирования и автоматического управления человеческой деятельностью (Koniakou, 2021:173—175). Если для отечественной культуры более характерен этический подход, то зарубежные авторы полагают, что права человека могут быть объектом дизайна, чем проблематизируют вопрос гуманизма и информационной безопасности человека.

В этой связи нет ясности в понимании роли искусственного интеллекта в правосудии. Например, в китайской юрисдикции искусственный интеллект давно заменяет судью по некоторым категориям дел, и такое состояние считается неизбежным проявлением цифровизации, к которому нужно привыкать (Rusakova, 2021:622). Все-таки более безопасным представляется другой подход, согласно которому автономия искусственного интеллекта ограничена, и он может оказывать судье лишь информационную помощь и содействие, так как нельзя полностью признать эквивалентными «холодный расчет» машины и чувственно-эмоциональную сферу человека (Dobryakov, et al., 2021:478).

В последние годы широко развиваются технологии беспроводного доступа к информации, среди которых популярность приобретает Интернет вещей, в том числе спутниковый. Данная технология включает различные приложения и интеллектуальные датчики, которые смогли объединить множество виртуальных и физических объектов в «умную» систему для принятия решений без вмешательства человека по принципу «машина — машина» (M2M) (Poongodi, et al., 2021:1). Однако слабое место Интернета вещей в той же централизованной серверной модели управления, которая не имеет общепринятых способов аутентификации и защиты конфиденциальности доступа к нему. Поэтому данные проблемы могут решаться за счет улучшения безопасности Интернета вещей на основе блокчейна. Одновременно оптимизируется методика агрегации данных блокчейна и проверки их непротиворечивости и синхронности, повышается производительность и безопасность самого блокчейна (Sharma, et al., 2022:187—189).

Приложения искусственного интеллекта расширяют возможности Интернета вещей путем перераспределения и сбалансированности нагрузки на сеть между серверами, выгрузки данных на внешние серверы, например, на мобильные устройства и т.д. Перспективы развития безопасности Интернета вещей связываются с несколькими решениями. Одно из них — это обеспечение безопасной

передачи сигнала Интернета вещей с учетом смыслового контекста данных (Ruan, et al., 2021:414—419). Другое — повышение точности распознавания устройств Интернета вещей в сети благодаря расширению словаря ключевых поисковых слов, сопоставляющих информацию об устройствах и выполняемых ими функциях до требуемой степени корреляции (Xu, et al., 2021:287).

Следует отметить, что развитие альтернативных цифровых технологий приводит не к смене, а только к интеграции с традиционной централизованной архитектурой «сервер — клиент», которая для нашей страны является актуальной в свете территориального масштаба и многоуровневой структуры публичного управления.

Например, в целях усиления централизации контроля за информационной безопасностью в системах ГАС «Выборы», ГАС «Правосудие», Единой информационной системе государственных закупок и др. государственных информационных системах могут использоваться отдельные элементы технологии блокчейн, но не вся технология целиком. Очевидно, что публичные интересы обусловливают невозможность предоставления копии реестра всех операций каждому участнику информационной системы. В связи с этим, в частности, блокчейн может записывать в базу данных факты дистанционного электронного волеизъявления избирателей, а механизмы подсчета голосов и определения результатов голосования реализуются на защищенных централизованных серверах либо в защищенных облачных хранилищах.

Правовые режимы информационной безопасности

Закрепление в конституционных поправках 2020 года положения об обязанности Российской Федерации принимать меры по обеспечению информационной безопасности личности, общества и государства дает основание выдвинуть идею о выделении в рамках ее теоретической модели конституционного и отраслевых режимов.

Конституционный режим информационной безопасности — это совокупность основополагающих установок, общеправовых принципов и конкретных конституционных предписаний, регулирующих общественные отношения в сфере безопасного применения информационных технологий и цифровых данных, а также закрепляющих процедурные механизмы их реализации и обеспечения, устанавливающих на основании этих правил наиболее общий порядок безопасного оборота информации в Российской Федерации.

По своему юридическому содержанию конституционный режим информационной безопасности направлен на гармонизацию конституционных прав и свобод личности в информационной сфере и публичных интересов, ограничивающих эти права и свободы. Главным критерием соразмерности такого ограничения является положение ч. 3 ст. 55 Конституции РФ об ограничении основных прав человека федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обороны и безопасности государства. Задача юридической науки и практики — находить и закреплять в теоретических моделях и проектах изменений правовых

норм максимально адекватные варианты баланса публичных и частных интересов по вопросам информационной безопасности общества.

В целом к базовым информационным правам и свободам человека отнесены неприкосновенность частной жизни (ст. 24); свобода мысли и слова, поиска информации (ст. 29); право на достоверную информацию о состоянии окружающей природной среды (ст. 42). Информационные интересы граждан затрагиваются также при реализации права на участие в управлении делами государства (ст. 32); права на труд (ст. 37) и обеспечении равенства граждан перед законом (ст. 19).

Например, при высказываниях в социальных сетях мы каждый раз осуществляем акт депривации и должны осознавать, что наша частная жизнь в информационном обществе находится в общем доступе, что налагает особые публичные ограничения и требования к свободе слова в соответствии с профессиональным, должностным, этническим положением лица. Соответственно, проактивный поиск или фильтрация контента администрацией социальной сети не может рассматриваться как цензура, так как направлена на предупреждение правонарушений, а также на защиту правомерной информации от преждевременного удаления, блокировки, отрицательной маркировки (Krönke, 2020:160—162).

В числе отраслевых режимов информационной безопасности следует выделить, прежде всего, административно-правовой, уголовно-правовой и гражданско-правовой.

Административно-правовой режим информационной безопасности — это осуществление, как правило, в порядке подзаконного нормотворчества политики управления информационной безопасностью, в рамках которой последовательно определяются угрозы информационной безопасности, устанавливаются требования к защите информации, принимаются конкретные организационные и технические меры для выполнения этих требований, вводится административная ответственность за нарушение законодательства в области защиты информации.

При реализации основных прав и свобод с применением информационных технологий идентификация личности проводится по ее персональным данным. Согласно ст. 5 Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 (далее — Закон о персональных данных) оператор информационной системы персональных данных обязан обеспечить сохранность и целевой характер обработки персональных данных при условии получения письменного согласия лица на обработку его персональных данных, за исключением предусмотренных законом случаев принудительной их обработки.

В этой связи ученые правильно обращают внимание, что в настоящее время отсутствует эффективный механизм борьбы с коммерческим оборотом персональных данных граждан без их согласия (Gaivoronskaya, et al., 2021:656). Имеется в виду, что отсутствуют правовые гарантии того, что согласно ст. 5 Закона о персональных данных по достижении целей обработки они будут уничтожаться и обезличиваться. В то же время следует возразить тем авторам, которые полагают необходимым сделать big data (большие персональные данные) россиян собственностью государства (Ionova, 2021:44).

Механизм контролируемой коммерциализации возможен и в действующей редакции Закона о персональных данных (ст. 6), когда субъект является

выгодоприобретателем по договору и может получать определенную плату за использование своих персональных данных. Однако именно для воспрепятствования незаконной торговле данными следует уточнить диспозицию ч. 2 ст. 13.11 КоАП РФ, дополнив после слов «обработка персональных данных» формулировкой «в том числе возмездная их передача…».

Реализация административно-правового режима информационной безопасности требует определенной терминологической унификации Закона об информации и Закона о персональных данных на том основании, что персональные данные — это особая разновидность сведений о личности, отвечающих всем признакам информации.

Например, в ст. 19 Закона о персональных данных дается определение угроз безопасности персональных данных и уровня защищенности персональных данных, в то время как в ст. 16 Закона об информации определений угроз информационной безопасности и уровня защищенности информации не дается. В приказах ФСБ России и ФСТЭК России используется термин «класс защищенности».

В постановлении Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01.11.2012 уровень защищенности персональных данных определяется в зависимости от типа угроз, категории персональных данных и количества субъектов. В то же время приказом ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» № 17 от 11.02.2013 класс защищенности информационной системы зависит от уровня значимости информации и масштаба информационной системы (федеральный, региональный, объектовый).

При подключении к информационно-телекоммуникационным сетям ключевую роль играет аутентификация пользователя, которая в современных условиях осуществляется тремя способами: 1) пароль (постоянный или разовый); 2) устройство для аутентификации (например, мобильный телефон); 3) биометрия (Stefanova, 2020:250).

Идентификация личности с помощью биометрических персональных данных является перспективным способом обеспечения информационной безопасности, но влечет определенные риски, связанные с перехватом или случайным подбором ключа или пароля биометрического образа человека (тайного или электронного), взломом материального носителя, содержащего цифровой код биометрии. Основное регулирование использования биометрических персональных данных человека содержится в ст. 14.1 Закона об информации. Представляется, что логично было урегулировать этот вопрос в специальном Законе о персональных данных, который сегодня содержит лишь небольшую ст. 11, формально не имеющую никакой связи со ст. 14.1 Закона об информации.

При этом ст. 14.1 Закона об информации отсылает к перечню актуальных угроз безопасности биометрических персональных данных, к которым подзаконные нормативные акты относят лишь конфиденциальность, целостность, доступность и достоверность данных без учета более широких защитных требований ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации.

Требования к средствам высоконадежной биометрической аутентификации». Учитывая рост интереса к биометрической аутентификации человека в условиях нарастающей цифровизации, необходимо перевести эту проблему с уровня нормативно-технической документации в правовую плоскость, законодательно закрепить повышенные требования к защите биометрических персональных данных.

Уголовно-правовой режим информационной безопасности — это система уголовно-правовых запретов, устанавливающих круг преступлений, посягающих на информационную безопасность личности, общества и государства, а также меры уголовного наказания за их совершение. Специально преступления в сфере компьютерной информации закреплены главой 28 Особенной части УК РФ (ст. ст. 272—274.1).

Законодательное регулирование составов преступлений в сфере компьютерной информации подвергается значительной критике в специальной литературе (Petrova & Lobachev, 2020:54—58). Отметим ряд моментов, которые, на наш взгляд, следует скорректировать в целях оптимизации средств уголовно-правовой охраны в информационной сфере.

Во-первых, в диспозициях первых частей ст. ст. 272—274 УК РФ необходимо расширить перечень общественно опасных последствий преступлений, так как они не сводятся только к «уничтожению, блокированию, модификации либо копированию компьютерной информации», а должны быть дополнены формулировками «предоставление», «распространение», «иные неправомерные действия в отношении этой информации», что соответствует Закону об информации.

Во-вторых, необходимо исключить из диспозиций ч. 1 ст. 274 и ч. 3 ст. 274.1 УК РФ формулировку «нарушение правил доступа к информации, информационным системам, информационно-телекоммуникационным сетям», так как она охватывается составом нарушения правил эксплуатации средств хранения, обработки или передачи информации. На практике без нарушения правил доступа посторонними лицами какого-либо реального ущерба для эксплуатации информационных ресурсов не приносится.

В-третьих, абсолютно правильным является выделение в отдельную ст. 274.1 УК РФ преступных посягательств на объекты критической информационной инфраструктуры Российской Федерации. В соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ от 26.07.2017 к их числу относятся военные объекты, объекты топливно-энергетического комплекса, добывающей промышленности, здравоохранения и науки. Для уголовно-правовой квалификации посягательств на эти объекты достаточно причинения любого вреда.

Одновременно существует доктринальная и практическая потребность снизить размер крупного ущерба для иных преступлений, содержащихся в главе 28 УК РФ, который сейчас определяется как сумма более 1 млн руб. Данный стоимостный критерий исключает из круга уголовно наказуемых деяний действительно общественно опасные деяния с меньшей оценочной стоимостью. Тем более, например, ст. 159.6 УК РФ предусматривает ответственность за мошенничество в сфере компьютерной информации, где она выступает не как объект

посягательства, а как средство совершения имущественных преступлений. В главе 21, где расположена ст. 159.6 УК РФ, крупным размером считается сумма более 250 тыс. руб., что нуждается в согласовании.

Гражданско-правовой режим информационной безопасности представляет собой совокупность правил создания, распространения и использования информации в имущественном обороте на согласованных сторонами условиях договора либо в соответствии с императивными нормами гражданского законодательства, например, в режиме коммерческой тайны (ст. 1465 ГК РФ).

С точки зрения ст. 128 ГК РФ информация — это особый непоименованный объект гражданского права, который может быть отнесен к «иному имуществу, в том числе имущественным правам…». Об этом можно судить по конструкции ст. 141.1 ГК РФ, где информационные по своей форме выражения цифровые права обозначены как обязательственные и иные права, оборот которых воспроизводит с некоторыми особенностями порядок распоряжения имуществом.

В целях развития цифровой экономики и расширения рынка цифровых услуг в Российской Федерации приняты Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ от 31.07.2020 (далее — Закон о цифровых финансовых активах») и Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ от 02.08.2019 (далее — Закон об инвестиционных платформах).

Согласно ст. 9 Закона о цифровых финансовых активах оператор информационной системы по выпуску цифровых финансовых активов возмещает убытки пользователям информационной системы в результате утраты информации; сбоя информационных технологий и технических средств; предоставления недостоверной, неполной или вводящей в заблуждение информации; нарушения правил работы информационной системы; несоответствия информационной системы требованиям законодательства. Однако такая же ответственность оператора обмена цифровых финансовых активов ст. 10 Закона не предусмотрена, что следует признать существенным пробелом, требующим законодательного восполнения.

Кроме того, в соответствии со ст. 12 Закона об инвестиционных платформах ответственность оператора инвестиционной платформы за убытки пользователей ограничена лишь нарушениями правил работы инвестиционной платформы и оборотом недостоверной или неточной информации. В связи с этим необходимо привести ее в соответствие со ст. 9 Закона о цифровых финансовых активах, дополнив такими формулировками об основаниях гражданско-правовой ответственности оператора, как утрата информации и сбой в работе информационных ресурсов. Это позволит обеспечить единство правового регулирования безопасной цифровой финансовой информации, отвечающей общим требованиям Закона об информации.

Как отмечено в литературе, в эпоху стремительного развития цифровых технологий человек должен сохранять за собой право на жизнь в традиционной бесцифровой среде обитания. «Государство не должно превращаться в «цифровой концлагерь», общество — в «цифровую колонию», а человек — в «цифровую

личность» (Ovchinnikov, 2020:18). Тем не менее, по мере развития новых прорывных технологий потребность в модернизации информационной инфраструктуры и усилении информационной безопасности будет только возрастать (Bertovsky, 2021:745).

Заключение

В результате рассмотрения поставленной в статье проблемы мы пришли к выводу, что конституционное закрепление информационной безопасности является основой для модернизации ее теоретической модели.

Решение проблемы информационной безопасности затрагивает базовые основы гуманистической концепции права. Сегодня полный отказ от цифровых технологий уже невозможен в силу плотной их интеграции в пространство современных социальных отношений. Поэтому нужно установить такой режим безопасного оборота информации, при котором остаются неизменными сущностные основы природы человека, а он получает возможность развивать и совершенствовать свой потенциал в рамках цифровой среды.

References / Список литературы

Bertovsky, L.V. (2021) High-tech law: concept, genesis and prospects. *RUDN Journal of Law*. 25 (4), 735—749. (in Russian). https://doi.org/10.22363/2313-2337-2021-25-4-735-749
Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735—749. https://doi.org/10.22363/2313-2337-2021-25- 4-735-749

Bieger, J., Thórisson, K.R. & Wang, P. (2015*) Safe Baby AGI. In: Bieger, J., Goertzel, B., Potapov,* A. (eds.). *Artificial General Intelligence. AGI 2015. Lecture Notes in Computer Science*. Vol. 9205. Springer, Cham. pp. 46—49. https://doi.org/10.1007/978-3-319-21365-1_5

Cao N., Jiang, D., Liu Y., Zhou Y., Du, H., Qiao, X., Xia, Y. & Zhu, D. (2021) Revisit Raft Consistency Protocol on Private Blockchain System in High Network Latency. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). *Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science*. Vol. 1423. Springer, Cham. pp. 571—579. https://doi.org/10.1007/978-3-030-78618-2_47

Chen, J., Liu, X., Han, W. & Cheng, J. (2021) A Model Design of Blockchain-Based Data Storage for E-Government Application. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). *Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science*. Vol. 1423. Springer, Cham. pp. 666—676. https://doi.org/10.1007/978-3-030-78618-2_55

Chen, Z., Jia, X., Zhang, L. & Yin, G. (2021) Intelligent Security Image Classification on Small Sample Learning. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). *Artificial Intelligence and Security. ICAIS 2021. Lecture Notes in Computer Science*. Vol. 12736. Springer, Cham. pp. 726—737. https://doi.org/10.1007/978-3-030-78609-0_61

Dobryakov, D.A., Kasa, I. & Sukhostavskaya, Yu.V. (2021) Application of digital technologies in litigation and dispute resolution. *RUDN Journal of Law*. 25 (2), 461—481. https://doi.org/10.22363/2313-2337-2021-25-2-461-481 (in Russian).
Добряков Д.А., Каса И., Сухоставская Ю.В. Применение цифровых технологий в судопроизводстве и внесудебном урегулировании споров // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2021. Т. 25. № 2. С. 461—481. https://doi.org/10.22363/2313-2337-2021-25-2-461-481

Gaivoronskaya, Ya.V., Miroshnichenko, O.I. & Shakirov, S.Sh. (2021) Trends and lessons of anti-crisis legal regulationin in the period of the COVID-19 pandemic. *RUDN Journal of Law*. 25(2), 634—662. https://doi.org/10.22363/2313-2337-2021-25-2-634-662 (in Russian).
Гайворонская Я.В., Мирошниченко О.И., Шакиров С.Ш. Тенденции и уроки антикризисного правового регулирования в период пандемии COVID-19 // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2021. Т. 25. № 2. С. 634—662. https://doi.org/10.22363/2313-2337-2021-25-2-634-662

He, M., Jin, L. & Song, M. (2021) Interpretability Framework of Network Security Traffic Classification Based on Machine Learning. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). *Artificial Intelligence and Security. ICAIS 2021. Lecture Notes in Computer Science*. Vol. 12737. Springer, Cham. pp. 305—320. https://doi.org/10.1007/978-3-030-78612-0_25

Ionova, E.A. (2018) Information security of communications in the digital economy. *Communicology: electronic scientific journal*. 3 (4), 39—47. (in Russian).
Ионова Е.А. Информационная безопасность коммуникаций в условиях цифровой экономики // Коммуникология: электронный научный журнал. 2018. Т. 3. №. 4. С. 39—47.

Koniakou, V. (2021) Governing Artificial Intelligence and Algorithmic Decision Making: Human Rights and Beyond. In: Dennehy D., Griva A., Pouloudi N., Dwivedi Y.K., Pappas I., Mäntymäki M. (eds). *Responsible AI and Analytics for an Ethical and Inclusive Digitized Society. I3E 2021. Lecture Notes in Computer Science*. Vol. 12896. Springer, Cham. pp. 173—184. https://doi.org/10.1007/978-3-030-85447-8_16

Krönke, C. (2020) Artificial Intelligence and Social Media. In: Wischmeyer T., Rademacher T. (eds). *Regulating Artificial Intelligence*. Springer, Cham. pp. 145—173. https://doi.org/10.1007/978-3-030-32361-5_7

Lyutova, O.I. & Fialkovskaya, I.D. (2021) Blockchain technology in tax law theory and tax administration. *RUDN Journal of Law*. 25 (3), 693—710. https://doi.org/10.22363/2313-2337-2021-25-3-693-710

Ovchinnikov, A.I. (2020) Security of the individual and the state in the digital age: political and legal aspects. *Journal of Russian Law*. (6), 5—21. https://doi.org/10.12737/jrl.2020.064 (in Russian).
Овчинников А.И. Безопасность личности и государства в цифровую эпоху: политико-правовой аспект // Журнал российского права. 2020. № 6. С. 5—21. https://doi.org/10.12737/jrl.2020.064

Petrova, I.A. & Lobachev, I.A. (2020) Crimes in the field of computer (digital) information: controversial issues of definition of the concept, the object of criminal law protection and the subject of encroachments. *Journal of Applied Research*. (1), 52—62. (in Russian).
Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. С. 52—62.

Polyakova, T.A., Minbaleev, A.V. & Boychenko, I.S. (2018) Problems of legal provision of information security in the process of using digital technologies in the global digital environment. *Bulletin of the Academy of Law and Management*. 3 (52), 32—36. (in Russian).
Полякова Т.А., Минбалеев А.В., Бойченко И.С. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. № 3 (52). С. 32—36.

Poongodi, T., Gopal, R. & Saini, A. (2021) IoT Architecture, Communication Technologies, and Its Applications. In: Kumar R., Wang Y., Poongodi T., Imoize A.L. (eds). *Internet of Things, Artificial Intelligence and Blockchain Technology*. Springer, Cham. pp. 1—24. https://doi.org/10.1007/978-3-030-74150-1_1

Ruan, Z., Huang, L. & Luo, H. (2021) Securing Satellite Internet of Things by Perceiving Content Semantics. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). *Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science*. Vol. 1424. Springer, Cham. pp. 414—425. https://doi.org/10.1007/978-3-030-78621-2_34

Rusakova, E.P. (2021) Integration of “smart” technologies in the civil proceedings of the People’s Republic of China. *RUDN Journal of Law*. 25 (3), 622—633. https://doi.org/10.22363/2313-2337- 2021-25-3-622-633

Sharma, S., Parihar, A. & Gahlot, K. (2022) Blockchain-Based IoT Architecture. In: Raj P., Dubey A.K., Kumar A., Rathore P.S. (eds). *Blockchain, Artificial Intelligence, and the Internet of Things. EAI/Springer Innovations in Communication and Computing*. Springer, Cham. pp. 187—205. https://doi.org/10.1007/978-3-030-77637-4_10

Stefanova, N.A. (2020) Multifactor authentication as an information security tool in the digital economy. *Topical issues of modern economics*. (4), 246—252. https://doi.org/10.34755/IROK.2020.85.79.036 (in Russian).

Стефанова Н.А. Многофакторная аутентификация как инструмент информационной безопасности в цифровой экономике // Актуальные вопросы современной экономики. 2020. № 4. С. 246—252. https://doi.org/10.34755/IROK.2020.85.79.036

Vlasenko, N.A. (2018) The problem of sufficiency and aggressiveness of legal regulation. *Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 41 (1), 41—47. https://doi.org/10.24411/2078-5356-2018-00005 (in Russian).

Власенко Н.А. Проблема достаточности и агрессивности правового регулирования // Юридическая наука и практика: Вестник Нижегородской Академии МВД России. 2018. № 1 (41). С. 41—47. https://doi.org/10.24411/2078-5356-2018-00005

Xie, L., Hang, F., Lv, Y. & Guo, W. (2021) Research on Data Security Protection System of Monitoring and Acquisition System Based on Block Chain Technology. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). Advances in Artificial Intelligence and Security. ICAIS 2021. *Communications in Computer and Information Science*. Vol. 1424. Springer, Cham. pp. 502—513. https://doi.org/10.1007/978-3-030-78621-2_42

Xu, Z-X., Chen, X-B., Xu, G., Yuan, K-G., Cui, J. & Yang, Y-X. (2021) Research on Feature Words for IoT Device Recognition Based on Word2vec. In: Sun X., Zhang X., Xia Z., Bertino E. (eds). Advances in Artificial Intelligence and Security. ICAIS 2021. *Communications in Computer and Information Science.* Vol. 1423. Springer, Cham. pp. 287—298. https://doi.org/10.1007/978-3-030-78618-2_23

Zharova, A.K. (2020) Issues of ensuring the security of a person's digital profile. *Lawyer*. (3), 55—61. https://doi.org/10.18572/1812-3929-2020-3-55-61 (in Russian).

Жарова А.К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55—61. https://doi.org/10.18572/1812-3929-2020-3-55-61

Zheng, Z., Dai, H-N. & Wu, J. (2021) Overview of Blockchain Intelligence. In: Zheng Z., Dai H-N., Wu J. (eds). *Blockchain Intelligence*. Springer, Singapore. pp. 1—14. https://doi.org/10.1007/978-981-16-0127-9_1

Сведения об авторе:

Гаврилова Юлия Александровна — кандидат юридических наук, доцент, доцент кафедры философии и теории права, Институт права, Волгоградский государственный университет; Российская Федерация, 400062, г. Волгоград, Университетский пр-т, д. 100

ORCID ID: 0000-0002-8055-4710

e-mail: gavrilova_ua@volsu.ru

About the author:

Yulia A. Gavrilova — Candidate of Legal Sciences, Associate Professor of the Department of Philosophy and Theory of Law, Law Institute, Volgograd State University; 100, Universitetsky ave., Volgograd, 400062, Russian Federation

ORCID ID: 0000-0002-8055-4710

e-mail: gavrilova_ua@volsu.ru