Научная статья
УДК 343.237
DOI: 10.14529/law230102

ТЕНДЕНЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИИ

Ю. А. Воронин, *voroninya@yandex.ru*
А. А. Дмитриева, *dmitrievaaa@susu.ru*
Южно-Уральский государственный университет, г. Челябинск, Россия

Аннотация. Статья посвящена основным тенденциям правовой политики в сфере обеспечения информационной безопасности Российского государства, отразившимся в значительном числе правовых актов, сформулировавших цели, задачи и содержание мер по реагированию на кибератаки и по ликвидации последствий посягательств на объекты критической информационной инфраструктуры. В статье подчеркивается, что, несмотря на предпринимаемые меры, эта проблема остается чрезвычайно актуальной, а ее решение предполагает дальнейшее совершенствование каждого структурного элемента упомянутого комплекса, в том числе его законодательной базы. Ведь улучшение нормативно-правовой базы, в свою очередь, в немалой степени определяет качество и надежность как информационно-коммуникационных технологий, так и самой среды их функционирования. При этом для успешного решения назревших задач несомненное значение имеют также международные контакты, налаживание более тесного сотрудничества государств в этой сфере, включая совместную разработку глобальных информационно-цифровых стандартов и унификацию уголовного законодательства стран мирового сообщества в части установления ответственности за информационно-цифровые деликты.

Ключевые слова: объекты критически важной информационной инфраструктуры, нормативно-правовые акты в сфере обеспечения информационной безопасности, информационно-коммуникационные технологии, межгосударственное сотрудничество.

Для цитирования: Воронин Ю. А., Дмитриева А. А. Тенденции правового регулирования в сфере обеспечения безопасности критически важной информационной инфраструктуры России // Вестник ЮУрГУ. Серия «Право». 2023. Т. 23, № 1. С. 16–23. DOI: 10.14529/law230102.

Original article
DOI: 10.14529/law230102

TRENDS IN LEGAL REGULATION IN THE FIELD OF SECURITY OF THE CRITICALLY IMPORTANT INFORMATION IN FRASTRUCTURE OF RUSSIA

Yu. A. Voronin, *voroninya@yandex.ru*
A. A. Dmitrieva, *dmitrievaaa@susu.ru*
South Urals State University, Chelyabinsk, Russia

Abstract. The article is devoted to the main trends of legal policy in the field of information security of the Russian state, reflected in a significant number of legal acts that formulated goals, objectives and content of measures to respond cyber attacks and to eliminate the consequences of encroachments on the objects of the critical information infrastructure complex. The article emphasizes that despite taken measures, this problem remains extremely urgent, and its solution involves further improvement and increasing the effectiveness of the mentioned complex, including its legislative framework. After all, the improvement of the regulatory framework largely ensures the quality and reliability of both information and communication technologies and the very environment of their functioning. At the same time, international contacts and the establishment of closer cooperation between states in this area are also of undoubted importance for the successful solution of urgent tasks. This includes joint development of global digital informational standards and the unification of criminal legislation of countries of the world community in terms of establishing responsibility for digital crimes, taking into account factors of a transnational nature.

Keywords: objects of critically important information infrastructure, regulations in the field of information security, information and communication technologies, interstate cooperation.

For citation*:* Voronin Yu. A., Dmitrieva A. A. Trends in legal regulation in the field of security of the critically important information infrastructure of Russia. Bulletin of the South Ural State University. Series "Law". 2023. vol. 23. no. 1, pp. 16–23. (in Russ.) DOI: 10.14529/law230102.

Мировое развитие информационно-цифровой среды, являясь объективно неизбежным процессом, приносит не только позитивные результаты, но вместе с тем порождает негативные социальные и правовые последствия для большинства стран мирового сообщества, включая нарушение их суверенитета. В равной мере это касается и Российской Федерации, систематически подвергающейся посягательствам извне на безопасность ее критически важной информационной инфраструктуры. Речь идет об атаках на совокупность российских автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий (Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»). Несомненно, это требует опережающего принятия мер, нейтрализующих или предотвращающих криминальные проявления в данной сфере и в этой связи усиления государственного контроля над состоянием информационно-цифрового пространства [2, с. 74–80].

Актуальность решения данной задачи трудно переоценить. Ведь по приблизительной оценке российских специалистов в области мониторинга предупреждения и блокирования атак подобного рода их среднегодовая численность превышает 100 миллионов интернет-адресов, и каждый год число таких посягательств увеличивается в среднем на 40 % [8, с. 65]. Причем особую интенсивность кибератаки извне, направленные на национальную безопасность нашей страны, приобрели в последние годы. В частности, по данным экспертов по вопросам кибербезопасности абсолютное большинство (около 92 %) кибератак, совершенных высокопрофессиональными хакерами в начале 20-х гг. нынешнего столетия, было направлено именно на объекты критической информационной инфраструктуры. Чаще всего внимание преступников с высокой квалификацией – кибернаемников и членов определенных зарубежных проправительственных группировок – привлекали российские государственные организации, предприятия энергетики, промышленности и Военно-промышленного комплекса [5]. В этой ситуации одновременно с мерами по обеспечению кибербезопасности как элемента защиты суверенитета нашей страны назрела необходимость совершенствования не только средств телекоммуникаций с целью повышения эффективности функционирования объектов критической инфраструктуры (военной, промышленной, информационной), но логически естественной является также потребность в продолжении интенсивного развития соответствующей нормативно-правовой базы.

2. Исторически, по устоявшемуся мнению специалистов, анализирующих эту проблему, развитие правовой базы противодействия информационно-цифровой преступности в нашей стране берет свое начало с принятием УК РФ, содержащего, среди прочих уголовно-правовых норм, соответствующие составы компьютерных преступлений. С течением времени упомянутые составы не раз подвергались качественной переработке как структурно, так и содержательно. В частности, одной из последних, уже современных новелл, предусматривающих уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру, явилась ст. 274.1 УК РФ, вступившая в силу спустя два с лишним десятилетия – с 1 января 2018 г. после включения в УК РФ первых компьютерных составов преступлений. Прослеживая общую динамику развития нормотворчества в этой сфере, принципиально важно также отметить, что в ст. 2 Федерального

закона от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» было сформулировано очень содержательное законодательное определение понятия информационной безопасности. В упомянутой статье информационная безопасность определялась как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства посредством применения мер, направленных на уменьшение, предотвращение или поддержание на приемлемом уровне негативных последствий от неправомерного воздействия на объекты информационной сферы. Позже, после прекращения действия упомянутого законодательного акта, определение информационной безопасности стало трактоваться в несколько иной (более лаконичной) редакции, а именно: как состояние защищенности национальных интересов России, определяющихся совокупностью сбалансированных интересов личности, общества, государства [6, с. 20].

В дальнейшем, в русле реализации стоящей перед российским государством задач в области обороны, охраны систем связи, атомных электростанций и других стратегических объектов от внешнего воздействия правовая база защиты национальной информационной сети, обеспечения ее нормального функционирования год от года неуклонно расширялась [1, с. 78–84]. Одновременно чрезвычайно актуальной становилась необходимость создания и нормативно-правового оформления статуса суверенного российского сегмента Интернета в виде собственной информационной сети («суверенного рунета»). Вполне логично, что необходимость такого шага затем нашла обоснование в Доктрине информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646. В этом документе было справедливо отмечено, что современные возможности трансграничного оборота информации, и прежде всего сети Интернет, все чаще используются для достижения террористических, экстремистских, криминальных и иных противоправных целей, увеличивают масштабы и скоординированность компьютерных атак на объекты критической информационной инфраструктуры, способствуют нарастанию угроз суверенитету, территориальной целостности, политической и социальной стабильности российского государства.

3. Сегодня, на наш взгляд, есть основания утверждать, что генеральной тенденцией в становлении правовой базы, нацеленной на противодействие преступности в сфере информационно-телекоммуникационных технологий, является продолжающееся формирование обширного и разнообразного комплекса правовых норм, так или иначе касающихся основных принципов и задач этого сегмента законотворчества, сопровождающееся реальным повышением эффективности информационной безопасности, охраны объектов критической информационной инфраструктуры страны. Названный комплекс представлен, во-первых, федеральным законодательством концептуального характера, закрепляющим основные принципы, правовые институты и нормы, а также цели и задачи государственной политики в отношении широкого спектра проблем безопасности соответствующих объектов; во-вторых, отраслевыми правовыми актами, регулирующими более специфические вопросы в информационно-цифровой сфере, касающиеся отдельных объектов или их групп в критической информационной инфраструктуре страны; в-третьих, международными нормативно-правовыми документами, посвященными данной проблеме, в подписании и ратификации которых Российская Федерация принимала участие или их инициировала, но по тем или иным причинам они не дошли до стадии принятия.

На наш взгляд, применительно к первому элементу упомянутого комплекса документов, речь идет в первую очередь о положениях целого ряда таких концептуальных правовых актов, как Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»; Указ Президента РФ от 3 февраля 2012 г. № 803 «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»; Указ Президента РФ от 24 июля 2013 г. № Пр-1753 «Основы государственной политики Российской Феде-

рации в области международной информационной безопасности на период до 2020 года»; Указ Президента РФ от 5 декабря 2016 г. № 646 «Доктрина информационной безопасности Российской Федерации»; Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; Указ Президента РФ от 9 мая 2017 г. № 203 «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»; Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», а также некоторые другие, помимо названных, нормативно-правовые документы.

Что же касается нормативных актов второй группы, то, по сути, параллельно, но будучи естественным ответвлением от концептуального содержания упомянутой первой категории правовых актов, они отражают вполне закономерную тенденцию «рассредоточения» правового регулирования уже применительно к специфике отдельных конкретных сфер (объектов, отраслей) критической информационной инфраструктуры. Об этом свидетельствует все увеличивающийся перечень законодательных актов, принимаемых в минувшие два с лишним десятилетия и последовательно отражающих специфику этих конкретных сфер. Перечень нормативных актов второй группы достаточно широк. К их числу, в частности, относятся: Федеральный закон от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»; Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»; Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»; Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а также целый ряд других нормативно-правовых актов.

Следует подчеркнуть, что сегодня – именно в контексте двух рассмотренных выше тенденций – нормотворческие усилия в данной сфере концентрируются прежде всего на разработке и последующем принятии норм, основной особенностью содержания которых является акцентирование внимания на приоритетной правовой поддержке развития и защиты (ст. 274.2 УК РФ) информационно-коммуникационных технологий, включая отечественную сеть Интернета. При этом, как справедливо отмечается российскими исследователями анализируемой проблемы, жизненно необходимым был и остается именно комплексный и одновременно конкретный подход к ее решению, сочетающий развитие как самой нормативной базы, так и реальное внедрение лучших образцов управления информационной безопасностью, а также – что особенно актуально в нынешней экономической и политической ситуации – создание и применение собственного оборудования и средств защиты от криминальных хакерских атак. При этом российские специалисты подчеркивают необходимость не только более интенсивного электронного взаимодействия органов власти и управления, но и соблюдения технологической независимости и информационной безопасности названных субъектов, а также обеспечения информационной безопасности автоматизированных систем управления и, наконец, достижения качественного прорыва, в сфере научных исследований упомянутого профиля. Только в этом случае возможен выход на качественно новый уровень создания единой системы кибербезопасности как составной части информационной и национальной безопасности российского государства [1, с. 83].

В этой связи вполне логичным является то, что не ограничиваясь уже упомянутыми ранее основополагающими и отраслевыми нормативными актами и в целях дальнейшего развития их положений, а также в связи со складывающейся международной и внутриполитической ситуацией, Президент РФ В. В. Путин 1 мая 2022 г. издал Указ «О дополнительных мерах по обеспечению информационной безопасности России». Названным документом на федеральные и региональные органы исполнительной власти, управленче-

ские и ведомственные подразделения были возложены дополнительные обязанности по обнаружению, предупреждению и безотлагательной ликвидации кибератак и иных компьютерных инцидентов. И прежде всего в нем подчеркивается роль правоохранительных органов в решении упомянутых задач. В частности, это касается осуществления прокуратурой конкретных, упомянутых в Указе, мер в сфере надзора за соблюдением законов об обеспечении безопасности объектов критической информационной структуры. Далее обращается внимание на особую роль Федеральной службы безопасности и МВД РФ в деле профилактирования, оперативного противодействия и раскрытия информационно-цифровых преступлений. Именно подразделениям этих служб отводится основная роль и предоставляется необходимый объем полномочий по координации оперативных разработок и расследованию особенно сложных преступлений, связанных с киберпосягательствами на стратегические объекты критической информационной инфраструктуры России.

Но, помимо силовых ведомств, Указ коснулся также государственных компаний и иных юридических лиц, по своим характеристикам относящихся к субъектам критической информационной инфраструктуры. В частности, в этих органах, ведомствах, учреждениях и предприятиях, а также в их системообразующих подразделениях постановлено создать отделы по IT-безопасности или возложить эти функции на уже существующие отделы. Следует напомнить, что наряду с упомянутыми нововведениями, но несколько раньше (в конце марта 2022 года), в качестве профилактической меры госструктурам уже было запрещено без соответствующего согласования закупать зарубежное программное обеспечение для использования его на объектах критической инфраструктуры. В дальнейшем, начиная с января 2025 года, вообще будет наложено вето на использование иностранного программного обеспечения на всех объектах критической информационной структуры. Предполагается, что эти меры потенциально способны повысить уровень защиты информационной безопасности и суверенитета российского государства.

Необходимо отметить, однако, что такая позиция не исключает и не противоречит развитию сложившейся за многие годы тенденции участия Российской Федерации совместно с другими странами мирового сообщества в международной нормотворческой деятельности по вопросам информационной безопасности и сотрудничества в сфере противодействия информационно-цифровым деликтам. Речь идет, прежде всего, об участии Российской Федерации в реализации принципов и норм, содержащихся в подписанных и ратифицированных ею международных соглашениях или во внутрироссийских нормативно-правовых актах, касающихся данной злободневной проблемы. Пожалуй, к одному из первых актов внутреннего нормативного регулирования в рамках анализируемой тенденции, на наш взгляд, можно отнести уже упоминавшийся ранее Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене». В дальнейшем эта тенденция получила развитие и совершенно естественно вписалась в содержание и цели принятых в 2001 году Генеральной ассамблеей ООН двух резолюций «О борьбе с преступным использованием информационных технологий» (№55/63 и 56/121), в которых справедливо констатируется, что интенсивный рост информационно-цифровой преступности диктует настоятельную необходимость взаимодействия государств в противодействии ей не только на национальном, но и на международном уровне.

Важно подчеркнуть, что в минувшие два с половиной десятилетия российское государство прилагало настойчивые усилия по активизации и укреплению международного сотрудничества в данной области. Так, 18 ноября 2019 г. Российской Федерацией были внесены на рассмотрение Третьего комитета сессии Генеральной ассамблеи ООН и одобрены большинством голосов (вопреки позиции США) пакет предложений и резолюция «Противодействие использованию информационно-коммуникационных технологий в преступных целях» [3, с. 16]. Эти документы включают формулировки соответствующих международных принципов взаимодействия государств в связи с назревшей необходимостью укрепления безопасности глобальных телекоммуникационных и информационно-цифровых систем в борьбе как с кибертерроризмом, так и с общеуголовной цифровой преступностью. Кроме того, Российская Федерация предложила создать систему международного слежения за добросовестностью

выполнения государствами взятых на себя обязательств в этой сфере.

Свидетельством стремления к укреплению такого сотрудничества являются также усилия российской стороны в этом направлении на региональном уровне. Так, в 2001 году участниками СНГ было подписано Соглашение о взаимодействии входивших в него стран в борьбе с преступлениями в сфере компьютерной информации с четким перечнем таких умышленных общественно опасных деяний, которые предлагалось считать уголовно наказуемыми. В 2018 году теми же государствами было подписано Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий, в котором был значительно расширен их перечень, по сравнению с предыдущим соглашением. Ярким примером осуществления попыток унификации национальных законодательств в этой области служит также инициированное Российской Федерацией и ратифицированное затем государствами – членами Шанхайской организации сотрудничества – ШОС (в данном случае – Россией, Казахстаном, Таджикистаном) межправительственное соглашение о сотрудничестве в сфере обеспечения международной информационной безопасности от актов использования информационных ресурсов и (или) воздействия на них в информационном пространстве в противоправных целях. В первую очередь речь шла о противодействии кибертерроризму и общеуголовной компьютерной преступности. Правда, от ратификации упомянутого соглашения воздержалась Китайская Народная Республика [3, с. 29]. Тем не менее, участие России в подготовке этого международного документа и в его реализации, несомненно, является большим вкладом в обеспечение международной информационной безопасности. В равной мере велика роль Российской Федерации в подготовке и проведении XII саммита членов БРИКС (Бразилии, России, Индии, Китая, Южной Африки), состоявшегося 17 ноября 2020 г. и затронувшего в том числе проблему международной информационной безопасности. Очевидно, таким образом, Россия выступает активным участником в деле разработки и осуществления совместной стратегии государств в противодействии информационно-цифровой преступности. Важнейшим элементом этой международной стратегии является унификация уголовно-правовых норм, регулирующих ответственность за неправомерный доступ к компьютерной информации и использование вредоносных компьютерных программ.

Вместе с тем приходится с сожалением констатировать, что, несмотря на общность интересов стран мирового сообщества в обеспечении безопасности объектов критической информационной структуры, в том числе с помощью уголовно-правовых средств, подходы конкретных государств к решению этой проблемы существенно различаются. В частности, обращает на себя внимание тот факт, что усилия России по разработке и принятию единой нормативно-правовой базы сотрудничающих государств для противодействия все возрастающему использованию в преступных целях информационно-цифровой среды не всегда встречают понимание и поддержку со стороны других государств. Так, Российская Федерация вынуждена была отказаться от ратификации Конвенции о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) в силу своего несогласия с некорректным формулированием в тексте конвенции ст. 32, фактически дающей право представителям стран-участниц трансграничного доступа к хранящимся на территории другого государства компьютерным данным, поскольку это может нанести ущерб его безопасности. Вполне логично, что, несмотря на сложившуюся ситуацию, Россия сохранила за собой право ратифицировать указанную конвенцию, но лишь в случае пересмотра странами-участницами упомянутого пункта. И подобный пример, к сожалению, не единственный. Свидетельство тому, на наш взгляд, итоги уже упомянутого выше XII саммита членов БРИКС. Так, с одной стороны, в Московской декларации этого саммита подчеркивалась важность разработки единой нормативно-правовой базы для противодействия неуклонно возрастающему использованию информационно-коммуникационных технологий в преступных целях, а с другой – в ходе дискуссии страны БРИКС так и не смогли принять отдельного документа, в котором демонстрировался бы их согласованный подход к законодательной трактовке преступлений в сфере высоких технологий.

4. Но как бы там ни было, в заключение есть все основания утверждать следующее. В сложившейся международной ситуации пристальное внимание к современным тенденциям в сфере анализируемого направления пра-

вовой политики, проявившееся в значительном числе принятых правовых актов, отражающих задачи в сфере обеспечения кибербезопасности российского государства, является предельно актуальным и его трудно переоценить. В этой связи, по справедливому мнению специалистов в области кибербезопасности [7], очевидно и другое: реализация существующего комплекса мер по защите информации, включая реагирование на кибератаки и своевременность ликвидации последствий посягательств на объекты критической инфраструктуры, нуждается в дальнейшем повышении эффективности каждого структурного элемента упомянутого комплекса, в том числе его законодательной базы. И это вполне объяснимо. Ведь совершенствование нормативно-правовой базы во многом обеспечивает качество и надежность как информационно-коммуникационных технологий, так и самой среды их функционирования. При этом для успешного решения назревших задач несомненное значение имеет развитие международных контактов и более тесного сотрудничества государств в этой сфере, включая совместную разработку глобальных информационно-цифровых стандартов и унификацию уголовного законодательства в части ответственности за информационно-цифровые деликты.

Список источников

1. Ватрушкин А. А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. № 6 (31). С. 78–84.

2. Воронин Ю. А. Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. 2020. № 1 (23). С. 74–80.

3. Воронин Ю. А. Преступления в сфере обращения цифровой информации: сравнительные аспекты: учебное пособие. Челябинск: Издательский центр ЮУрГУ, 2021. 40 с.

4. Воронин Ю. А., Дмитриева А. А., Кухтина Т. В. Взаимодействие субъектов обеспечения информационно-цифровой безопасности: страноведческий анализ // Вестник Южно-Уральского государственного университета. Серия «Право». 2022. Т. 22. № 3. С. 13–20.

5. Безопасность критической информационной инфраструктуры РФ // Государство, бизнес, технологии. 2022. 20 мая. Яндекс-Интернет-Ресурс.

6. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие / А. В. Аносов и др. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

7. Стрельцов А. А. Проблемы правового обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Интернет изнутри. 2016. № 4. Яндекс-Интернет-Ресурс.

8. Хлопов О. А. Проблемы кибербезопасности и защиты критической инфраструктуры // Журнал «The Scientific Heritage». 2020. № 45-5 (45). С. 64–69.

References

1. Vatrushkin A. A. [Legal bases for ensuring cybersecurity of critical infrastructure of the Russian Federation]. *Evraziyskaya advokatura [Eurasian Advocacy]*, 2017, no. 6 (31), pp. 78–84. (in Russ.)

2. Voronin Yu. A. [Crimes in the sphere of digital information circulation and their determinants]. *Viktimologiya [Victimology]*, 2020, no. 1 (23), pp. 74–80. (in Russ.)

3. Voronin Yu. A. *Prestupleniya v sfere obrashcheniya tsifrovoy informatsii: sravnitel'nye aspekty* [Crimes in the sphere of digital information circulation: comparative aspects]. Chelyabinsk, 2021, 40 s.

4. Voronin Yu. A., Dmitrieva A. A., Kukhtin T. V. [Interaction of subjects of information and digital security: a country-specific analysis]. Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya «Pravo» *[Bulletin of the South Ural State University. Series "Law"]*, 2022, Vol. 22, no. 3, pp. 13–20. (in Russ.)

5. *Bezopasnost' kriticheskoy informatsionnoy infrastruktury RF* [Security of the critical information infrastructure of the Russian Federation]. *Gosudarstvo, biznes, tekhnologii [State, business, technologies]*, 2022, 20 maâ. Ândeks-Internet-Resurs.

6. Anosov A. V. *Deyatel'nost' organov vnutrennikh del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informatsionnykh, kommunikatsionnykh i vysokikh tekhnologiy* [Activities of the internal affairs bodies to combat crimes committed with the use of information, communication and high technologies]. Moscow, 2019, Ch. 1, 208 p.

7. Ctrel'tsov A. A. *Problemy pravovogo obespecheniya bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii* [Problems of legal security of critical information infrastructure of the Russian Federation]. Internet iznutri [Internet from the inside], 2016, no. 4. Yandeks-Internet-Resurs.

8. Khlopov O. A. [Problems of cybersecurity and protection of critical infrastructure]. *Zhurnal «The Scientific Heritage» [The Scientific Heritage Magazine]*, 2020, no. 45-5 (45), pp. 64–69.

Информация об авторах

Воронин Юрий Александрович, доктор юридических наук, профессор кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск, Россия.

Дмитриева Анна Александровна, доктор юридических наук, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск, Россия.

Information about the authors

Yuri A. Voronin, Doctor of Sciences (Law), Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russia.

Anna A. Dmitrieva, Doctor of Sciences (Law), Head of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russia.

Поступила в редакцию 10 октября 2022 г.
Received 10 October 2022.