УДК 349.681
DOI https://doi.org/10.17308/vsu.proc.law.2021.3/3553

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ ЗАПИСЕЙ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ

И. А. Трофимец

Посольство России в Испании

Поступила в редакцию 25 июля 2021 г.

Аннотация: *исторически записи актов гражданского состояния проводились, прежде всего, в публичных интересах, информация в подтверждение существования лица и его правовых статусов собиралась для исполнения налоговых и воинских повинностей. Традиционно сведения о гражданском состоянии лица являются конфиденциальными, доступ к ним ограничен. Институт записей актов гражданского состояния подвергся существенным метаморфозам: от церковных метрических книг до электронного ресурса. Цифровая трансформация всех сфер общественных отношений, с одной стороны, обеспечивает более комфортные условия жизнедеятельности людей, а с другой – создает определенные проблемы, связанные, в том числе, с обеспечением информационной безопасности. Меры, направленные на гарантию информационной безопасности, носят технический и юридический характер. В статье предпринята попытка охарактеризовать меры информационной безопасности и информационной сферы записей актов гражданского состояния.*
Ключевые слова: *записи актов гражданского состояния, информационная сфера, информационная безопасность, юридические и технические меры.*

Abstract: *historically, civil status records were carried out primarily in the public interest, information confirming the existence of a person and his legal status was collected for the performance of tax and military duties. Traditionally, information about a person's civil status is confidential, access to it is limited. The Institute of Civil Status Records has undergone significant metamorphoses: from church metric books to an electronic resource. The digital transformation of all spheres of public relations, on the one hand, provides more comfortable living conditions for people, and on the other hand, creates certain problems related, inter alia, to ensuring information security. Measures aimed at guaranteeing information security are of a technical and legal nature. The article attempts to characterize the information security of the information sphere of civil status records.*
Key words: *civil status records, information sphere, information security, legal and technical measures.*

Информация записей актов гражданского состояния и информационная сфера записей актов гражданского состояния (далее – ЗАГС) – категории не тождественные. Понятие информационной сферы трактуется широко как в официальных источниках, так и в научных работах[1]. Наи-

[1] См.: *Морозов А. В., Полякова Т. А.* Организационно-правовое обеспечение информационной безопасности. М., 2013 ; *Лопатин В. Н.* Информационная безопасность России : человек, общество, государство. М., 2007.

более полное определение содержится в Доктрине информационной безопасности Российской Федерации: «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений»[2]. Таким образом, информационная сфера это более широкое понятие, одним из компонентов которого является информация, считающаяся базовой категорией в информационном праве.

Под информационной сферой ЗАГС понимаем совокупность объектов: правовые источники и правовые принципы, регулирующие сферу общественных отношений по записи актов гражданского состояния, информация об актах гражданского состояния, так называемая база данных о гражданском состоянии граждан, федеральная государственная информационная система «Единый государственный реестр записей актов гражданского состояния», официальные сайты региональных органов исполнительной власти в сфере государственной регистрации актов гражданского состояния, официальные сайты региональных органов местного самоуправления в сфере государственной регистрации актов гражданского состояния, Единый портал государственных услуг и функций (ЕПГУ), официальные сайты многофункциональных центров предоставления государственных и муниципальных услуг, мобильное приложение «Реестр ЗАГС», программное обеспечение, технологическое оборудование, телекоммуникационные сети, а также архивы ЗАГС.

Только во взаимосвязи и взаимодействии всех компонентов может «жить» сложный механизм (организм) под названием «информационная сфера» ЗАГС. Основополагающим элементом является информация о государственной регистрации актов гражданского состояния, которая относится к информации ограниченного доступа. Собственно, ради государственной регистрации актов гражданского состояния, имеющей юридическое значение, запущен весь этот механизм. Для его бесперебойного функционирования необходим комплекс организационных, правовых, технических мер, обеспечивающих его защищенность от внешних и внутренних угроз, который называется информационной безопасностью.

По мнению Г. Г. Камаловой, «в системе правового обеспечения информационной безопасности в информационном праве в настоящее время сформировано относительно устойчивое объединение группы норм права, регулирующих совокупность имеющих специфику общественных отношений по обеспечению конфиденциальности сведений – институт

[2] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru

информации ограниченного доступа»[3]. Действительно одна из проблем построения глобального информационного общества – это соблюдение прав и свобод граждан, прежде всего гарантированных Конституцией России, в частности обеспечение конфиденциальности частной и семейной жизни. Информационная безопасность – это фундаментальное понятие информационного права и важная категория для информационной сферы ЗАГС. Наиболее разработана концепция информационной безопасности в работах Т. А. Поляковой[4].

В Доктрине информационной безопасности Российской Федерации содержится понятие информационной безопасности применительно к Российской Федерации, что означает состояние защищенности личности, гражданского общества и государства за счет сбалансированности и компромисса частных и публичных интересов в информационной среде. Для государства информационная безопасность связывается с охраной общих национальных интересов, что приобретает большую актуальность в связи с реальной возможностью применения потенциала новейших информационно-коммуникационных технологий в целях обеспечения военно-политического превосходства, силового противоборства и шантажа[5].

Под информационной безопасностью понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений (в том числе владельцам и пользователям информации). По причине интенсивного развития информационных отношений, их трансграничного характера отмечаем тенденцию все большего заимствования зарубежных юридических терминов и правовых конструкций, в частности по вопросам защищенности информационной сферы как особого пространства взаимодействия людей и машин. Такой подход оправдан, поскольку разрастание информационного пространства, совершенствование технических устройств и технологического оборудования опережает объективные возможности самих средств информационной безопасности. Но именно языковый барьер порождает терминологическую путаницу, в том числе и на законодательном уровне.

Прежде чем перейти к анализу информационной безопасности в информационной сфере записей актов гражданского состояния, следует определиться с терминами, стремительно меняющимися и обновляющимися, которые необходимы для понимания института «информационная безопасность». Информационную безопасность сопоставляют с IT-без-

[3] *Камалова Г. Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. … д-ра юрид. наук. М., 2020. С. 73.

[4] См., например: *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России : дис. … д-ра юрид. наук. М., 2008

[5] Стратегический вектор обеспечения международной информационной безопасности / сост. М. А. Вус, О. С. Макаров. СПб., 2016.

опасностью и кибербезопасностью. Объединяет эти термины то, что они относятся к категории «защищенность» и имеют трансграничный характер[6]. Но тождественны ли эти категории? В доктрине существуют различные точки зрения, имеющие антагонистический характер и не вносящие ясность в понимание этой юридической категории.

Обратимся к Международному стандарту по информационной безопасности (ISO/IEC 27001 2005 г.), который стал справочным документом для управления и обеспечения безопасности информации в публичных и частных структурах и организациях[7]. Исходя из содержания этого стандарта информационная безопасность рассматривается исключительно в контексте процессов цифровизации информации (информационные технологии – методы безопасности (средства, способы) – системы информационной безопасности – нормативные требования) и включает юридические, организационные и технические меры.

Информационная безопасность относится к защите информации и является частью кибербезопасности, которая считается общим (родовым) понятием, поскольку имеет отношение ко всей системе управления информацией[8].

Существует противоположное мнение: кибербезопасность и информационная безопасность сооотносятся как частное и общее[9]. Так, А. К. Жарова пытается обосновать вывод о том, что кибербезопасность является составной частью информационной безопасности, под которой она в свою очередь предлагает понимать «состояние защищенности личности, общества и государства от внутренних и внешних вызовов и угроз, создаваемых противоправной деятельностью, направленной на нарушение конфиденциальности, целостности, доступности и устойчивости информационной инфраструктуры и безопасности информационной среды доверия, при котором обеспечиваются оборона и безопасность государства, реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, информационный суверенитет и устойчивое социально-экономическое развитие Российской Федерации»[10]. При этом А. К. Жарова в своей диссертационной работе утверждает, что в зарубежном праве термин кибербезопасность чаще используется в значении информационная безопасность.

[6] Вопросы информационной безопасности и кибербезопасности в различных аспектах исследовали Ю. М. Батурин, И. Л. Бачило, А. П. Баранов, Л. А. Букалерова, О. В. Дамаскин, А. А. Ефремов, А. К. Жарова, Н. Н. Куняев, Д. А. Ловцов, О. С. Макаров, А. В. Минбалеев, В. Б. Наумов, Т. А. Полякова, А. Н. Савенков, А. В. Тонконогов, А. А. Фатьянов и др.

[7] Разработан совместно Международной организацией по стандартизации и Международной электротехнической комиссией.

[8] См.: *Лидовский В. В.* Теория информации. М., 2004. С. 4.

[9] См.: *Жарова А. К.* Теоретические основания правового регулирования создания и использования информационной инфраструктуры в Российской Федерации : автореф. дис. … д-ра юрид. наук. М., 2020. С. 15.

[10] Там же.

Кибербезопасность и информационная безопасность – не сопоставимые категории, находятся в разных плоскостях, относятся к разным явлениям реальной действительности[11]. В качестве примера приводятся такие понятия, как информационные войны и киберконфликты (кибератаки), которые различаются, поскольку имеют разные объекты посягательств. Информационные войны с применением фейков, троллингов, вбросов, астротурфинга и др. имеют своим объектом информацию (факты объективной реальности) и сводятся к ее искажению или удалению. Однако в конечном счете кибератаки направлены на доступ к информации с целью ее незаконного изменения, передачи, удаления, распространения или использования в противоправных целях. В связи с этим разграничение по вышеупомянутому критерию считаем нецелесообразным.

Термин «ИТ-безопасность» в официальных источниках не встречается (информационные технологии, инновационные технологии). В трудах ученых ИТ-безопасность связана с технической уязвимостью устройств и оборудования (машин). Полагаем, что в конечном счете это связано с защищенностью самой обрабатываемой, передаваемой, хранящейся информацией. Информационно-коммуникационные технологии признаны главным фактором развития глобального информационного общества.

Информационная безопасность и кибербезопасность – это синонимы[12]. Полагаем, что такой подход может быть аргументирован определением кибернетики как науки об информации в сложных управляющих системах и абсолютной тождественностью многих категорий, например: информационная сфера (информационное пространство, информационная среда) и киберсфера (киберпространство, киберсреда). Верность этого подхода подтверждается официальной терминологической позицией, используемой в законодательных и правоприменительных актах.

Считаем, что научные дискуссии по вопросу соотношения терминов «информационная безопасность», «ИТ-безопасность» и «кибербезопасность» нецелесообразны по причине образования ими синонимического ряда адекватности (тождественности) значения и функционально-стилевого употребления. Встречаем и другие термины, например «цифровая безопасность»[13], которые могут дополнить синонимический ряд «информационной безопасности».

Цифровизация государственного управления признана необходимым направлением цифрового развития страны[14]. Цифровизация обще-

[11] См., например: *Аллеев А. С.* Терминология безопасности : кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5(8). С. 39–42.

[12] См., например: *Ключевская Н.* Информационная безопасность и COVID-19 : рекомендации для бизнеса и граждан. URL: https://www.garant.ru/article/1421147/ (дата обращения: 04.05.2021).

[13] См.: *Овчинский В. С.* Виртуальный щит и меч. М., 2018.

[14] См.: *Ефремов А. А., Южаков В. Н.* Механизмы выявления правовых ограничений цифровизации государственного управления // Информационное общество. 2020. № 4. С. 80–88.

ственных отношений ставит перед государством новые задачи в сфере обеспечения информационной безопасности, доступа к информации и ее использования, для решения которых требуется создание необходимой организационно-правовой основы.

Под информационной безопасностью понимается совокупность превентивных юридических, организационных и технических мер, направленных на охрану (защищенность) информационной сферы, в том числе информации (данных, сведений и сообщений).

Концепция информационной безопасности основана на четырех принципах: *легитимность доступа, конфиденциальность, целостность* и *авторизация*. Легитимность означает исключение несанкционированного доступа к информации. Конфиденциальность – невозможность разглашения сведений без согласия их бенефициара. Целостность – недопустимость неправомерной модификации информации. Авторизация – подтверждение идентификации и аутентификации пользователя. Соблюдение этих руководящих начал в информационной сфере означает ее киберустойчивость, т. е. способность управлять внешними и внутренними рисками и преодолевать их с минимальными потерями и затратами. Большая нагрузка в реализации концепции информационной безопасности ложится на разработку технических решений и анализ рисков, которые обеспечивают защиту инфраструктуры и предлагают необходимые инструменты для эффективного управления ею, а также гарантируют непрерывность в ее работе в случае нарушения (атаки, угрозы).

Угроза информационной безопасности информационной сферы актов гражданского состояния – это возможная опасность причинения вреда объектам этой информационной сферы, затрагивающая как публичные, так и частные права и законные интересы. *Атака* информационной безопасности информационной сферы записей актов гражданского состояния – это попытка осуществления угрозы информационной безопасности этой информационной сферы. *Нарушение* информационной безопасности информационной сферы актов гражданского состояния – это реализация угрозы информационной безопасности информационной сферы актов гражданского состояния.

Угроза информационной безопасности может быть направлена на подрыв киберустойчивости, а именно представлять возможную опасность легитимности доступа, конфиденциальности, целостности и авторизации.

Угрозы информационной безопасности могут классифицироваться по разным критериям. Угрозы информационной безопасности могут представлять возможную опасность компонентам информационной сферы: непосредственно базе данных (информации), программному обеспечению и технологической инфраструктуре. В зависимости от пространственной расположенности источника угрозы информационной безопасности могут быть внутренними и внешними. По участию человека в создании

опасности информационной безопасности угрозы могут быть субъективные, вызванные действиями человека, умышленными или случайными, а также объективные, независимые от воли и желания человека, вызванные событиями непреодолимой силы.

Нарушения информационной безопасности информационной сферы ЗАГС могут сводиться к следующим неблагоприятным последствиям: порча оборудования, сбой программного обеспечения (в том числе системного), искажение и удаление файлов, содержащих информацию ЗАГС, изменение режимов работы технических устройств, обслуживающих офисы и серверы ЗАГС, повреждение носителей информации (форматирование), распространение в сети «Интернет» таких сведений, не подлежащих разглашению, как информация ограниченного доступа, разглашение сертификатов, обеспечивающих легитимность доступа, дешифрование, несоблюдение криптографических протоколов, хищение информации и носителей информации и др.). Способы нарушения информационной безопасности информационной сферы ЗАГС: несанкционированный доступ и иные несанкционированные действия по отношению к информации ЗАГС с помощью технических средств, запуск вредоносных (вирусных) программ, физическое уничтожение носителей информации и т. д.

Информационная безопасность в информационной сфере записей актов гражданского состояния обеспечивается организационными, техническими и юридическими мерами.

Юридические меры – закрепленные в нормативных правовых актах требования, соблюдение которых обеспечивает охрану информации и других компонентов информационной сферы. Юридические меры определяют права и обязанности участников и правовые режимы объектов информационных отношений, носят превентивный характер, направлены на профилактику правонарушений в информационной сфере, устанавливают ответственность (гражданскую, административную, уголовную и дисциплинарную) в случае правонарушений. Юридические меры – это санкции за нарушение норм информационного права.

Установление правовых режимов информации, в том числе определения критериев отнесения сведений к информации ограниченного доступа, – это одна из юридических мер. Информация ЗАГС имеет следующие качества:

– информация ограниченного доступа;

– персональные данные;

– профессиональная тайна.

Каждое свойство акта гражданского состояния закреплено на законодательном уровне как правовой режим этого объекта, т. е. специальным порядком возникновения, изменения и прекращения прав, особым содержанием правоотношения, а также видами санкций за ненадлежащее исполнение обязанностей. Характеристики зарегистрированного акта гражданского состояния обозначены в п. 8 ст. 6 Федерального закона от

15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»[15]: «Сведения, ставшие известными *работнику* органа записи актов гражданского состояния или *работнику* многофункционального центра предоставления государственных и муниципальных услуг в связи с государственной регистрацией акта гражданского состояния, в том числе *персональные данные*, являются *информацией*, *доступ* к которой *ограничен* в соответствии с федеральными законами, и разглашению не подлежат». Отнесение сведений к категории информации ограниченного доступа производится федеральным законом в целях охраны конституционных основ, нравственных устоев, здоровья граждан, прав и законных интересов участников общественных отношений, обеспечения безопасности государства. Поскольку информация ЗАГС получена работником органа записи актов гражданского состояния или работником многофункционального центра предоставления государственных и муниципальных услуг при выполнении ими профессиональных обязанностей, а именно в связи с государственной регистрацией акта гражданского состояния, то она составляет профессиональную тайну. Однако в законе нет прямого закрепления обязанности по соблюдению конфиденциальности такой информации. Прослеживается тенденция отказа от прямого использования термина «конфиденциальность» применительно к актам гражданского состояния. Так, с 2018 г. утратила силу ст. 12 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния», где определялась информация о государственной регистрации актов гражданского состояния как конфиденциальная.

В связи с этим предлагаем изложить п. 8 ст. 6 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния» в следующей редакции: *«Сведения, ставшие известными работнику органа записи актов гражданского состояния или работнику многофункционального центра предоставления государственных и муниципальных услуг в связи с государственной регистрацией акта гражданского состояния, в том числе персональные данные, являются информацией, доступ к которой ограничен в соответствии с федеральными законами, и разглашению не подлежат. Работник органа записи актов гражданского состояния или работник многофункционального центра предоставления государственных и муниципальных услуг обязан соблюдать конфиденциальность информации, полученной им в связи с государственной регистрацией акта гражданского состояния».*

Одним из составляющих юридической меры информационной безопасности на ограничение доступа к информации является указание на бенефициара информации о государственной регистрации актов гражданского состояния, содержащееся в Едином государственном реестре записей актов гражданского состояния. Бенефициар информации о госу-

[15] Об актах гражданского состояния : федер. закон от 15 ноября 1997 г. № 143-ФЗ (в ред. от 24.04.2020) // Собр. законодательства Рос. Федерации. 1997. № 47. Ст. 5340.

дарственной регистрации актов гражданского состояния, содержащейся в Едином государственном реестре записей актов гражданского состояния – это лицо, имеющее право на доступ к информации, в отношении которого произведена государственная регистрация акта гражданского состояния, а также в отношении каждого из его детей, не достигших совершеннолетия. Информация о государственной регистрации актов гражданского состояния предоставляется бенефициарам через единый портал государственных и муниципальных услуг и региональные порталы государственных и муниципальных услуг, т. е. исключительно авторизованным пользователям государственных и муниципальных услуг через единую систему идентификации и аутентификации. Органы записи актов гражданского состояния также предоставляют сведения бенефициарам при личном посещении офисов или направляют ответы по почте, включая электронные сообщения, при условии достоверного подтверждения личности бенефициара.

Важной юридической мерой, сопровождаемой техническими разработками, является процесс авторизации пользователей информацией ЗАГС. Здесь речь идет как о работниках органа записи актов гражданского состояния или работниках многофункционального центра предоставления государственных и муниципальных услуг, так и о бенефициарах информации ЗАГС.

Выделяем еще одну юридическую меру – законодательно закрепленный алгоритм получения информации о государственной регистрации актов гражданского состояния. В настоящее время сведения, содержащиеся в федеральной государственной информационной системе (ФГИС) «Единый государственный реестр записей актов гражданского состояния» предоставляются системой межведомственного электронного взаимодействия (СМЭВ) посредством доступа (для органов исполнительной власти) и запросов иных уполномоченных лиц. Проблема защищенности канала связи для подключения к СМЭВ носит технический характер.

Введение электронного документооборота и межведомственного электронного взаимодействия информационной сферы записей актов гражданского состояния поставили проблему идентификации и аутентификации уполномоченных лиц, законодательное решение которой свелось к введению института электронной подписи.

Система юридических мер, обеспечивающих информационную безопасность в информационной сфере актов гражданского состояния, представлена превентивными требованиями, соблюдение которых направлено на охрану субъектов информационных отношений и санкциями в случае правонарушений в информационной сфере.

Превентивные меры составляет соблюдение следующих требований:

– определение режима ограниченного доступа применительно к информации о государственной регистрации актов гражданского состояния;

– установление федеральным законом видов сведений, составляющих информацию об актах гражданского состояния;

– предоставление сведений об актах гражданского состояния исключительно бенефициару, а также уполномоченным органам исполнительной власти и организациям;

– применение процесса авторизации при допуске или запросе к информации об актах гражданского состояния, а также получении государственной услуги в сфере ЗАГС;

– использование электронной подписи, усиленной квалифицированной электронной подписи в электронном документообороте информационной сферы ЗАГС.

Таким образом, меры-санкции, предусматриваемые за правонарушения в информационной сфере ЗАГС и направленные на восстановление нарушенных прав и законных интересов субъектов информационных отношений, можно сгруппировать по отраслевой принадлежности:

– гражданско-правовые санкции, которые содержатся в Гражданском кодексе Российской Федерации[16] и заключаются в денежных возмещениях причиненного ущерба (в случае нарушения личных неимущественных прав граждан-бенефициаров ст. 15 (возмещение убытков) и ст. 151 (компенсация морального вреда));

– административные санкции, которые устанавливаются Кодексом Российской Федерации об административных правонарушениях[17] за административные проступки, как правило, наложение административного штрафа (в случае нарушения порядка государственного управления в информационной сфере актов гражданского состояния: ст. 13.28 (нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления); ст. 13.33 (нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи); ст. 13.33.1 (нарушение установленных правил создания (замены) и выдачи ключа простой электронной подписи и правил использования федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» и др.);

– уголовные санкции за совершение преступлений (преступления в информационной сфере ЗАГС могут иметь следующие составы в соответствии с Уголовным кодексом Российской Федерации[18]: ст. 155 (раз-

[16] Гражданский кодекс Российской Федерации : федер. закон от 30 ноября 1994 г. № 51-ФЗ (ч. 1) (в ред. от 11.06.2021) // Собр. законодательства Рос. Федерации. 1994. № 32. Ст. 3301.

[17] Кодекс Российской Федерации об административных правонарушениях : федер. закон от 30 декабря 2001 г. № 195-ФЗ (в ред. от 11.06.2021) // Собр. законодательства Рос. Федерации. 2002. № 1 (ч. 1). Ст. 1.

[18] Уголовный кодекс Российской Федерации : федер. закон от 13 июня 1996 г. № 63-ФЗ (в ред. от 11.06.2021) // Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 2954.

глашение тайны усыновления (удочерения)), ст. 159 (мошенничество), ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание, использование и распространение вредоносных компьютерных программ), ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей), ст. 290 (получение взятки), ст. 285 (злоупотребление должностным положением), ст. 292 (служебный подлог);

– дисциплинарные санкции за неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей в виде замечания, выговора, увольнения, предусмотренные Трудовым кодексом Российской Федерации[19].

Библиографический список

Аллеев А. С. Терминология безопасности : кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 5 (8). С. 39–42.

Ефремов А. А., Южаков В. Н. Механизмы выявления правовых ограничений цифровизации государственного управления // Информационное общество. 2020. № 4. С. 80–88.

Жарова А. К. Теоретические основания правового регулирования создания и использования информационной инфраструктуры в Российской Федерации : дис. … д-ра юрид. наук. М., 2020. 429 с.

Камалова Г. Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. … д-ра юрид. наук. М., 2020. 472 с.

Ключевская Н. Информационная безопасность и COVID-19 : рекомендации для бизнеса и граждан. URL: https://www.garant.ru/article/1421147/

Лидовский В. В. Теория информации. М., 2004. 111 с.

Лопатин В. Н. Информационная безопасность России : человек, общество, государство. М., 2007. 428 с.

Морозов А. В., Полякова Т. А. Организационно-правовое обеспечение информационной безопасности. М., 2013. 276 с.

Овчинский В. С. Виртуальный щит и меч. М., 2018. 320 с.

Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : дис. … д-ра юрид. наук. М., 2008. 438 с.

Стратегический вектор обеспечения международной информационной безопасности / сост. М. А. Вус, О. С. Макаров. СПб., 2016. 122 с.

References

Alleev A. S. Terminology of security: cybersecurity, information security // Questions of cybersecurity. 2014. № 5 (8). P. 39–42.

[19] Трудовой кодекс Российской Федерации : федер. закон от 30 декабря 2001 г. № 197-ФЗ (в ред. от 30.04.2021) // Собр. законодательства Рос. Федерации. 2002. № 1(ч. 1). Ст. 3.

Efremov A. A., Yuzhakov V. N. Mechanisms for identifying legal limitations of digitalization of public administration // Information Society. 2020. №. 4. P. 80–88.

Zharova A. K. Theoretical foundations of legal regulation of the creation and use of information infrastructure in the Russian Federation: Dissertation for the degree of doctor of legal sciences. M., 2020. 429 p.

Kamalova G. G. Legal provision of information confidentiality in the conditions of the development of the information society: Dissertation for the degree of doctor of legal sciences. M., 2020. 472 p.

Klyuchevskaya N. Information security and COVID-19: recommendations for business and citizens. URL: https://www.garant.ru/article/1421147/

Lidovsky V. V. Information theory. M., 2004. 111 p.

Lopatin V. N. Information security of Russia: Man, society, state. M., 2007. 428 p.

Morozov A. V., Polyakova T. A. Organizational and legal support of information security: monograph. M., 2013. 276 p.

Ovchinsky V. S. Virtual shield and sword. M., 2018. 320 p.

Polyakova T. A. Legal support of information security in the construction of an information society in Russia: Dissertation for the degree of doctor of legal sciences. M., 2008. 438 p.

Strategic vector of ensuring international information security / comp. M. A. Vus, O. S. Makarov. Saint Petersburg, 2016. 122 p.

Для цитирования:

Трофимец И. А. Информационная безопасность в информационной сфере записей актов гражданского состояния // Вестник Воронежского государственного университета. Серия: Право. 2021. № 3 (46). С. 229–240. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3553

Recommended citation:

Trofimets I. A. Information security in the information sphere of civil status records // Proceedings of Voronezh State University. Series: Law. 2021. № 3 (46). P. 229–240. DOI: https://doi.org/10.17308/vsu.proc.law.2021.3/3553

Посольство России в Испании

Трофимец И. А., кандидат юридических наук, доцент

E-mail: kosareva-khv@mail.ru

Embassy of Russia in Spain

Trofimets I. A., Candidate of Legal Sciences, Associate Professor

E-mail: kosareva-khv@mail.ru