

Ссылка для цитирования этой статьи:

Канина Е.Н. Правовая информация в аспекте информационных технологий // Human Progress. 2025. Том 12, Вып. 1. URL: http://progress-human.com/images/2026/Tom12_1/Kanina.pdf DOI 10.46320/2073-4506-2026-1a-6.

УДК 340

ПРАВОВАЯ ИНФОРМАЦИЯ В АСПЕКТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Канина Елена Николаевна

доцент кафедры гуманитарных и социально-экономических дисциплин,
Восточно-Сибирский филиал,
Российский государственный университет правосудия имени В.М. Лебедева,
г. Иркутск, Российская Федерация

Аннотация. В настоящее время внедрение информационных технологий в правовую сферу существенно меняет процессы создания, изменения и распространения законодательства. Информационные технологии улучшают доступность правовой информации для населения. До настоящего времени в Российской Федерации не принят единый закон о нормативных правовых актах, регулирующий единые требования, предъявляемые к нормативным правовым актам и к их подготовке. Правовое регулирование данного вопроса осуществляется при помощи Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»; Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»; Постановления Правительства РФ от 20.11.2012 № 1198 «О федеральной государственной информационной системе, обеспечивающей процесс досудебного (внесудебного) обжалования решений и действий (бездействия), совершенных при предоставлении государственных и муниципальных услуг»; Постановление Правительства РФ от 25.08.2012 № 851 «О порядке раскрытия федеральными органами исполнительной власти информации о подготовке проектов нормативных правовых актов и результатах их общественного обсуждения» и др. Рассматривая в статье преимущества внедрения цифровых технологий автор в то же время акцентирует внимание на существующих проблемах, делает значимые выводы, вносит предложения про разрешению существующих проблем.

Ключевые слова: цифровые технологии, электронное Правительство, электронный документооборот, электронное общественное обсуждение, компьютерный мониторинг, фишинговые атаки, анонимайзеры.

Цифровые технологии проникают во все сферы жизнедеятельности, в том числе, в систему права и в систему законодательства. Внедрение информационных технологий в правовую сферу существенно меняет процессы создания, изменения и распространения законодательства, а также улучшает доступность правовой информации для населения.

В Российской Федерации нет единого федерального закона, который однозначно определил бы сущность цифровых технологий. Однако, существуют нормативные правовые акты, в которых раскрывается понятие цифровых технологий. Например, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в статье 2 которого говорится, что информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Иными словами, информационные технологии – это область знаний и практических навыков, связанных с использованием компьютеров и программного обеспечения, помощью которых были созданы электронное правительство – электронные платформы и системы для обмена информацией между органами власти, гражданами и предприятиями, которые позволяют получать государственные услуги, оплачивать госпошлины, штрафы и задолженности¹.

Процесс создания, изменения и публикации законов и других правовых актов с использованием информационных технологий называется электронное законодательство. Именно электронное законодательство позволяет ускорить разработку и внедрение законодательных актов, а также повысить их доступность и прозрачность².

¹ Пример электронного правительства – единый портал государственных и муниципальных услуг Gosuslugi.ru.

² Пример, информационно-правовая система «Законодательство России» – официальный интернет-портал правовой информации, где можно найти правовые документы федерального и регионального уровня, материалы судебной практики; сайт Министерства юстиции РФ – предлагает базу данных действующих правовых актов: документы федерального законодательства, нормативные правовые акты субъектов РФ, муниципальных образований и уставы; федеральный портал проектов нормативных правовых актов это ресурс Минэкономразвития России, где граждане могут знакомиться с новыми законопроектами и изменениями в нормативно-правовых актах, принимать участие в их обсуждении и вносить предложения; государственная автоматизированная система «Правосудие», на основе которой формируется единое информационное пространство судов общей юрисдикции в России. Пользователь может найти сведения о судебных органах, нормативные акты судов, информацию о находящихся в судах делах и принятых по ним решениях, а также образцы документов: исковых заявлений и жалоб.

Электронный документооборот используется при проведении экспертиз, прогнозировании последствий принятия нормативных правовых актов, при их согласовании и направлении в правотворческий орган³.

С использованием информационных технологий, стало возможным электронное общественное обсуждение, которое позволяет вести речь о развитии правотворческой инициативы гражданского общества. Отдельные граждане и их организации могут вносить на рассмотрение соответствующего правотворческого органа или проект нормативного правового акта, или предложение принять нормативный правовой акт по конкретному вопросу, а так же довести до сведения государственных органов своё мнение по поводу планируемых «властных» решений, проектов нормативных правовых актов и других значимых общественных вопросов⁴.

Компьютерный мониторинг законодательного процесса применяется с целью получить оперативную информацию о состоянии и динамике всей массы законопроектов, о соблюдении установленных Конституцией РФ сроков выполнения тех или иных действий⁵.

Однако, при всех преимуществах использования цифровых технологий, существует ряд проблем, одной из самых значимых считаем безопасность данных. Юридические прецеденты, документы и дела содержат конфиденциальную информацию, которую нужно защитить от несанкционированного доступа, что не всегда возможно в условиях

³ Пример использования электронного документооборота в правотворческой деятельности в России – подготовка проектов правовых актов в территориальных органах Министерства внутренних дел РФ. Согласно приказу МВД России от 26.12.2018 №880 «Об утверждении Правил подготовки правовых актов в территориальных органах Министерства внутренних дел Российской Федерации», подготовка проектов правовых актов осуществляется с помощью Сервиса электронного документооборота единой системы информационно-аналитического обеспечения деятельности МВД России.

⁴ Например, интернет-ресурс «Российская общественная инициатива» (РОИ). Это платформа для публичного представления предложений граждан по различным вопросам существующего законодательства, а также для объективного, всестороннего и конструктивного рассмотрения этих инициатив. В Иркутской области на форуме «Сообщество» в 2024 году были представлены проекты по профилактике семейного насилия и оказанию экстренной и комплексной помощи одиноким женщинам с детьми, беременным женщинам, пострадавшим от семейного насилия; проекты по улучшению качества жизни детей-сирот и детей, оставшихся без попечения родителей, проживающих в социальных учреждениях и в приёмных семьях; проекты по оказанию комплексной помощи семьям, воспитывающих детей с ОВЗ, в том числе по адаптивному конному спорту; проекты по социальной поддержке онкопациентов; проекты по популяризации народных бурятских игр. Также в Иркутской области уже больше десяти лет активно работает программа «Народные инициативы». Некоторые примеры реализованных проектов: ледовый каток на сквере Кирова, креативное пространство «Гуркин. Послесловие», фестиваль «Алые паруса Иркутска», посвящённый Дню выпускника.

⁵ Пример компьютерного мониторинга законодательного процесса – автоматизированная система обеспечения законодательной деятельности (АСОЗД), запущенная в 1997 году для информационного обеспечения деятельности Совета Федерации и Госдумы. С помощью этой системы пользователи могли отслеживать ход законодательного процесса, изучать тексты законопроектов, законов и связанной с ними документации. В базе системы находились, например: исходный вариант законопроекта, этапы его движения в государственных органах, сведения о лицах, ответственных за состояние законопроекта, и другие параметры.

цифровизации. Так, количество фишинговых атак⁶ с использованием Telegram увеличилось в 3,6 раза, через WhatsApp (принадлежит признанной в России экстремистской и запрещённой корпорации Meta) – в 4 раза. Злоумышленники маскируют фишинговые ссылки под сообщения от друзей, курьеров или представителей сервисов [1].

Разновидностью фишинговых атак является электронный фишинг (почтовый) – мошенники отправляют письмо, которое выглядит как сообщение от банка, магазина или другой официальной организации. Внутри есть ссылка и мотивация к действию, например, подтвердить аккаунт или проверить персональную скидку. Примером тому служат подделки страницы входа на «Госуслуги». Пользователь получает «уведомление» о штрафе или судебной задолженности, переходит по ссылке и без подозрений вводит логин и пароль, которые и являются целью мошенников [2].

Еще одной проблемой, на наш взгляд, являются регуляторные ограничения в сфере информационных технологий, связанные с ограничениями доступа к информации. Например, Закон о суверенном интернете⁷, Закон об анонимайзерах⁸, который запретил использовать на территории РФ информационно-телекоммуникационные сети и информационные ресурсы (анонимайзеры) для получения доступа к информации, доступ к которой ограничен на территории РФ.

⁶ Фишинговые атаки (фишинг, англ. phishing) – это способ интернет-мошенничества, при котором злоумышленники пытаются получить личную информацию пользователей: логины, пароли, номера банковских карт и т. д. – с помощью маскировки под надёжные источники. Цель – заставить человека перейти по ссылке, ввести данные и тем самым передать их мошенникам.

⁷ «Закон о суверенном интернете» – неформальное название Федерального закона от 1 мая 2019 года №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Цель закона – создание независимой инфраструктуры для бесперебойного функционирования интернета в России. Она должна обеспечить работоспособность сайтов в случае невозможности подключения российских операторов связи к зарубежным корневым серверам интернета. В законе говорится, что операторы связи обязаны установить государственное оборудование на точках обмена трафиком для анализа и фильтрации трафика внутри страны и линиях связи, пересекающих границу России; операторы связи обязаны вносить в регистр и использовать исключительно эти точки обмена (порядок определяет Правительство); Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций реализует «централизованное управление» Рунетом; Роскомнадзор реализует ограничение доступа к запрещённым в России сайтам; для проверки процедур проводят учения; создаётся национальная система доменных имён. Официальная точка зрения властей о необходимости принятия этого закона заключается в защите российского сегмента Сети от внешних угроз, однако эксперты и правозащитные организации основной целью закона считают контроль, цензуру и изоляцию российского сегмента интернета.

⁸ Поправки в федеральный закон «Об информации, информационных технологиях и о защите информации», которые вступили в силу с 1 ноября 2017 года. Суть закона – ограничение доступа к запрещённой информации через анонимайзеры – технологии, которые позволяют обходить блокировку сайтов с запрещённой информацией. Закон не распространяется на операторов государственных операционных систем, госорганы и органы местного самоуправления. Закон не содержит положений об ответственности простых интернет-пользователей за обход блокировок запрещённых сайтов. Ответственность несут те, кто обеспечивает доступ к таким сайтам – владельцы анонимайзеров.

Далее, запрет на использование VPN. Выявленным анонимайзерам направлялось требование подключиться к Федеральной государственной информационной системе, содержащей реестр запрещённых сайтов. Если владелец анонимайзера не делал этого в течение 30 дней с момента получения требования, его работа блокировалась Роскомнадзором. Например, в марте 2025 года Роскомнадзор начал вводить массовое ограничение на IP-адреса Cloudflare, на котором работают многие VPN-сервисы. Это привело к сбоям в работе TikTok, Twitch, Epic Games и других платформ. За март 2025 года ведомство потребовало удалить 47 VPN-приложений из магазина приложений Google Play. При этом, технология VPN сама по себе не запрещена. Главное – не позиционировать эти решения как способ доступа к ограниченному контенту. Однако, по мнению некоторых авторов, техническая блокировка новых каналов распространения информации является неэффективной. Это связано с тем, что в информационном обществе новые способы и каналы распространения информации появляются быстрее, чем оказываются заблокированы старые.

Хотелось бы остановиться на еще одной проблеме, а именно вопросе о юридической силе соглашений, заключённых в электронной форме. Собственно законодательство РФ позволяет заключать сделки в письменной форме с помощью электронных документов, передаваемых по соответствующим каналам связи. Об этом говорится в статьях 160, 434 Гражданского кодекса РФ (далее – ГК РФ), статье 11 ФЗ № 149-ФЗ.

Однако, чтобы электронный договор имел юридическую силу, необходимо соблюсти ряд нюансов, связанных с использованием определённого вида электронной подписи. Если стороны договорились использовать простую электронную подпись (далее – ЭП), в соглашении об этом должны содержаться: условие о правилах идентификации подписанта документа и условие о соблюдении лицом конфиденциальности ключа простой ЭП (статьи 6, 9 Федерального закона РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»). Если стороны договорились использовать неквалифицированную ЭП, то в соглашении об её использовании они должны предусмотреть порядок проверки такой подписи (ст. 9 ФЗ № 63-ФЗ). При использовании сторонами усиленной квалифицированной электронной подписи такого соглашения не требуется.

Чтобы электронный договор признали действительным, нужно соблюдать два требования: содержание можно воспроизвести на материальном носителе – например, распечатать; партнёров, указанных в договоре, можно безошибочно установить.

Если заключить договор без учёта этих требований, его нельзя будет использовать как доказательство в судебном разбирательстве. Кроме того, не всегда получается использовать электронные договоры, у такого формата есть ряд исключений. Например, если в законе прямо

указан бумажный формат или между сторонами сделки заключено соглашение, по которому договор составляется только на бумаге.

К проблемам можно отнести и высокие затраты на инфраструктуру. Разработка и внедрение новых технологий в правовой сектор могут потребовать значительных инвестиций⁹.

Таким образом, информационные технологии позволяют формировать ресурсы правовой информации, собирать, обрабатывать и анализировать её, что помогает государственным органам разрабатывать и принимать нормативные правовые акты, с другой стороны, существующие проблемы требуют скорейшего законодательного разрешения. Необходимо разработать и принять новые нормативно-правовые акты, которые обеспечивали бы информационную безопасность на современном уровне, исходя из понимания того, что цифровая среда постоянно создаёт всё новые риски, государство и общество должны осознать эти риски, а также создать средства для их предупреждения.

Список литературы

1. Число утечек в 2024-м выросло до 455, атак шифровальщиков — до 500. URL: <https://www.anti-malware.ru/news/2025-02-19-111332/45308> (дата обращения: 18.10.2025).
2. Фишинг в 2025-м – мошенники всё чаще маскируются под банки, мессенджеры и маркетплейсы. URL: <https://securitymedia.org/news/fishing-v-2025-m-moshenniki-vsye-chashche-maskiruyutsya-pod-banki-messendzhery-i-marketpleysy.html> (дата обращения: 18.10.2025).

⁹ По информации на 1 октября 2025 года, в рамках национального проекта «Экономика данных и цифровая трансформация государства» запланировано финансирование в размере 507,9 млрд рублей на ближайшие три года. Так, на 2026 год – 155,3 млрд рублей, на 2027 год – 168,9 млрд рублей, на 2028 год – 183,7 млрд рублей. В «Экономику данных» входят такие проекты, как «Инфраструктура доступа», «Цифровые платформы в отраслях социальной сферы», «Искусственный интеллект», «Цифровое государственное управление» и другие.

LEGAL INFORMATION IN THE ASPECT OF INFORMATION TECHNOLOGY

Kanina Elena Nikolaevna

Associate Professor of the Department of Humanities and Socioeconomic Disciplines
East Siberian Branch,
Russian State University of Justice named after V.M. Lebedeva
Irkutsk, Russian Federation

Abstract. Currently, the introduction of information technology in the legal sphere is significantly changing the processes of creating, amending, and disseminating legislation. Information technology improves the accessibility of legal information to the public. To date, the Russian Federation has not adopted a unified law on regulatory legal acts that would regulate uniform requirements for regulatory legal acts and their preparation. Legal regulation of this issue is carried out by the Federal Law of 27.07.2006 No. 149-FZ "On Information, Information Technologies and Information Protection"; Federal Law of 27.07.2010 No. 210-FZ "On the Organization of the Provision of State and Municipal Services"; Federal Law of 06.04.2011 No. 63-FZ "On Electronic Signature"; RF Government Resolution of 20.11.2012 No. 1198 "On the Federal State Information System Ensuring the Process of Pre-Trial (Extra-Judicial) Appealing of Decisions and Actions (Inactions) Committed in the Provision of State and Municipal Services"; Russian Government Resolution No. 851 of August 25, 2012, "On the Procedure for Disclosing Information by Federal Executive Authorities on the Preparation of Draft Regulatory Legal Acts and the Results of Their Public Discussion," and others. While examining the advantages of implementing digital technologies, the author also highlights existing challenges, draws significant conclusions, and makes proposals for resolving them.

Keywords: digital technologies, e-Government, electronic document management, electronic public discussion, computer monitoring, phishing attacks, anonymizers.

References

1. The number of leaks in 2024 increased to 455, ransomware attacks to 500. URL: <https://www.anti-malware.ru/news/2025-02-19-111332/45308> (date of access: October 18, 2025).
2. Phishing in 2025 – fraudsters increasingly disguise themselves as banks, instant messengers, and marketplaces. URL: <https://securitymedia.org/news/fishing-v-2025-m-moshenniki-vsye-chashche-maskiruyutsya-pod-banki-messendzhery-i-marketpleysy.html> (date of access: October 18, 2025).