

НОВЫЙ ВЕКТОР В РЕГУЛИРОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ: ПРОБЛЕМЫ И НЕОБХОДИМЫЕ ШАГИ ДЛЯ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ РУНЕТА

Шварц Л.В.¹

Ключевые слова: информация, идентификация, аутентификация, авторизация, информационная система, контроль доступа, пользователь, владелец информационного ресурса, новостной агрегатор, провайдер хостинга.

Аннотация

Цель работы: анализ законодательных новелл в сфере информационной безопасности, действие которых распространяется на способы авторизации пользователей на российских сайтах и деятельность провайдеров хостинга, освещение решаемых за счет настоящих перемен существующих проблем и возможных последствий принятых изменений.

Методы исследования: анализ, синтез, систематизация научных, а также нормативных правовых источников.

Результаты исследования: сформулирована авторская позиция о требуемых изменениях в законодательстве с точки зрения их прикладного применения для восполнения созданной законодателем правовой неопределенности в области информационной безопасности. Сделаны выводы о необходимости проработки существующих правовых понятий взамен включения нового понятия «авторизация пользователя», а также о пересмотре правового регулирования функционирования провайдеров хостинга в части переноса ответственности за действия пользователей на провайдеров, что фактически блокирует возможность нормальной работоспособности хостинга.

DOI: 10.24412/1994-1404-2025-2-72-78

Введение

Вопрос информационной безопасности на сегодняшний день приобрел национальный масштаб и является одним из актуальнейших аспектов борьбы с возможным негативным информационным воздействием, имеющим направленный и намеренный характер. Один из основополагающих документов, имеющий программный характер и на законодательном уровне регламентирующий эту борьбу, — Доктрина информационной безопасности, утвержденная Указом Президента РФ от 05.12.2016 № 646. Она декларирует необходимость обеспечения полноценного самостоятельного присутствия Российской Федерации в международном информационном поле и формирование механизма отбора каналов поставки достоверных данных и новостей, чтобы минимизировать риски и ущерб от дезинформационных вбросов и определить дальнейшее совершенствование правовых институтов с целью представления интересов населения и государства в коммуникационном

пространстве. Как утверждает В.Н. Лопатин, именно система информационной безопасности интегрирует все ключевые компоненты политики нацбезопасности в единое целое [1, с. 40—41]. При этом, исходя из Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 02.07.2021 № 400, в приоритете не просто обеспечение безопасного использования информационных технологий, но и создание для этого надлежащих условий (п. 57). Этот стратегический национальный приоритет развития созвучен Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон № 149-ФЗ), одно из положений которого устанавливает, что защита информации включает в себя в том числе и меры по реализации права на доступ к информации (ст. 16). Действительно, широкое использование информационных технологий, цифровизация различных сфер жизни обще-

¹ Шварц Лариса Владимировна, кандидат юридических наук, доцент, доцент кафедры гражданского и трудового права Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Санкт-Петербург, Российская Федерация.

E-mail: shvarts-lv@ranepa.ru

ства привели к тому, что «информационная политика Российской Федерации является регулятором публичных и частных правоотношений, посредством чего реализуются стратегические задачи государства» [2, с. 55].

В конце 2023 года вступила в силу новая редакция Закона № 149-ФЗ, где уточняются требования, предъявляемые к владельцам российских информационных ресурсов, провайдером хостинга и новостным агрегаторам. Эта редакция подготовлена с учетом изменений, внесенных Федеральным законом от 31.07.2023 № 406-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“ и Федеральный закон „О связи“» и Федеральным законом от 12.12.2023 № 588-ФЗ «О внесении изменения в статью 8 Федерального закона „Об информации, информационных технологиях и о защите информации“». По сути, происходит переностройка законодательства на решение задач, возникших среди прочего в связи с необходимостью информационной защиты россиян [3, с. 17].

Остановимся на двух ключевых моментах предстоящих изменений.

Способы авторизации на интернет-сайтах

Первое ключевое изменение коснулось ст. 8: в ней появился п. 10, обязывающий владельца сайта (программы, аккаунта, иного сетевого ресурса) авторизовывать пользователей одним из доступных в данный момент способов:

- через личный номер мобильной связи (при исключении обязанности соблюдения государственного порядка использования номера мобильной связи и отмене правила о заключении с мобильным оператором или поставщиком беспроводной связи договора об идентификации);
- через подтвержденную учетную запись абонента в Единой системе идентификации и аутентификации (ЕСИА, которой на данный момент является портал Госуслуг);
- через Единую биометрическую систему (ЕБС), хранящую такие персональные данные, как изображение лица и образец голоса человека;
- через иную систему, отвечающую установленным правовым нормам защиты информации и принадлежащую отечественному юридическому лицу или физическому лицу, имеющему только гражданство РФ.

В указанных выше случаях под российским юридическим лицом понимается юридическое лицо, находящееся под контролем РФ, субъекта РФ, муниципального образования, гражданина РФ, не имеющего гражданства другого государства, и (или) контролируемых ими совместно или по отдельности лиц. Под контролем, в свою очередь, понимается возможность определять решения, принимаемые указанным юридическим лицом, в силу наличия права прямо или косвенно распоряжаться более чем 50% общего количества голосов,

приходящихся на голосующие акции (доли), составляющие уставный капитал юридического лица.

Представители Государственной Думы РФ пояснили, что под «иной информационной системой» понимается ряд российских сервисов, таких как социальная сеть «ВКонтакте» или почтовый и поисковый сервис Mail.ru, не имеющих государственного или муниципального характера и созданных частными юридическими или физическими лицами².

Ограничение нужно будет соблюдать российским организациям и гражданам с интернет-бизнесом в РФ. Перечисленные способы авторизации распространяются на пользователей, которые находятся в России.

Так, 1 декабря 2023 года должен был вступить в силу запрет на регистрацию в Рунете с иностранной электронной почты. Планировалось, что нововведение распространится только на бизнес, осуществляемый на отечественных интернет-платформах, и указанные методы авторизации не коснутся международного интернет-бизнеса.

Если иностранные компании, сайтом которых пользуются россияне, находятся под контролем государственных органов РФ, то на них ограничение распространяется аналогично.

Автор приводимых в статье поправок депутат Государственной Думы Антон Вадимович Горелкин заверил, что данные изменения, призванные ограничить «использование для авторизации российских пользователей на информационных ресурсах, владельцами которых являются российские граждане и организации, иностранных систем, обеспечивающих такую авторизацию»³, обсуждались с представителями отечественного бизнеса разных уровней.

В тексте поправок не содержится сведений об ограничении способов регистрации новостных агрегаторов, включенных в реестры Роскомнадзора — федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Имеются в виду ресурсы с доступом более миллиона пользователей в сутки, такие как паблик «ВКонтакте», новостной агрегатор «Рамблер» и блогинг-платформа «Дзен», а также организаторы распространения информации — владельцы сайтов, соцсетей, мессенджеров и отзовиков.

Включенность всех вышеперечисленных субъектов в реестр Роскомнадзора обеспечивает их полную информационную прозрачность для органов государственной власти и контроля: ведомствам известны собственники этих ресурсов и инструментов распространения информации, способы связи с ними, сфера их ответственности (проще говоря, за что с них

² См., например, пояснения председателя Комитета Госдумы РФ по информационной политике Хинштейна А.Е. URL: <https://www.forbes.ru/tekhnologii/493489-duma-prinala-zakon-o-zaprete-na-registraciu-v-runete-s-zarubeznoj-elektronnoj-pochtoj> (дата обращения: 01.11.2024)

³ России с 1 декабря вводится запрет на регистрацию в Рунете с иностранной электронной почты. URL: <https://habr.com/ru/news/751532/> (дата обращения: 02.11.2024).

спрашивать, кому направлять предписания и запросы, а также на кого накладывать штрафные санкции). Таким образом, новые поправки в закон затронут всех без исключения владельцев сайтов с пользовательской авторизацией⁴.

Сложность видится и в том, что деятельность большинства информационных систем носит трансграничный характер, поэтому правильно подмечено, что «национальные правила идентификации могут оказаться неэффективными» [4, с. 178].

В поправках к ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ «О связи» не предусмотрены санкции для владельцев интернет-ресурсов, которые не обеспечат возможность регистрации нужными способами. Видимо, меры ответственности будут прописаны в будущем после оценки правоприменительной практики [5, с. 12].

По замыслу разработчиков, новации затронут только сайты с регистрацией и аутентификацией пользователей — например, электронные торговые площадки, выступающие посредниками между продавцом и покупателем товара.

Согласно ст. 15.1 Закона № 149-ФЗ, при выявлении факта распространения сайтом или доменом информации о способах обхода установленных в РФ блокировок появляется основание для внесения такого ресурса в Единый реестр запрещенной информации Роскомнадзора. Однако запрет касается только любой рекламы способа обхода блокировок и никак не затрагивает само право пользователя применять инструменты безопасного соединения с общедоступной сетью, такие как VPN-сервисы⁵.

Тем, кто на момент принятия закона уже зарегистрированы на российских сайтах при помощи иностранной электронной почты, проходить аутентификацию заново не придется, т. е. обратной силы у закона не будет.

Итак, вводятся новые правила регистрации на интернет-площадках, которые уже прозвали Законом об авторизации. Система управления доступом к информации должна обеспечивать надежную и безопасную идентификацию и аутентификацию [6, с. 1], поскольку именно от эффективности этих процессов во многом зависит общая безопасность информационных систем.

Тем не менее пока что применение закона вызывает вопросы из-за неоднозначности трактовки некоторых его положений. Например, подпадают ли под действие вновь установленных правил сайты с подпиской на информационную рассылку или регистрацией пользователей на мероприятия через подтверждение адреса

электронной почты, в том числе и корпоративной? И что подразумевается под «авторизацией» — только первичная регистрация пользователя или любой его вход в аккаунт или систему?

Попробуем разобраться.

В первом случае проблема возникнет, если речь идет о регистрации новых пользователей с зарубежной почты, так как она будет находиться под запретом в целях сохранности персональных данных и снижения интеграции сервисов из недружественных стран в российские системы. Однако буквальных требований к стране регистрации почты в законе нет, если она используется в качестве логина. Физические лица, уже имеющие аккаунты в иностранных почтовых сервисах (Gmail, Microsoft и т. п.), могут продолжать пользоваться ими. Единственная ситуация, когда потребуются обязательный российский адрес электронной почты (e-mail) — при создании нового аккаунта на российском сайте. Естественно, никто не будет проверять, с помощью каких e-mail регистрируют блоги или малые инфосайты, так как это невозможно технически, как и нереально проверить документы на принадлежность системы регистрации корпоративного адреса российскому правовому полю.

Вместе с тем программисты советуют пользователям менять способы входа на сайты. Представляется, что во избежание сложностей лучше перейти на российские сервисы, как это сделали государственные служащие. Вероятнее всего, со временем интернет-площадки, отказавшиеся ввести регистрацию на базе российских «технологий единого входа», будут подвержены штрафным санкциям за несоблюдение требований по работе с персональными данными. Многие российские сайты уже убрали авторизацию через иностранные системы — к примеру, маркетплейс Ozon.

Что касается подписки на e-mail-рассылки, новые требования Закона № 149-ФЗ сработают, если форма регистрации совмещена с согласием на получение рекламных писем, так как e-mail будет использоваться для входа. Поэтому во всех остальных случаях пользователь вправе указать российский или иностранный адрес электронной почты, как посчитает нужным.

Во втором случае ситуация представляется сложнее в связи с тем, что зачастую «информационное законодательство не успевает за развитием информационно-коммуникационной сферы на базе электронной среды и оперирует устаревшими словами, а также тавтологичными, метафоричными и противоречивыми определениями легальных понятий» [7, с. 645].

Авторизация и аутентификация — это два совершенно разных процесса. Аутентификация нужна, чтобы проверить право доступа к данным, об авторизации же можно говорить только после получения доступа.

Стоит отметить, что в соответствии с требованиями ч. 1 ст. 16 Закона № 149-ФЗ защита информации, включая доступ к телекоммуникационным сетям, представляет собой принятие правовых, организационных

⁴ Установлен запрет регистрации на российских сайтах с помощью иностранных электронных почтовых сервисов. URL: https://admrebr.gosuslugi.ru/dlya-zhiteley/informatsiya-01/novosti_1309.html (дата обращения: 02.11.2024).

⁵ Данные о способах обхода блокировок станут основанием для включения сайта в реестр РКН. URL: <https://tass.ru/obschestvo/18326933> (дата обращения: 04.11.2024).

и технических мер. Идентификацию, аутентификацию и авторизацию пользователей относят к техническим мерам, дополняющим организационные меры и улучшающим общую защиту сайта [8, с. 414], создавая комплексную систему безопасности для серверных систем, защищающую данные от внутренних и внешних угроз [9, с. 447].

Проверка всегда начинается с идентификации, за ней идёт аутентификация и в конце авторизация. Все эти этапы помогают обезопасить важную информацию и защищают, например, персональные данные пользователей, деньги на подключенных к профилю счетах.

Идентификация — установление системой существования конкретного пользователя на основе предоставленных им определенных данных (например, номера телефона или логина).

Аутентификация — подтверждение пользователем своего права доступа в систему путем введения пароля, пин-кода, биометрии или другим предустановленным способом.

Авторизация — определение персональных привилегий и прав пользователя на данном ресурсе (например, просмотр и отправка электронной почты).

По тексту поправок речь идет о том, чтобы обязать владельцев сайтов проводить авторизацию, т. е. про действия внутри системы, так как авторизация — это элемент работы самой системы по определению набора прав в этой системе.

Представляется, что по замыслу инициаторов данных поправок речь все-таки идет об аутентификации, и названные мероприятия призваны контролировать доступ к информационной системе. Но если заменить термин «авторизация» на «аутентификацию», то не может быть использован четвертый способ регистрации пользователей — с использованием других систем, отвечающих требованиям о защите сведений, причем владеть этой системой должен российский гражданин либо человек без гражданства другой страны. Получается, что для того, чтобы иметь функции в одной информационной системе, необходимо получить разрешение в другой информационной системе. Таким образом, идентифицировать пользователей могут и частные информационные системы, но при условии наличия необходимой для этого инфраструктуры. Например, исходя из Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями, утвержденных постановлением Правительства РФ от 12 апреля 2018 г. № 447, доступ к негосударственной информационной системе обеспечивается с использованием подтвержденной учетной записи физического лица в федеральной государственной информационной системе с получением из нее набора сведений о заявителе (п. 5).

При этом многие авторы отмечают высокую степень риска от различного уровня использования сведений с информационных систем, принадлежащих частным лицам [10, с. 16].

К слову, утвержден и введен в действие приказом Росстандарта от 10.04.2020 № 159-ст «ГОСТ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения», в котором прописано, что в целях защиты информации решение о предоставлении доступа для использования информационных и вычислительных ресурсов средств вычислительной техники, а также ресурсов автоматизированных (информационных) систем основывается на результатах идентификации и аутентификации. Кстати, в Федеральном законе от 29.12.2022 № 572-ФЗ «Об использовании биометрических персональных данных» речь идет об осуществлении именно идентификации и аутентификации на основе биометрических персональных данных физических лиц.

Регулирование работы хостинг-провайдеров

Второе изменение, на которое необходимо обратить внимание, коснулось уже самих провайдеров в части утверждения новой ст. 10.2-1 Закона № 149-ФЗ. Напомним, что провайдер хостинга — это лицо, осуществляющее деятельность по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет. С 1 декабря 2023 года деятельность хостингов контролируется Роскомнадзором через учет определенных действий провайдера. Так, провайдер хостинга должен:

- уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале такой деятельности;
- обеспечить соответствие защиты персональных данных требованиям, предъявляемым законом к данной деятельности;
- соблюдать требования к вычислительной мощности, установленные государственными органами, уполномоченными на ведение деятельности по обеспечению госбезопасности и правопорядка, для проведения мероприятий в целях реализации возложенных на них задач;
- предоставить вычислительные мощности для публикации данных в Интернете гражданам, обратившимся к провайдеру, только после прохождения идентификации и аутентификации.

Отметим, что вышеупомянутый государственный орган ведет Реестр хостингов, где хранит подробные сведения о них и об их действиях. В некоторых случаях Роскомнадзор вправе привлечь к ведению списка сторонние уполномоченные организации.

После 1 февраля 2024 года лица, которые не включены в Реестр, не могут оказывать услуги хостинга в России. Кроме того, с 1 сентября 2024 года операторы

государственных и муниципальных информационных систем могут пользоваться услугами хостинга только у провайдеров, не находящихся под иностранным контролем и размещающих технические средства хостинга в России.

Однако если ведомство обнаружит нарушение требований по защите данных, получив информацию от Федеральной службы безопасности РФ или подведомственных органов, то будет обязано выдать нарушителю предписание с указанием срока устранения недочетов. При этом максимальный срок исправления составляет 10 суток. Провайдер же, в свою очередь, обязан проинформировать государственный орган о выполнении обязательств в письменном виде. Если он не исправит ситуацию, отказавшись от принятия предложенных мер либо не оповестит о ликвидации ситуации, Роскомнадзор вправе исключить провайдера из соответствующего реестра.

Это буквально означает, что теперь тот, кто сдает свои вычислительные мощности в аренду, обязан с целью соблюдения требований по защите информации отслеживать действия своих клиентов и нести за них ответственность. Теперь будут блокироваться не пути, а сам ресурс, и обязанность эта возлагается на хостинг-провайдера. И если ранее не было законных оснований на разрыв экономических отношений, то согласно новым правилам (оказание услуг по предоставлению хостинга только компаниями из Реестра), Роскомнадзор полномочен исключать из данного Реестра, а за этим немедленно последует лишение лицензии.

Справедливости ради следует заметить, что согласно Федеральному закону от 12 декабря 2023 г. № 588-ФЗ «О внесении изменения в статью 8 Федерального закона „Об информации, информационных технологиях и о защите информации“» переход российских IT-компаний к авторизации через отечественные государственные сервисы перенесли на 2025 год. На сегодняшний день российские владельцы сайтов и программ могут проводить авторизацию через отдельную информационную систему, которая должна отвечать требованиям к защите информации и принадлежать владельцу ресурса или экономически значимой организации.

Решение об установлении переходного периода до 1 января 2025 г. для вступления вышеуказанных ограничений было принято с целью гарантии стабильного функционирования платформ и подготовки

их к переводу под российский контроль⁶. В понимании автора, вряд ли послабления в исполнении данных новелл позволят добиться единообразного толкования как понятия авторизации, так и нового порядка регистрации на российских сайтах, но хотя бы дадут время владельцам и провайдерам информационных ресурсов адаптироваться под новые правила.

Заключение

Таким образом, несмотря на вполне оправданные опасения относительно сложности перенесения технических категорий в правовые без потери качественной составляющей [11], для решения обозначенных стратегических задач следовало начать с фундаментальной работы по унификации нормативной правовой терминологии в сфере использования информационных технологий, на основе которой разработать юридический тезаурус, где закрепить также общие принципы идентификации и аутентификации, не углубляясь в подробную регламентацию авторизации. Исходя из реалий, справедливым будет отметить, что право как инструмент и средство управления процессами социума меняет свои формы, содержание, механизмы формирования и реализации, подвергаясь воздействию цифровых технологий [12, 13]. В части изменений правового регулирования деятельности хостинг-провайдеров попытка законодателя обеспечить выполнение правил информационной безопасности за счет агента, предоставляющего платформу для пользователей, размещающих на ней контент, содержание которого вне контроля провайдера, представляется нежизнеспособной правовой конструкцией, не приводящей к повышению уровня безопасности Рунета. Необходимо смена субъекта ответственности, а именно возложение ответственности на лиц, определяющих информационный контент, публикуемый на том или ином ресурсе, для существования которого хостинг-провайдеры предоставляют свои услуги. Настоящие изменения являются неэффективными и становятся очередной преградой для бизнеса из-за выбора тактики борьбы законодателя с нарушениями законодательства об информации.

⁶ Данные о способах обхода блокировок станут основанием для включения сайта в реестр РКН. URL: <https://tass.ru/obschestvo/18326933> (дата обращения: 04.11.2024).

Литература

1. Лопатин В.Н. Проблемы информационного права в цифровой экономике // Право и государство. 2019. № 1 (82). С. 40—56.
2. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51—56.
3. Цифровое право / А. Дюфло, Л.В. Андреева, В.В. Блажеев [и др.]; под общей редакцией В.В. Блажеева, М.А. Егоровой; Министерство науки и высшего образования Российской Федерации, Московский государственный юридический университет им. О.Е. Кутафина. Учеб. изд. М. : Проспект, 2020. 640 с.

4. Непомнящий П.А. Идентификация наследодателя цифровых прав // Гуманитарные, социально-экономические и общественные науки. 2024. № 6. С. 177—180. DOI: 10.24412/2220-2404-2024-6-16.
5. Ершова Е.А. Комментарий к Федеральному закону от 31 июля 2023 г. № 406-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О связи» // Нормативные акты для бухгалтера. 2023. № 16. С. 12.
6. Бельский В.С., Герасимов И.Ю., Сабанов А.Г., Царегородцев К.Д. Анализ моделей идентификации и аутентификации // International Journal of Open Information Technologies. 2024. Т. 12. № 5. С. 1—14.
7. Нестеров А.В. Информационно-терминологические проблемы персональных данных в условиях цифровизации экономики // Россия: тенденции и перспективы развития : ежегодник. Материалы XX Национальной научной конференции с международным участием, Москва, 14—15 декабря 2020 г. Вып. 16. Ч. 1. М. : Институт научной информации по общественным наукам РАН, 2021. С. 645—648.
8. Матевосян Г.А. Системы обеспечения информационной безопасности в официальных сайтах образовательных организаций // Вестник науки. 2024. Т. 1. № 4 (73). С. 408—415.
9. Лисай В.Э. Безопасность в backend-разработке: современные методы защиты и шифрования данных // Вестник науки. 2024. Т. 3. № 4 (73). С. 437—449.
10. Антропов Д.В., Комаров С.И., Рассказова А.А. Обоснование приоритетности данных единого государственного реестра недвижимости перед данными иных информационных систем // Современные проблемы земельно-имущественных отношений, урбанизации территории и формирования комфортной городской среды : сборник докладов Международной научно-практической конференции, Тюмень, 28 октября 2022 года. Тюмень : Тюменский индустриальный университет, 2023. С. 13—18.
11. Щеглов Е.Н. Организационно-правовые аспекты авторизации пользователей для доступа к информационным системам с использованием сети Интернет // Полиция и общество: проблемы и перспективы взаимодействия. 2021. № 3. С. 205—210.
12. Хабриева Т.Я. Технологические революции и их проекция в праве // Вопросы истории. 2022. № 2-2. С. 256—270.
13. Хабриева Т.Я. Технологические императивы современного мира и право // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19. № 1. С. 5—12. DOI: 10.12737/jzsp.2023.001.

SECTION:
CONSTITUTIONAL LAW

A NEW VECTOR IN REGULATING INFORMATION RESOURCES: PROBLEMS AND STEPS NEEDED FOR ENSURING THE SECURITY OF RUNET

Larisa Schwartz, Ph.D. (Law), Associate Professor at the Department of Civil and Labour Law of the Russian Presidential Academy of National Economy and Public Administration, Saint Petersburg, Russian Federation.

E-mail: shvarts-lv@ranepa.ru

Keywords: information, identification, authentication, authorisation, information system, access control, user, information resource owner, news aggregator, hosting provider.

Abstract

Purpose of the study: analysing legislative novelties in the information security field whose effect extends to ways of user authorisation on Russian websites and hosting provider activities, covering the existing problems that are being solved using the said changes in law and possible consequences of these changes.

Methods used in the study: analysis, synthesis, and systematisation of legal sources, scholarly as well as regulatory ones.

Study findings: the author's stance is worded on the required changes in law from the standpoint of applying them for filling in the legal uncertainty in the information security area created by the law makers. The following conclusions are made: an elaboration of existing legal notions is needed instead of introducing a new one, that is, "user authorisation", and legal regulation of hosting providers' operation to the extent of shifting the responsibility for users' actions to the provider should be reviewed since such a shift practically blocks the possibilities for normal hosting operation.

References

1. Lopatin V.N. Problemy informatsionnogo prava v tsifrovoi ekonomike. Pravo i gosudarstvo. 2019. No. 1 (82). Pp. 40–56.
2. Duben' A.K. Informatsionnaia bezopasnost' v sisteme natsional'noi bezopasnosti: aktual'nye problemy informatsionnogo prava. Voprosy bezopasnosti. 2023. No. 1. Pp. 51–56.
3. Tsifrovoe pravo. A. Diuflo, L.V. Andreeva, V.V. Blazheev [i dr.] ; pod obshchei redaktsiei V.V. Blazheeva, M.A. Egorovoi; Ministerstvo nauki i vysshego obrazovaniia Rossiiskoi Federatsii, Moskovskii gosudarstvennyi iuridicheskii universitet im. O.E. Kutafina. Ucheb. izd. M. : Prospekt, 2020. 640 pp.
4. Nepomniashchii P.A. Identifikatsiia nasledodatelia tsifrovyykh prav. Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki. 2024. No. 6. Pp. 177–180. DOI: 10.24412/2220-2404-2024-6-16 .
5. Ershova E.A. Kommentarii k Federal'nomu zakonu ot 31 iiulia 2023 g. No. 406-FZ "O vnesenii izmenenii v Federal'nyi zakon "Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii" i Federal'nyi zakon "O svyazi". Normativnye akty dlia bukhgaltera. 2023. No. 16. P. 12.
6. Bel'skii V.S., Gerasimov I.Iu., Sabanov A.G., Tsaregorodtsev K.D. Analiz modelei identifikatsii i autentifikatsii. International Journal of Open Information Technologies. 2024. T. 12. No. 5. Pp. 1–14.
7. Nesterov A.V. Informatsionno-terminologicheskie problemy personal'nykh dannykh v usloviakh tsifrovizatsii ekonomiki. Rossiia: tendentsii i perspektivy razvitiia : ezhegodnik. Materialy XX Natsional'noi nauchnoi konferentsii s mezhdunarodnym uchastiem, Moskva, 14–15 dekabria 2020 g. Vyp. 16. Ch. 1. M. : Institut nauchnoi informatsii po obshchestvennym naukam RAN, 2021. Pp. 645–648.
8. Matevosian G.A. Sistemy obespecheniia informatsionnoi bezopasnosti v ofitsial'nykh saitakh obrazovatel'nykh organizatsii. Vestnik nauki. 2024. T. 1. No. 4 (73). Pp. 408–415.
9. Lisai V.E. Bezopasnost' v backend-razrabotke: sovremennye metody zashchity i shifrovaniia dannykh. Vestnik nauki. 2024. T. 3. No. 4 (73). Pp. 437–449.
10. Antropov D.V., Komarov S.I., Rasskazova A.A. Obosnovanie prioritnosti dannykh edinogo gosudarstvennogo reestra nedvizhimosti pered dannymi inyykh informatsionnykh sistem. Sovremennye problemy zemel'no-imushchestvennykh otnoshenii, urbanizatsii territorii i formirovaniia komfortnoi gorodskoi sredy : sbornik dokladov Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Tiumen', 28 oktiabria 2022 goda. Tiumen' : Tiumenskii industrial'nyi universitet, 2023. Pp. 13–18.
11. Shcheglov E.N. Organizatsionno-pravovye aspekty avtorizatsii pol'zovatelei dlia dostupa k informatsionnym sistemam s ispol'zovaniem seti Internet. Politsiia i obshchestvo: problemy i perspektivy vzaimodeistviia. 2021. No. 3. Pp. 205–210.
12. Khabrieva T.Ia. Tekhnologicheskie revoliutsii i ikh proektsiia v prave. Voprosy istorii. 2022. No. 2-2. Pp. 256–270.
13. Khabrieva T.Ia. Tekhnologicheskie imperativy sovremennogo mira i pravo. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia. 2023. T. 19. No. 1. Pp. 5–12. DOI: 10.12737/jzsp.2023.001 .