УДК 340.13:004 Вестник УрФО № 2(24) / 2017, с. 41–45

Жернова В. М., Минбалеев А. В.

ОСОБЕННОСТИ ПРАВОГО СТАТУСА СУБЪЕКТОВ-УЧАСТНИКОВ ОТНОШЕНИЙ, ВОЗНИКАЮЩИХ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье поднимается вопрос о некоторых особенностях правового статуса информационных систем. Предлагается авторская классификация субъектов-участников правоотношений, возникающих при использовании информационных систем, в соответствии с набором действий и полномочий в отношении информации, входящей в состав информационной системы. Вводится понятие «пользователь информационной системы», которой предлагается ввести на законодательном уровне, ввиду отсутствия этого понятия, в отличие от дефиниций других субъектов-участников. Поднимается вопрос о процедурах идентификации и анонимизации, являющихся частью вступления субъекта в правоотношения. Кроме этого, предлагается зонирование ответственности в зависимости от компонент и составляющих информационных систем.

Ключевые слова: *информационные системы, идентификация и анонимизация, правовой статус субъектов-участников информационных правоотношений.*

Zhernova V. M., Minbaleev A. V.

PECULIARITIES OF THE RIGHT STATUS OF SUBJECTS-PARTICIPANTS IN LEGAL RELATIONSHIPS ARISING FROM THE USE OF INFORMATION SYSTEMS

The article raises the question of some features of the legal status of information systems. Author's classification of subjects-participants in legal relations arising from the use of information systems is suggested, in accordance with a set of actions and powers with regard to information that is part of the information system. The term "user of the information system" is introduced, which is proposed to be introduced at the legislative level, in view of the absence of this concept, in contrast to the definitions of other participants-participants. The issue of procedures for identification and anonymization, which are part of the subject's entry into legal relations, is being raised. In addition, the zoning of responsibility is proposed depending on the components and components of information systems.

Keywords: *information systems, identification and anonymization, legal status of subjects-participants of information legal relations.*

Повсеместное использование информационных систем в деятельности государства и граждан порождает новые виды отношений. Так, в соответствии со стадиями жизненного цикла информационных систем можно выделять стадии разработки, производства, применения и т.д. На каждой из существующих стадий жизненного цикла информационных систем преобладают присущие именно этой стадии отношения, часть из которых, подвергаясь правовому регулированию, становятся правоотношениями.

Формирующееся множество отношений определяется также и различным субъектным составом, определенными характеристиками стадии жизненного цикла информационной системы. Например, на стадии разработки ключевыми субъектами-участниками являются субъекты, которые занимаются вопросами проектирования, а на стадии применения – операторы, пользователи информационных систем. Перечень субъектного состава при этом не является исчерпывающим. Бесспорно, он открытый, поскольку развитие информационных технологий порождает новые виды субъектов соответствующих правоотношений, о чем свидетельствуют и постоянное совершенствование информационного законодательства. Так, за последние годы, перечень субъектов пополнили блогеры, новостные агрегаторы и другие. Появление в информационной сфере новых субъектов-участников информационных систем влечет за собой необходимость изменения информационного законодательства. Анализ существующих субъектов-участников информационных систем позволяет провести их классификацию в целях выявления особенностей правового статуса каждой группы субъектов.

Определение набора прав и обязанностей субъектов правоотношений является одной из главных задач для формирования правового статуса. Как отмечает И. Л. Бачило, «только правовые средства регулирования могут обеспечить прочность и порядок связей всех субъектов, задействованных в создании, формировании, использовании информационной системы с учетом ее технических, технологических и собственно информационных характеристик»[1].

Исследуем особенности правового стату-

са субъектов информационных систем. Ключевым из них является пользователь. Понятие «пользователь информационной системы» довольно широко охватывает другие категории субъектов отношений, складывающихся по поводу информационных систем. Амелин Р. В. под пользователем понимает «лицо, имеющее право на получение всей или определенной информации, содержащейся в системе»[2]. На основании исследования законодательства и локальных правовых актов отдельных организаций информационной сферы можно сделать вывод, что пользователь зачастую имеет право на все операции в отношении информации, содержащейся в информационной системе, в том числе на ее ввод и изменение. Исходя из вышесказанного под пользователем информационной системы можно понимать авторизованного в информационной системе субъекта, имеющего определенный уровень доступа к ней и возможность производить операции с информацией, хранящейся в информационной системе. Данное определение предлагается внести в ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) с целью определения прав и обязанностей данного вида субъектов, а также классификации отдельных типов пользователей.

Копылов В.А. указывал, что субъекты правового регулирования в данной области могут быть подразделены на две группы: субъекты, организующие и осуществляющие разработку информационных систем (заказчики и разработчики – органы государственной власти, юридические и физические лица – организации и предприятия, специалисты), и субъекты, осуществляющие эксплуатацию перечисленных объектов (органы государственной власти, их подразделения, юридические и физические лица)».

Мы предлагаем определить субъектный состав в зависимости от набора действий, осуществляемых с информацией в информационных системах:

– субъекты, формирующие сведения (могут являться источником информации);

– субъекты, обрабатывающие информацию;

– субъекты, передающие информацию;

– субъекты, получающие информацию.

Учитывая последние изменения в законодательстве[3], можно заявить о необходимости типологизации субъектов отношений, складывающихся, в том числе, в связи с использованием сети «Интернет», и выделения соответствующих типов субъектов. Подобная типологизация учитывает постоянное появление новых субъектов при использовании информационных систем и позволяет сформулировать общие законодательные требования к данным субъектам. Такая классификация, дополняющая Закон об информации (например, в ст. 10.2), позволит избежать неоправданного введения отдельных категорий субъектов в законодательство, таких как «блогер» или «новостной агрегатор».

На наш взгляд, определение понятия «правовой статус» не требует специальных исследований. Воспользуемся ранее предложенными выводами ученых о сущности правового статуса. Так, И. Л. Бачило[4] предлагает к рассмотрению следующее:

- общий правовой статус субъекта в информационной сфере;

- специальный правовой статус субъекта в информационной сфере;

- исключительный правовой статус субъекта в информационной сфере.

Учитывая специфику роли, которую выполняет субъект, правовой статус будет переходить в одну из предложенных категорий.

Считаем, что применительно к информационным системам, дефиниция «правовой статус субъектов» определяется как набор прав, свобод и обязанностей, определенный как на законодательном уровне, так и документацией информационной системы, а также предусмотренные меры ответственности за нарушение информационного законодательства и ненадлежащую эксплуатацию информационной системы.

Одним из условий функционирования любого субъекта информационной системы является его идентификация в ней. Проблемы идентификации наиболее остро проявляются при дистанционном обслуживании или взаимодействии пользователей с информационной системой ввиду специфики такого вида предоставления услуг. Некоторые проблемы в правовом, организационном и техническом обеспечении защиты информации, в том числе отсутствие точного регулирования процессов идентификации и авторизации, могут привести к несанкционированному доступу к данным информационной системы. Кроме этого, необходимо учитывать и процесс, обратный идентификации, - анонимизацию. Определение понятия «идентифи-

кация» находит отражение во многих нормативных документах[5], в то время, как понятие анонимности отражено в ГОСТ Р ИСО/МЭК 15408-2-2008 в части безопасности информационных технологий6 и представляет собой возможность совершать действия, не раскрывая идентификационных данных пользователей. На самом деле, определено несколько степеней сокрытия данных – анонимность, псевдонимность, невозможность ассоциации, ненаблюдаемость[7].

Применение средств для обеспечения одной их этих степеней анонимности приводит к так называемому процессу анонимизации. Понятие «анонимизация» не раскрыто в отечественном законодательстве, но есть распространенное мнение под этим понятием понимать «процесс удаления данных (из документов, баз данных и т. д.) с целью сокрытия источника информации, действующего лица и т. д.», т.е. процесс удаления персональных данных[8]. Регулирование оборота персональных данных – отдельный блок правовых норм, но в данном случае необходимо понимать, что оборот персональных данных может осуществляться без согласия субъекта в целях обеспечения безопасности, в целях предотвращения экстремистских и террористических действий. Таким образом, сам термин говорит о том, что существует необходимость защищать свои данные, конституционные права граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

В попытке защитить свои права, субъекты отношений в сети «Интернет» используют различные способы анонимизации, которые, как считается, могут обеспечить защиту именно интересов пользователей. Наиболее распространенными инструментами для сокрытия IP адресов являются: плагины, сервисы, прокси-сервера, сеть TOR и др. Стоит отметить, что применение средств анонимизации, с одной стороны, направлено на защиту прав одной группы субъектов, а с другой – на нарушение, например, авторских прав, в случае несанкционированного распространения объектов авторских прав, например в сети TOR.

Доктрина информационной безопасности[9] также освещает вопросы идентификации и анонимизации. Помимо упоминания права на свободный поиск и распространение информации, в Доктрине зафиксировано, что деятельность государственных органов по обеспечению информационной безопасности основывается, в том числе, на соблюдении баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности в информационной сфере.

Представляется возможным, что такой баланс можно найти в случае определения необходимости идентификации субъектов (или, наоборот, возможной анонимизации) при выполнении различных действий. В таком случае, можно прийти к выводу, что идентификации подлежит не факт вступления субъекта в правоотношения, возникающие при использовании информационных систем, а факт обращения к определенным ресурсам, к услугам, осуществление которых без идентификации может нанести вред субъекту таких отношений в частности, и обществу и государству в целом.

С точки зрения социальных отношений, информационные системы в целом моделируют и обеспечивают функции хранения, преобразования, обмена информацией на различных уровнях и во множестве применений. Информационные системы весьма широко используются сегодня многими организациями – государственными, банковскими, производственными, коммуникационными, бухгалтерскими и др., при этом должно быть гарантированное обеспечение правильности функционирования всех компонентов системы с целью полной реализации возложенных на нее функций.

Поскольку, практически любая информационная система, с точки зрения функциональной и технической, представляет собой многокомпонентную систему, имеет смысл выделять компоненты систем с целью возможной детализации юридической ответственности за нарушение законодательства при обработке, хранении и передачи информации каждой из этих компонент, возникающие в результате неверной работы системы, поскольку в процессе обработки информации могут возникать различного рода ошибки: ошибки сбоя, ошибки алгоритмизации, ошибки ввода и т.д. Причем, можно отметить, что определенной стадии жизненного цикла информационных систем соответствует возможность совершения характерной для данной стадии ошибки. Поскольку владельцами раздельных компонент систем могут являться различные административные подразде-

ления организации, необходимо разграничить зоны ответственности за некорректную работу тех или иных составляющих информационную систему в целом в целом. При проектировании сложных информационных систем необходимо определить границы частей информационной системы, эксплуатацию которых проводят группы субъектов с различным правовым статусом. Контроль за исполнением обязанностей и за технической составляющей работы по вводу, передаче и обработке информации необходим не только для государственных, но и для любых других информационных систем.

Примечания

1. См. Информационное право : учебник / И. Л. Бачило. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2016.

2. Амелин Р.В. Правофой режим информационных систем: Монография. – М.: ГроссМедиа, 2016. С. 138

3. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27.07.2006 (с изм. и доп.) // Российская газета. 2006. 29 июля.

4. Информационное право : учебник / И. Л. Бачило. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2016. — 437 с. С. 47 – 52.

5. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27.07.2006 (с изм. и доп.) // Российская газета. 2006. 29 июля.

6. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (утв. Приказом Ростехрегулирования от 18.12.2008 № 520-ст).

7. См ГОСТ. Анонимность – возможность совершать действия, не раскрывая идентификационных данных пользователей, псевдонимность – анонимность с сохранением подотчётности, невозможность ассоциации – анонимность с сокрытием связи между действиями одного пользователя, скрытость или ненаблюдаемость – сокрытие самого факта использования ресурса или услуги.

8. Анонимизация и деанонимизация в сети Интернет. URL: ЭР РД https://habrahabr.ru/post/137416/ (дата обр 03.02.2017).

9. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ № 646 от 05.12.2016 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

МИНБАЛЕЕВ Алексей Владимирович, профессор кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета, доктор юридических наук. Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: alexmin@bk.ru.

MINBALEEV Aleksey Vladimirovich, professor department of Theory of state and law, constitutional and administrative law of the South Ural State University (national research university). Doctor of Law. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: alexmin@bk.ru.