УДК 340.5:004.738.5(44+430+71+73)

DOI: 10.12737/jflcl.2021.010

Правовое регулирование доступа к информации пользователя сети Интернет после его смерти: сравнительно-правовое исследование

*Н. А. Данилов¹, В. В. Силкин²*¹Публичное акционерное общество «МегаФон», Москва, Россия, Nikita.Danilov@megafon.ru²Национальный исследовательский университет «Высшая школа экономики», Москва, Россия, silkinvladislav@gmail.com

Аннотация. Проблема определения единого режима предоставления информации от интернет-сервисов актуальна для современного мира, где использование сервисов в сети Интернет стало обыденным. Правила управления информацией пользователя нередко устанавливаются самими платформами, предоставляющими меньше гарантий защиты интересов пользователя после его смерти. Указанная проблема составляет один из аспектов области исследований, в социальных науках получившей название «цифровая смерть».

Цель исследования — выявление особенностей правового регулирования цифровой смерти в странах со сформировавшейся высокой правовой культурой, предложивших свое решение указанной проблемы. Сравнительно-правовой анализ законодательства США, Франции, Германии и Канады позволяет определить основные тенденции в правовом регулировании вопросов цифровой смерти и выделить два аспекта: личностный, делающий акцент на неприкосновенности данных лица и провозглашающий принцип автономии воли в отношении судьбы данных после смерти пользователя, и имущественный, рассматривающий отношения по поводу некоторой информации с точки зрения гражданского права. Имущественный аспект раскрывается в договорном направлении, где все отношения регулируются пользовательским соглашением, и внедоговорном, предполагающем, что некоторые данные могут иметь имущественную ценность, и поэтому должны учитываться как цифровые активы, включая результаты интеллектуальной деятельности в сети Интернет. Правовое регулирование цифровой смерти в России предлагается формировать не по пути наследования договорных или имущественных прав, но в рамках информационного права с предоставлением права на доступ к информации лица после смерти, не нарушая его права на неприкосновенность частной жизни и тайну переписки.

Ключевые слова: цифровая смерть, цифровое наследство, право на доступ к информации покойного, наследование исключительного авторского права, наследование в сети Интернет, коммерциализация персональных данных

Для цитирования. Данилов Н. А., Силкин В. В. Правовое регулирование доступа к информации пользователя сети Интернет после его смерти: сравнительно-правовое исследование // Журнал зарубежного законодательства и сравнительного правоведения. 2021. Т. 17. № 1. С. 86—101. DOI: 10.12737/jflcl.2021.010

Legal Regulation of Access to Information of the Internet User after His Death: Comparative Legal Research

*Nikita A. Danilov¹, Vladislav V. Silkin²*¹Public Joint Stock Company "MegaFon", Moscow, Russia, Nikita.Danilov@megafon.ru²National Research University "Higher School of Economics", Moscow, Russia, silkinvladislav@gmail.com

Abstract. The problem of defining a single mode of providing information from Internet services is relevant for the modern world, the use of services on the Internet has become ordinary. The rules for managing user information are often set by the platforms themselves, which provide fewer guarantees for protecting the user's interests after death. This problem is one of the aspects of research. In the social sciences it is called "digital death".

The purpose of the study is to identify the features of the legal regulation of "digital death" in countries with a well-established legal culture that have proposed their own solution to this problem. A comparative legal analysis of regulation in the United States, France, Germany and Canada allows us to identify the main trends. In the legal regulation of digital death, two aspects are distinguished: personal, which emphasizes the inviolability of a person's data and proclaims the principle of autonomy of will in relation to the fate of data after the death of the user, and property, which considers relations about certain information from the point of view of civil law. The property aspect is disclosed in the contractual way; all relations are regulated by the user agreement. And non-contractual, assuming that some data may have property value and therefore should be considered as digital assets, including the results of intellectual activity on the Internet. The legal regulation of digital death in Russia is proposed to be formed not along the path of inheritance of contractual or property rights, but within the framework of information law with the provision of the right to access information of a person after death, without violating his right to privacy and the secrecy of correspondence.

Keywords: digital death, digital inheritance, the right to access the information of the deceased, inheritance of exclusive copyright, inheritance on the Internet, commercialization of personal data

For citation. Danilov N. A., Silkin V. V. Legal Regulation of Access to Information of the Internet User after His Death: Comparative Legal Research. *Journal of Foreign Legislation and Comparative Law*, 2021, vol. 17, no. 1, pp. 86—101. (In Russ.) DOI: 10.12737/jflcl.2021.010

Введение. Современный человек использует множество сервисов в сети Интернет, в каждом из них он оставляет данные, размещает свои произведения или использует чужие, ведет переписку с другими пользователями. Такой объем информации в социальных науках получил название «цифровая идентичность». По мере развития оборота данных информация, размещаемая лицом в сети Интернет, приобретает коммерческую ценность: электронные денежные средства, криптовалюта, виртуальная собственность в видеоиграх, произведения, доступ к которым возможен только через определенный сервис, электронные документы коммерческой значимости. Одновременно информация может носить и личный характер, содержать переписку лица, заметки для личного пользования. Различные элементы цифровой идентичности следуют, таким образом, разным правовым режимам, вступающим в конфликт при разрешении вопроса о получении к ним доступа третьими лицами без согласия пользователя.

Пользователь не лишен правовой защиты полностью и потенциально может использовать один из существующих правовых механизмов в зависимости от характера информации. Например, при незаконном использовании его произведений пользователь может как автор воспользоваться установленными в его юрисдикции механизмами защиты авторских прав, а при сборе информации о нем из различных источников — нормами об охране частной жизни лица. При таких условиях вопрос о едином правовом режиме для аккаунта, который включает разнородные с точки зрения права элементы, еще может оставаться в тени. Он получает особое рассмотрение в ситуации, когда волеизъявление пользователя больше не может быть осуществлено, — в случае его смерти. Разнородность условий пользовательских соглашений и наличие более сильной стороны в таких соглашениях говорят о необходимости теоретического осмысления и формирования единого режима правопреемства в отношении данных лица в сети Интернет, обычно регулируемых разными правовыми режимами. Такая проблематика может быть обозначена также как «цифровая смерть» или «цифровое наследство».

Следует различать использование и доступ к цифровой идентичности после смерти ее создателя и создание новой цифровой идентичности исключительно в целях уважения к усопшему. Существуют так называемые цифровые мемориалы в память о массовых трагедиях и массовых смертях, где каждый в интерактивном режиме может почтить память погибших¹. Например, в сети Твиттер есть проект Remembrance Day в память о погибших во время

войны. Любой желающий может сделать свой твит с предлагаемыми хештегами, а затем перенести на стену своей страницы в аккаунте².

Также иногда создается отдельный аккаунт в память о конкретном погибшем человеке, где друзья и родственники могут в интерактивном режиме оставлять воспоминания и комментарии, что нередко помогает родителям и близким пережить утрату. Например, в социальной сети Фэйсбук есть цифровой мемориал некой Джэн³. Возможность создания цифрового мемориала изначально не предусматривалась социальными сетями, однако свобода заполнения профиля позволила создавать такие цифровые идентичности. Вместо создания нового цифрового мемориала близкие иногда хотят получить доступ непосредственно к профилю лица, использовавшемуся им при жизни, и переделать его в цифровой мемориал, оставив нетронутыми «следы» погибшего⁴.

Создание отдельных общественных и личных цифровых мемориалов относится к феномену цифровой смерти в широком смысле, однако с юридической точки зрения не имеет отношения к проблеме формирования единого правового режима доступа к данным лица в сети Интернет после его смерти, в связи с чем не рассматривается в данной статье.

Также в более широком контексте под цифровой смертью можно понимать и удаление пользователем при жизни аккаунта в определенном сервисе. Однако, в культурологических исследованиях цифровая смерть рассматривается в большей степени именно в отношении умершего пользователя. В рамках настоящей статьи не рассматриваются аспекты удаления личной информации пользователем при жизни, как и особенности правового режима информации об умершем в государственных информационных системах.

В России вопрос об отдельных аспектах цифровой смерти только начинает развиваться на уровне доктрины⁵, как и в доктрине иных стран, однако метод синхронного сравнения позволяет учесть приме-

² См.: Профиль Remembrance day в социальной сети Твиттер. URL: <https://twitter.com/RemembranceDay> (дата обращения: 28.04.2020).

³ См.: Цифровой мемориал Джэн в социальной сети Фэйсбук. URL: <https://ru-ru.facebook.com/jensdigitalmemorial/> (дата обращения: 28.04.2020).

⁴ См.: Brudbaker J. R. Death, Identity and the Social Network: Dissertation for the degree of Doctor of Philosophy. Irvine, 2015. 278 p.; Albrezzi F. Visiting Digital Tombstones: Unearthing Questions of Digital Personhood, Commemoration and Remembrance Processes. A thesis for the degree of Master of Arts in Culture & Performance Studies. Los Angeles, 2015. 55 p.

⁵ См., например: Горихова О. Особенности наследования исключительного авторского права // Интеллектуальная собственность. Авторское право и смежные права. 2018. № 12. С. 39—44; Панарина М. М. Наследование аккаунта в соци-

¹ См.: Herbert S. Digital Memorialization: Collective Memory, Tragedy, and Participatory Spaces. A thesis presented to the Faculty of Arts and Humanities. Denver, 2008. 125 p.

ры разрешения проблемы цифровой смерти в иных юрисдикциях и сделать обобщения, необходимые для выбора наиболее действенного механизма в национальной юрисдикции.

Для сравнения выбраны страны со сформировавшейся правовой культурой, предложившие самостоятельное правовое решение к вопросу о предоставлении доступа к аккаунту после смерти пользователя: США, Франция, Германия и Канада. Поскольку рассматриваемый вопрос находится в развитии, исследование было направлено на анализ возможных подходов к правовому регулированию цифровой смерти, что обусловило принятие во внимание не только положений, имеющих обязательную юридическую силу, но и положений рекомендательного характера (модельные акты США, Канады), актов индивидуального правоприменения (решения судов Германии).

Правовое регулирование цифровой смерти сочетает две основные группы интересов: имущественных, связанных с необходимостью обеспечения гражданского оборота отдельных элементов в составе аккаунта пользователя (например, произведения), и личных неимущественных, обращающих внимание на тесную связь личности и аккаунта. Термин «личность» в данном случае употребляется не случайно. В отличие от терминов «гражданин», «человек» термин «личность» позволяет обратить внимание на творческий аспект создания аккаунта в сети Интернет, а равно на содержание персонального характера — переписку, заметки и т. п.

Выделенные группы интересов обуславливают выделение личностного и имущественного аспектов правового регулирования цифровой смерти. Личностный аспект показывает механизмы, обеспечивающие неприкосновенность частной жизни лица после смерти при отсутствии прямого волеизъявления об обратном, в то время как имущественный аспект отражает проблему распоряжения данными, доступ к которым получен наследниками или уполномоченным лицом, а равно учитывает потенциальную коммерческую ценность таких данных. Выделяемые аспекты не взаимоисключающие, они взаимно дополняют друг друга, показывая необходимость поиска баланса личных и имущественных интересов при формировании правового регулирования цифровой смерти. Одновременно в некоторых рассматриваемых в статье правовых решениях один из аспектов может играть более значимую роль, чем другой.

Предлагаемое деление определяет и структуру настоящей статьи, рассматривающую сначала личностный, а затем имущественный аспекты правового регулирования цифровой смерти. Результаты исследования позволяют сделать вывод о возможных особенностях разрешения вопроса о цифровом насле-

довании в России, выявить сложившиеся тенденции правового регулирования рассматриваемой проблемы в зарубежных странах.

Личностный аспект цифрового наследования.

В рамках личностного аспекта акцент ставится на уважении неприкосновенности частной жизни лица и тайны переписки. Речь идет о праве наследников или уполномоченного на распоряжение имуществом наследодателя на доступ к информации покойного, содержащейся в различных сервисах сети Интернет. Право на доступ как юридическая конструкция снимает необходимость оценки различных составляющих цифровой идентичности в качестве объектов гражданских прав и направлено на обеспечение баланса между личными правами покойного и необходимостью наследников получить ту или иную информацию, например для оценки наследственной массы, при этом создавая гарантии для получения доступа и к отдельным «цифровым активам», которые могут иметь как непосредственную имущественную оценку (криптовалюта, произведения, представленные только в цифровом виде, виртуальная собственность в компьютерных играх), так и предполагаемую (переписка).

Под влиянием личностного аспекта в отличие от классических наследственных отношений, когда при отсутствии прямого волеизъявления об обратном имущество перераспределяется между наследниками соответствующей очереди, в отношении цифровой смерти принцип автономии воли становится основополагающим: наследодатель может либо распорядиться о предоставлении данных определенным лицам в полном объеме или в части, либо запретить выдачу какой-либо информации. Отсутствие прямого волеизъявления пользователя приводит либо к минимальному предоставлению необходимой информации, либо к непредоставлению информации в целом. Такой подход закреплен в правовых решениях, предлагаемых США и Францией.

Рассмотрение личностного аспекта позволяет выделить два основных проблемных вопроса: 1) при установлении принципа автономии воли необходимо уточнить, как форма распоряжения лица в отношении доступа к аккаунту может влиять на его юридическую силу, каково соотношение электронной формы и иных форм — простой письменной, нотариальной; 2) при этом важным остается вопрос о возможности распоряжения в отношении доступа ко всей размещенной в сети Интернет информации.

1. *Юридическая сила распоряжения в электронной форме.* Учитывая особенности функционирования интернет-сервисов, при формировании правового регулирования цифровой смерти невозможно отказаться от признания электронной формы распоряжения пользователем в отношении доступа третьих лиц, в том числе наследников и представителей, к его аккаунту. Особенность электронной формы распоряже-

ния состоит в выделении специальной формы в рамках принадлежащего пользователю аккаунта, заполнение которой осуществляется отдельно от принятия условий пользовательского соглашения. В таком случае, если использовать терминологию российского законодательства, распоряжение является электронным документом, подписанным простой электронной подписью. В рамках исследования не рассматривается возможность подписания электронной формы, усиленной квалифицированной электронной подписью, поскольку ее использование значительно увеличивает издержки по оставлению распоряжения.

При определении соотношения юридической силы электронного распоряжения и распоряжений в иных формах можно выделить несколько подходов, основанных на приоритете либо формы, либо времени последнего волеизъявления.

Безусловный приоритет электронной формы был предложен в США. Для оценки закрепления такого приоритета в качестве рекомендательного в модельном законодательстве США необходимо рассмотреть особенности его формирования. США пошли по пути признания автономии воли лица по распоряжению цифровыми активами после его смерти с гарантией неприкосновенности частной жизни пользователя при отсутствии обратного распоряжения и были первыми, кто реализовал личностный аспект правового регулирования цифровой смерти. На формирование подхода, избранного США, значительное влияние оказали положения Акта о хранении сообщений. Акт о хранении сообщений в составе более широкого Акта о защите права на частную жизнь в электронных сообщениях был принят Конгрессом в 1986 г.⁶ с целью обеспечения надлежащих гарантий защиты права на частную жизнь (privacy) в цифровых условиях. Акт о хранении сообщений был призван ввести дополнительные гарантии в силу сложностей применения четвертой поправки к Конституции США к отношениям в сети Интернет.

Основная проблема состояла в том, что четвертая поправка к Конституции США предоставляет защиту от несанкционированных обысков, однако в случае с перепиской в сети Интернет расширенное толкование вызывало затруднения. О. С. Керр выделил три причины сложностей применения к отношениям в сети Интернет четвертой поправки Конституции США, которые потребовали введения Акта о хранении сообщений⁷. Во-первых, не однозначно, может ли пользователь иметь разумные ожидания защиты

неприкосновенности частной жизни в отношении информации, переданной третьему лицу (поставщику интернет-услуг). Во-вторых, четвертая поправка позволяет обязать поставщика интернет-услуг предоставить необходимую информацию на основании судебной повестки (subpoena). В-третьих, четвертая поправка не распространяется на поиск информации частным лицом. Интернет-провайдер как частное лицо может самостоятельно найти необходимую информацию и передать ее государству, что не подпадает под действие четвертой поправки.

Акт о хранении сообщений, таким образом, создал правовой режим, схожий со смыслом четвертой поправки к Конституции США, вводя ограничения на возможность запроса государством у интернет-сервисов пользовательской информации, а также на возможность самостоятельного раскрытия интернет-сервисами такой информации.

Параграф 2702 Акта о хранении сообщений выделяет два вида поставщиков информационных услуг: поставщик услуг электронного сообщения и поставщик услуг удаленного вычисления.

Услуги электронного сообщения включают предоставление пользователю возможности получать или отправлять проводные или электронные сообщения⁸. Электронные сообщения определяются как любая передача полностью или в части знаков, сигналов, письменного текста, изображений, звуков, данных или интеллектуального результата иной природы (intelligence of any nature), которая осуществляется посредством проводных, радио-, электромагнитных, фотоэлектронных или фотооптических систем, влияющих на коммерческий оборот между штатами или международный коммерческий оборот. Электронные сообщения не включают сообщения по проводной связи или устно, сообщения через одностороннее устройство пейджеринга, сообщения с устройства отслеживания, а также сообщения в электронных финансовых системах⁹.

Услуги удаленного вычисления предполагают предоставление возможности хранения и обработки информации посредством системы электронных сообщений¹⁰.

Акт о хранении сообщений действует, только если интернет-сервис предоставляет услуги электронного сообщения либо удаленного вычисления любому желающему (available to the public). Если интернет-сервис используется изначально ограниченной аудиторией (например, корпоративная почта), поло-

⁶ См.: Electronic Communications Privacy Act of 1986. 18 USC 2510. Oct. 21, 1986. URL : <https://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf> (дата обращения: 28.04.2020).

⁷ См.: Kerr O. S. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It // The George Washington Law Review. 2004. Vol. 72. No. 6. P. 1208—1243.

⁸ 18 U. S. Code § 2510. Definitions (15). URL: <https://www.law.cornell.edu/uscode/text/18/2510> (дата обращения: 28.04.2020).

⁹ 18 U. S. Code § 2510. Definitions (12). URL: <https://www.law.cornell.edu/uscode/text/18/2510> (дата обращения: 28.04.2020).

¹⁰ 18 U. S. Code § 2711. Definitions for chapter (2). URL: <https://www.law.cornell.edu/uscode/text/18/2711> (дата обращения: 28.04.2020).

жения Акта о хранении сообщений не применяются и остается возможность использовать только четвертую поправку к Конституции США для защиты от доступа государства к информации пользователя.

Исходя из предложенных определений, интернет-сервис может принимать тот или иной статус по мере взаимодействия пользователя с сообщением¹¹. Когда Мари отправляет сообщение Джону, интернет-сервис является поставщиком услуг электронного сообщения. Когда Джон получил сообщение и прочитал, он может оставить его храниться в своей электронной почте. В таком случае интернет-сервис будет поставщиком услуг удаленного вычисления. Факт прочтения пользователем сообщения в практике некоторых судов не имеет значения для изменения квалификации¹².

Параграф 2701 Акта о хранении сообщений предусматривает ответственность за умышленный доступ к электронным сообщениям без разрешения либо за умышленное превышение возможностей доступа, таким образом пресекая свободу доступа к электронным сообщениям пользователя третьими лицами¹³.

Параграф 2702 Акта о хранении сообщений устанавливает запрет для профессиональных поставщиков услуг: электронного сообщения и удаленного доступа. Поставщик услуг электронного сообщения не должен раскрывать кому-либо содержание хранимых им сообщений¹⁴. Поставщик услуг удаленного вычисления не должен раскрывать кому-либо содержание сообщения, осуществляемого или поддерживаемого на сервисе, который функционирует либо в интересах пользователя, получая от него информацию посредством электронной передачи, либо если поставщик услуг не имеет права доступа к содержанию сообщений, исключительно в целях обеспечения хранения и обработки сообщений. Кроме того, оба вида поставщиков услуг не должны предоставлять кому-либо доступ к информации о пользователе (метаданным).

Таким образом, Акт о хранении сообщений установил препятствие для раскрытия интернет-сервисами содержания аккаунта третьим лицам и органам государственной власти. Именно положения Акта о хранении сообщений использовались интернет-сервисами для отказа в предоставлении доступа как наследникам, так и любым иным лицам.

Раздел (b) параграфа 2702 Акта о хранении сообщений устанавливает исключения из общего правила о запрете предоставления информации, в частности исключение (3), предусматривающее законное согласие (lawful consent) отправителя сообщения, получателя или пользователя на предоставление его третьим лицам.

Исходя из представленного исключения, возможность предоставления доступа к аккаунту третьим лицам может быть реализована только в случае, если пользователь непосредственно выразил согласие на такой доступ. Под влиянием указанных положений в США сформировался подход, устанавливающий безусловный приоритет воли пользователя при определении доступа к аккаунту. Система приоритетов норм предоставления доступа к информации покойного в сети Интернет изложена в модельном Акте США о фидуциарном доступе к цифровым активам (UFADAA)¹⁵. В настоящий момент 44 штата адаптировали UFADAA в своем законодательстве¹⁶. Акт предусматривает трехсвязную систему приоритетов:

а) если поверенный предоставляет пользователю (доверителю) возможность отдельно от общих условий использования в онлайн-режиме указать третье лицо, в пользу которого разрешается доступ либо которому дается возможность прямой связи с поверенным, а равно которому дается возможность удалить данные, акт признает юридическую силу за таким распоряжением. В случае отличия информации, содержащейся в электронном распоряжении, от распорядительных актов в бумажной форме (завещания, доверенности и т. д.) либо от общих правил пользовательского соглашения, приоритет отдается электронному распоряжению, если пользователь может самостоятельно менять данные о лице, которому разрешается доступ к цифровым активам;

б) если поверенный не предоставляет такую возможность либо если пользователь не использует такой механизм, он может непосредственно в письменном документе дать соответствующие указания. Представитель направляет запрос поверенному, предоставив официальные копии правоустанавливающих документов. Поверенный, предоставивший доступ на этом основании, освобождается от ответственности за неправомерное предоставление доступа;

¹¹ См.: *Kerr O. S. Op. cit.* P. 1216.

¹² See *Theofel v. Farey-Jones*, 359 F. 3d 106 — Court of Appeals, 9th Circuit 2004.

¹³ 18 U. S. Code § 2701. Unlawful access to stored communications. URL : <https://www.law.cornell.edu/uscode/text/18/2701> (дата обращения: 28.04.2020).

¹⁴ 18 U. S. Code § 2702. Unlawful access to stored communications. URL : <https://www.law.cornell.edu/uscode/text/18/2702> (дата обращения: 28.04.2020).

¹⁵ См.: Revised Uniform Fiduciary Access to Digital Assets Act (2015). URL: http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2015_RUFADAA_Final%20Act_2016mar8.pdf (дата обращения: 17.05.2018).

¹⁶ См.: Legislative Fact Sheet — Fiduciary Access to digital Assets Act, Revised 2015. URL: [http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20\(2015\)](http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015)) (дата обращения: 17.05.2018).

в) если пользователь не дал никаких указаний ни в письменной, ни в электронной форме, должны применяться общие условия использования; если общие условия использования не регулируют такую ситуацию, применяются положения акта.

Таким образом, подход, предложенный в UFADAA, устанавливает безусловный приоритет распоряжения аккаунтом в электронной форме. Такая система приоритетов, с одной стороны, дает неоднозначное решение в случае, когда электронное распоряжение было сделано раньше, чем распорядительный документ в бумажной форме с другим содержанием, что фактически не позволяет принять во внимание последнюю волю пользователя. Кроме того, приоритет электронной формы создает трудности в установлении личности лица, осуществившего распоряжение о доступе к аккаунту. В отличие от нотариальной формы электронная форма основывается на презумпции, что распоряжение формируется именно самим пользователем, владеющим паролем и логином и обязанным обеспечить их конфиденциальность самостоятельно. С другой стороны, безусловный приоритет электронного распоряжения минимизирует издержки по установлению и исполнению воли пользователя платформой, что способствовало его закреплению в США.

В отношении определения иерархии различных форм распоряжений возможны еще два варианта. С одной стороны, возможно установление безусловного приоритета нотариальной формы¹⁷ распоряжения. В таком случае, однако, увеличиваются издержки по составлению распоряжения. С другой стороны, и электронная, и нотариальная формы могут быть признаны равнозначными, что ставит вопрос о необходимости разрешения конфликта различных распоряжений во времени.

Временной конфликт разрешается исходя из общего представления о признании приоритета изъятия последней воли при равнозначности форм. Такому подходу, например, следует Модельный акт Канады о фидуциарном доступе к цифровым активам¹⁸, согласно которому в случае, если владелец аккаунта делал несколько распоряжений в отношении ограничения или открытия доступа фидуциара к его аккаунту, действующим признается последнее из них. Приоритет последнего изъятия воли при равнозначности форм закреплён и в российском наследственном законодательстве, которое, однако, не затрагивает вопросы получения доступа к аккаунту после смерти лица: п. 2 ст. 1130 ГК РФ предусматрива-

ет, что завещатель имеет право новым завещанием отменить предыдущее или изменить его как в части, так и полностью.

Итак, правовое регулирование цифровой смерти в случае, если оно закрепляет принцип автономии воли пользователя при установлении прав доступа третьих лиц к его аккаунту, обязательно включает и электронную форму распоряжения. В таком случае возможно установление приоритета в отношении формы тремя способами: приоритет электронной формы, приоритет нотариальной формы, равнозначность форм. В случае равнозначности форм приоритет определяется посредством установления последнего волеизъявления пользователя.

Более обоснованным с точки зрения обеспечения прав личности решением при формировании правового регулирования цифровой смерти в Российской Федерации было бы сохранение равнозначности форм волеизъявления пользователя и установление приоритета последней воли пользователя. Даже если пользователем было сделано распоряжение, например в завещании, он может изменить его посредством заполнения электронной формы в сети Интернет. Таким образом, сокращаются издержки, связанные с необходимостью нотариального оформления нотариального волеизъявления. Одновременно такой подход должен необходимо учитывать возможность несанкционированного доступа третьих лиц к аккаунту и установить процедуру признания электронного распоряжения недействительным.

2. *Объем распоряжения.* Личностный аспект раскрывается также в определении объема информации, в отношении которой может быть предоставлен доступ после смерти пользователя. Обычно лицо использует в сети Интернет различные сервисы с множеством аккаунтов, в связи с чем своевременно оставить распоряжение в каждом из них может быть проблематично. Одновременно так же сложно определить весь объем сервисов, используемых лицом при жизни.

Для проблемы множества аккаунтов в сети Интернет существуют решения в цифровой индустрии. Подход «одно лицо — одна идентичность», позволяющий получать доступ к разным аккаунтам на основании подтверждения информации из других аккаунтов, получил распространение в частном секторе, что привело к возникновению единой децентрализованной системы аутентификации — OpenID. Используя систему, лицо может пользоваться различными сайтами без необходимости регистрации на каждом из них, так как система автоматически устанавливает его данные.

Над системой работают крупные корпорации — IBM, Google, Yahoo!, Microsoft¹⁹. В отношениях вну-

¹⁷ Здесь и далее под нотариальной формой понимается также любая иная форма, отличная от электронной формы в рамках самого аккаунта, признаваемая законодательством.

¹⁸ См.: Uniform Law conference of Canada, Uniform Access to Digital Assets by Fiduciaries Act (2016). URL: https://ulcc.ca/images/stories/2016_pdf_en/2016ulcc0006.pdf (дата обращения: 28.04.2020).

¹⁹ См.: Терещенко Л. К. Модернизация информационных отношений и информационного законодательства: монография. М., 2013.

три системы существуют три субъекта. Лицо предоставляет услуги по созданию и использованию единой идентичности пользователю, и третье лицо использует информацию из OpenID²⁰. На глобальном уровне также учрежден Фонд OpenID (OIDF), который организует конференции и проводит исследования для распространения и поддержания системы²¹. В таком случае наиболее значимым становится получение доступа именно к основному аккаунту, используемому в качестве OpenID при взаимодействии с другими аккаунтами. Одновременно один пользователь может иметь не только несколько аккаунтов, но и несколько OpenID, что сохраняет проблему получения доступа лицами к ним после смерти пользователя.

Для более детального уточнения юридической связи личности пользователя и информации о нем в сети Интернет необходимо рассмотреть особенности такой связи. Связь личности пользователя и интернет-сервиса в социальных науках получила название цифровой идентичности. В контексте цифровой смерти указанная проблема может быть рассмотрена лишь частично — с позиций определения границ расширения объема информации о пользователе в сети Интернет, правовое регулирование которого в целом допустимо.

В целом можно выделить узкий и широкий подходы к пониманию цифровой идентичности в социальных науках, имеющие юридическое значение в отношении правового регулирования цифровой смерти.

В рамках узкого подхода цифровая идентичность создается в результате активной деятельности индивида с определенной целью. Например, в одном аккаунте социальной сети можно позиционировать себя как примерную домохозяйку и заботливую мать, а в аккаунте в другой социальной сети — демонстрировать свои профессиональные качества, навыки и достижения. Если посмотреть на такую интерпретацию с юридической точки зрения, можно было бы говорить о субъективном праве лица управлять своими цифровыми идентичностями так, чтобы их сосуществование не наносило вред его интересам. Ш. Теркл одной из первых начала исследовать цифровую идентичность, предполагая, что она имеет свойства множественности и децентрализованности²². Автор полагает, что индивид создает множество online personae, т. е. стремится создать множество цифровых идентичностей так, чтобы каждая из них удовлетворяла

его отдельным интересам²³. Схожий подход был также обоснован Д. Вижневским и Р. Койном в теории масок, где идентичность, подлинное лицо индивида скрывается под множеством социальных масок, в том числе создаваемых в виртуальном пространстве²⁴. Узкий подход продемонстрирован и в классификации Ф. Джорджа²⁵, согласно которому, можно выделить декларативную идентичность (*identité déclarative*) — данные, которые мы сознательно раскрываем с определенной целью. Однако есть и другие типы идентичностей: действующая идентичность (*identité agissante*), представляющая собой впечатление других людей, например, при просмотре нашей страницы в социальных сетях, а также подсчитываемая идентичность (*identité calculée*), которая характеризуется количественными показателями интерактивности, как, например, количество «лайков» и др.

В рамках широкого подхода цифровая идентичность, напротив, рассматривается как совокупность данных, относящихся к индивиду, безотносительно к созданному им аккаунту. С юридической точки зрения такой подход вызывает необходимость рассматривать субъективное право лица на контроль за данными, оставляемыми им в процессе использования сети Интернет, в том числе «контроль над использованием истории наших действий» (*régulation des usages de nos hisotriques*)²⁶. Современный французский исследователь Л. Мерзо отходит от идеи цифровой идентичности в пользу «присутствия в сети»²⁷. Она обращает внимание на «следы», оставляемые индивидом в сети вне зависимости от его воли. В данном случае цифровая идентичность формируется в результате как активной, так и пассивной деятельности, которая не направлена непосредственно на раскрытие информации.

Хотя представленные подходы приводят к рассмотрению субъективного права на контроль над информацией, их основное различие состоит в смещении акцентов. В одном случае основное внимание уделяется связи между целью создания цифровой идентич-

²³ См.: *Turkle S. Cyberspace and Identity // Contemporary Sociology. 1999. Vol. 28. No. 6. P. 643—648.*

²⁴ См.: *Wiszniewski D., Coyne R. Mask and Identity: The Hermeneutics of Self-Construction in the Information Age // Building Virtual Communities: Learning and change in cyberspace / K. A. Renninger, W. Shumar (eds.). Cambridge University Press, 2002. P. 191—214.*

²⁵ См.: *Georges F., Seilles A., Artignan G., Arnaud B., Rodriguez N. et al. Sémiotique et visualisation de l'identité numérique: une étude comparée de Facebook et Myspace. 2009. URL: <https://hal-lirmm.ccsd.cnrs.fr/hal-00410952/document> (дата обращения: 28.04.2020).*

²⁶ *Merzeau L. La présence plutôt que l'identité // Documentaliste — Sciences de l'Information, 2010. Vol. 47. No. 1. P. 33.*

²⁷ Ibid.

²⁰ См.: *Jeng Y.-L. An OpenID Based Authentication Mechanism in a Distributed System Environment // International journal of Computer and Communication Engineering. 2012. No. 3. P. 250—252.*

²¹ OpenID Foundation. URL: <http://openid.net/wg/about/> (дата обращения: 28.04.2020).

²² См.: *Turkle S. Life on the screen: Identity in the Age of the Internet. New York, 1995.*

ности и ее содержимым. Во втором случае решающее значение имеет объем информации, оставляемой нами сознательно или нет. Таким образом, цифровая идентичность как социальное явление может пониматься либо как данные, непосредственно раскрываемые лицом с целью создания определенного впечатления в сети, либо как вся совокупность данных, сознательно или случайно раскрываемых лицом в сети Интернет.

Выявленное юридическое значение цифровой идентичности как социального явления современности позволяет охарактеризовать проблему определения объема распоряжения лицом в отношении его данных в сети Интернет на случай смерти и выявить сложности реализации широкого подхода на практике.

Нормы французского права учитывают как узкий, так и широкий подход к пониманию цифровой идентичности, предлагая решение к проблеме цифровой смерти. В 2016 г. Законом о цифровой республике²⁸ внесен ряд изменений в Закон об информационных технологиях и свободах, в числе которых введена ст. 40-1²⁹, регулирующая порядок распоряжения данными лица после его смерти. Согласно данной статье лицо может оставить соответствующие распоряжения (*directives*), которые делятся на общие (*générales*), устанавливающие волю лица об использовании всей совокупности данных о нем, и специальные (*particulières*), устанавливающие волю лица на распоряжение конкретными персональными данными.

Специальные распоряжения регистрируются у соответствующего оператора информационной системы. Например, можно распорядиться своим аккаунтом посредством специальных механизмов в социальной сети. В случае если никаких распоряжений пользователем не оставлено, наследники имеют право на доступ к информации, непосредственно связанной с доступом к наследуемому имуществу, а также обратиться с требованием об удалении аккаунта из общего доступа. При этом все издержки в любом случае несет владелец социальной сети.

В то же время нормы об общих распоряжениях не получили реализацию. Согласно закону общие распоряжения могут быть зарегистрированы у доверенного лица, сертифицированного Национальной ко-

миссией информационных технологий и свобод (*la Commission nationale de l'informatique et des libertés* — CNIL), а также вносятся в реестр. Правила ведения реестра должны быть определены декретом Государственного Совета с учетом мотивированного и опубликованного мнения CNIL. Известно, что на национальном конгрессе нотариусов упоминалась необходимость делегирования таких полномочий французскому нотариату³⁰, однако ни один из подзаконных актов до сих пор не был издан уполномоченными субъектами. При отсутствии официальных комментариев по этому вопросу нормы об общих распоряжениях французским законодателем тем не менее не устраняются и, видимо, будут реализованы позднее.

Из практики применения положений об общих директивах во французском праве нельзя однозначно заключить, какие проблемные вопросы могут возникать при распоряжении в отношении доступа ко всем данным. Нотариус мог бы выступить в роли лица, осуществляющего взаимодействие в интересах умершего со всеми возможными сервисами.

Французский пример показывает сложность реализации широкого подхода к цифровой идентичности на случай смерти пользователя. Достаточно трудно определить всю совокупность сервисов, которые использовало лицо: часть сервисов или аккаунтов могли быть забыты пользователем еще при жизни. При отсутствии возможности определить все сервисы достаточно сложно установить круг ответственных лиц в части удаления информации пользователя или предоставления ее наследникам.

Реализация положения об общих распоряжениях, несомненно, потребовала бы дополнительного правового решения. С одной стороны, доверенное лицо может обратиться к любому оператору сервиса, ссылаясь на нормы об общих распоряжениях. В данном случае проблема возникает не на уровне юридического обоснования, но с точки зрения определения всех сервисов, используемых лицом при жизни. С другой стороны, можно установить учет сервисов. Такой подход позволил бы доверенному лицу исполнить волю умершего в отношении его данных без дополнительного поиска информации о нем. Введение в правовое поле реестров сервисов одновременно также достаточно проблематично, поскольку поднимает вопрос об информационной безопасности личности пользователя. В данном случае возникают дополнительные риски злоупотребления оператором реестра своими правами, утечки информации. Кроме того, потребовалось бы уточнение, может ли доверенное лицо обращаться к сервисам, в которых пользователь имел аккаунт, но не указал его в реестре.

²⁸ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&dateTexte=20180111> (дата обращения: 28.04.2020).

²⁹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL : <https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000886460&idArticle=LEGIARTI000033219717&dateTexte=20180111&categorieLien=id> (дата обращения: 28.04.2020).

³⁰ Les propositions adoptées par le 113e Congrès des notaires de France. LexisNexis. URL : <http://bit.ly/2rJQtjF> (дата обращения: 17.05.2018).

В любом из указанных случаев вся информация о пользователе в сети Интернет раскладывается на отдельные сервисы и предполагает, что пользователь предусмотрительно совершил определенные действия, чтобы распорядиться своими данными на случай смерти в каждом конкретном сервисе. Хотя практика применения норм об общих распоряжениях во Франции в дальнейшем может продемонстрировать возможность их реализации, в настоящий момент можно заключить только, что правовое регулирование цифровой смерти целесообразно рассматривать не с точки зрения управления всей информацией о лице, а с позиций взаимоотношений пользователя с каждым конкретным сервисом.

Обобщая особенности личностного аспекта правового регулирования цифровой смерти, можно сделать вывод, что уважение интересов личности пользователя интернет-сервисов устанавливает определенные ограничения доступа для наследников в зависимости от воли умершего. Наследники получают доступ к данным такого лица, только если наследодатель непосредственно выразил на это свою волю. В противном случае наследники имеют право только на ту информацию, которая необходима для имущественной оценки наследственной массы. Личностный аспект правового регулирования цифровой смерти получил наиболее яркое выражение в США и во Франции. Одновременно рассмотрение личностного аспекта раскрывает также проблему определения юридической силы распоряжения пользователем в отношении его данных в электронной форме, особенности установления объема такого распоряжения. Пример Франции показывает, что в настоящее время существуют сложности для пользователя выразить волю о распоряжении всеми данными о нем в сети Интернет на случай смерти.

При формировании правового регулирования цифровой смерти в России целесообразно учитывать выявленную трудность и исходить из необходимости выражения воли пользователем в отношении каждого сервиса. Такой подход позволит сократить издержки поиска информации о пользователе, одновременно обеспечив ему возможность самостоятельно выбрать наиболее значимые для него сервисы.

Личностный аспект не нивелирует возможную имущественную ценность данных, содержащихся в аккаунте пользователя после его смерти. Имущественный аспект в условиях развития оборота данных и переосмысления коммерческой ценности информации неизбежен для правового регулирования цифровой смерти.

Имущественный аспект цифрового наследования. В рамках имущественного аспекта правового регулирования цифровой смерти права на отдельные элементы аккаунта либо на аккаунт в целом рассматриваются с точки зрения имущественного оборота. В рамках имущественного аспекта большую

значимость приобретает не правовой механизм, посредством которого пользователь оставляет распоряжение, но правовой механизм получения доступа наследниками или представителями к содержанию аккаунта. В зависимости от природы такого имущественного права можно выделить два направления: договорное и внедоговорное.

1. *Аккаунт как договорное обязательство.* Договорное направление является основным для правового регулирования цифровой смерти в таких правовых системах, где не существует специальных норм, регулирующих ее. Все возможности пользователя по управлению цифровой идентичностью описываются в пользовательском соглашении. Таким образом, право пользователя на распоряжение информацией и доступ к ней реализуется как право требования к интернет-сервису в рамках пользовательского соглашения.

Нередко договорное направление правового регулирования цифровой смерти не предоставляет возможности пользователю распорядиться своими данными после смерти. В большинстве стран основным препятствием получения доступа к цифровым данным родственниками после смерти лица выступило исключительно договорное регулирование отношений между пользователем и платформой. Социальные сети отказывались предоставлять какой-либо доступ к странице умершего, ссылаясь на политику использования сервиса, и блокировали профиль либо ставили отметку о смерти лица.

В Российской Федерации, например, из-за отсутствия специальных норм о цифровой смерти каждый интернет-сервис самостоятельно в пользовательском соглашении определяет порядок использования данных покойного. Каждый сервис, таким образом, получает возможность установить условия цифровой смерти в соответствии со своим функционалом и своей политикой. Ряд сервисов идет по пути регулирования, предложенному UFADAA в США. Facebook предоставляет возможность назначить хранителя на случай смерти и в любом случае переводит аккаунт в памятный статус при уведомлении о смерти лица. При этом не исключается возможность обоснованного запроса на предоставление значимой информации по решению суда от уполномоченных лиц. Пользователь может также распорядиться об удалении аккаунта в случае смерти³¹. Google также предоставляет возможность распорядиться информацией на случай смерти с помощью сервиса «На всякий случай»: закрыть доступ к аккаунту или предоставить данные по запросу на определенных условиях³². Некоторые

³¹ См.: Правила использования Facebook. URL: <https://www.facebook.com/help/1506822589577997?ref=tos> (дата обращения: 28.04.2020).

³² См.: Правила использования Google. URL: <https://support.google.com/accounts/troubleshooter/6357590?hl=ru> (дата обращения: 28.04.2020).

сервисы предоставляют более ограниченный набор действий, не давая возможности пользователю распорядиться о раскрытии информации самостоятельно. Instagram по запросу уполномоченных лиц может удалить аккаунт либо перевести его в памятный статус³³. ВКонтakte по предоставлении свидетельства о смерти от уполномоченного лица может заблокировать аккаунт или ограничить к нему доступ³⁴.

Одновременно возможность наследования прав из пользовательского соглашения и включения их в наследственную массу, опираясь на личную связь между пользователем и платформой, обычно отвергалась. Федеральный верховный суд Германии 12 июля 2018 г. по делу о возможности предоставления доступа наследникам — родителям несовершеннолетней девочки, покончившей жизнь самоубийством, — к ее аккаунту в сети Фейсбук утвердил правовую позицию, значительно меняющую подход к наследованию прав из пользовательского соглашения³⁵. Немецкие суды сделали акцент на договорной природе существования аккаунта в социальных сетях и заключили, что в порядке универсального правопреемства переходят права требования по пользовательскому соглашению с Фейсбук. Суды отклонили возражения ответчика о необходимости защиты тайны частной жизни девочки и тайны ее переписки, был также отвергнут довод о тайне связи. Со стороны истца приводилась интересная аналогия: личный дневник как вещь входит в состав наследственной массы и передается наследникам, несмотря на интимность его содержания. Такой подход, оправданный решением в конкретном деле, ставит под вопрос наследование договоров с огромным количеством субъектов интернет-пространства и абсолютно игнорирует личностный аспект правового регулирования цифровой смерти.

Решение Федерального верховного суда Германии, постулируя наследование аккаунта как договорного обязательства, сохраняет возможность для интернет-сервиса предусмотреть формулировки в пользовательском соглашении, которые бы позволяли ему отказаться от договора в случае смерти пользователя, и ставит два вопроса: о возможности действия наследника или представителя от имени и в интересах покойного при получении доступа к аккаунту и о юридической силе ограничительных формулировок пользовательского соглашения. В данном случае особый интерес для сравнения представляет реше-

ние Апелляционного суда штата Массачусетс США по делу “Ajemian v. Yahoo!, Inc.”³⁶.

В августе 2006 г. Джон Аджемиян погиб в аварии на мотоцикле, не оставив завещания. После его смерти остался аккаунт электронной почты Yahoo!. Покойный не оставил никаких распоряжений в отношении аккаунта. Впоследствии Роберт и Мариан Аджемиян были назначены личными представителями наследственной массы брата и обратились к сервису за предоставлением доступа к содержанию аккаунта. Роберт утверждал, что создал аккаунт для Джона самостоятельно в 2002 г. и периодически также пользовался им, но со временем забыл пароль. Yahoo! отказался предоставлять доступ, ссылаясь на положения Акта о хранении сообщений, а также самих Правил использования сервиса, из толкования которых Yahoo! утверждал, что может отказать личному представителю в доступе. Аккаунт Yahoo! также указал, что может предоставить информацию о пользователе (метаданные, которые включают общую информацию о пользователе, данные об отправителе и получателях сообщений и времени их отправления), если запрос об их предоставлении будет получен в судебном порядке. Роберт и Мариан позже получили информацию о пользователе на основании судебного решения.

В сентябре 2009 г. Роберт и Мариан подали в Суд по наследственным и семейным делам, заявляя, что аккаунт является частью наследственной массы покойного, в связи с чем они имеют право на полный доступ к аккаунту пользователя и требуют предоставить такой доступ.

Суд первой инстанции поддержал позицию Yahoo!, указав на применение положений Акта о хранении сообщений, запрещающих раскрытие информации третьим лицам, после чего истцом была подана апелляционная жалоба.

Суд апелляционной инстанции рассудил, что Акт о хранении сообщений не препятствует раскрытию содержания аккаунта личным представителям. Наоборот, он позволяет Yahoo! раскрыть аккаунт, так как личные представители предоставляют законное согласие (lawfully consent) на доступ от имени покойного.

Доводы об отнесении аккаунта к имущественной массе покойного (property) не оспаривались сторонами и не получили рассмотрения в судебном решении.

Раздел (b) параграфа 2702 Акта о хранении сообщений устанавливает исключения из общего правила о запрете предоставления информации³⁷. В деле

³³ См.: Правила использования Instagram. URL: <https://help.instagram.com/264154560391256?helpref=related&ref=related> (дата обращения: 28.04.2020).

³⁴ См.: Ответ от технической поддержки ВКонтakte. URL: https://vk.com/topic-22582448_24812401 (дата обращения: 10.01.2018).

³⁵ BGH, 12.07.2018 — III ZR 183/17 // ECLI:DE:BGH:2018:120718UIIIZR183.17.0.

³⁶ Ajemian v. Yahoo!, Inc., 2017. URL: <https://www.mass.gov/files/documents/2017/10/16/12237.pdf> (дата обращения: 28.04.2020).

³⁷ 18 U. S. Code § 2702. Unlawful access to stored communications. URL: <https://www.law.cornell.edu/uscode/text/18/2702> (дата обращения: 28.04.2020).

“*Ajemian v. Yahoo!*” были рассмотрены исключение (1), позволяющее передавать информацию адресату или предполагаемому получателю либо его агенту, а также исключение (3), предусматривающее законное согласие (*lawful consent*) отправителя сообщения, получателя или пользователя на предоставление его третьим лицам.

Личные представители ссылались на исключение (1) раздела (b) параграфа 2702 Акта о хранении сообщений, утверждая, что действуют как агенты покойного. Суд апелляционной инстанции отметил, что агент по определению действует в интересах и под контролем принципала. Напротив, личные представители были назначены не покойным, а судом по наследственным и семейным делам, в связи с чем они действовали под контролем суда по наследственным и семейным делам, но не покойного, и не могут быть признаны агентами.

Одновременно личные представители ссылались также на исключение (3) раздела (b) параграфа 2702 Акта о хранении сообщений, заявляя, что предоставляют законное согласие на раскрытие информации от имени покойного пользователя. Yahoo! возражал, что указанное исключение относится только к согласию, непосредственно выраженному живым пользователем (*actual consent*). Суд апелляционной инстанции отверг довод Yahoo!, пояснив, что сужение толкования только до согласия, выраженного непосредственно живым лицом, лишит личных представителей права получить доступ к электронным сообщениям и создаст специальный режим по отношению к общим положениям наследственного и семейного права штата. Хотя Акт о хранении сообщений не дает определения законного согласия, Суд установил, что под ним подразумевается согласие, разрешенное законом (*permitted by law*), но не непосредственное согласие живого лица. В связи с изложенным Суд апелляционной инстанции указал, что личные представители могут предоставить законное согласие от имени покойного на раскрытие сообщения из его аккаунта. В решении суда однако не содержалась обязанность для Yahoo! раскрыть содержание сообщений, но подчеркивалось, что Акт о хранении сообщений не создает препятствий для такого раскрытия.

В отношении аргумента Yahoo!, что в силу принятого покойным пользовательского соглашения аккаунт мог отказаться предоставить запрашиваемую информацию, Суд апелляционной инстанции отметил, что Суд по наследственным и семейным делам не смог установить, является ли указанное пользовательское соглашение имеющим силу, так как Yahoo! не предоставил доказательств достижения согласия сторонами в отношении пользовательского соглашения, в том числе получения условий пользовательского соглашения и их принятия покойным. В связи с этим Суд апелляционной инстанции признал правомочным отказ Суда по наследственным и се-

мейным делам принимать доводы Yahoo! о пользовательском соглашении и вернул дело в Суд по наследственным и семейным делам для рассмотрения указанных обстоятельств.

Одновременно в особом мнении судьи Гантс к решению Суда апелляционной инстанции указывалось, что, аргументируя возможность отказать личному представителю в доступе к аккаунту, Yahoo! ссылается на пункт пользовательского соглашения, который оставляет за организацией право в любой момент по своему усмотрению удалить аккаунт пользователя. Судья Гантс отмечал, что если бы пользовательское соглашение было признано имеющим силу, в рассматриваемом деле Yahoo! не удаляло аккаунт до обращения личных представителей о получении доступа. Если бы при подаче личным представителем иска о получении доступа к аккаунту организация удалила аккаунт, ее действия нарушили бы правило о запрете уничтожения доказательств. Судья подчеркивал, что возвращение дела в Суд по наследственным и семейным делам в данном случае только создает дополнительные судебные расходы со стороны личных представителей, так как в любом случае, поскольку дело рассматривается в суде, Yahoo! уже не может реализовать право на удаление аккаунта, предусмотренное пользовательским соглашением.

В рассмотренном судебном решении аналогично решению Федерального верховного суда Германии поднимался вопрос о возможности осуществления наследником или уполномоченным представителем покойного прав на основании пользовательского соглашения от имени покойного владельца аккаунта. Хотя такой подход позволяет предоставить наследнику доступ к аккаунту покойного, он во многом отходит от личностного аспекта цифровой смерти.

При формировании правового регулирования цифровой смерти в Российской Федерации следует учитывать, что возможность наследования в порядке универсального правопреемства прав из пользовательского соглашения может быть ограничена фидуциарным характером отношений пользователя и интернет-сервиса. В силу ч. 2 ст. 1112 ГК РФ в наследственную массу не входят права и обязанности, неразрывно связанные с личностью покойного. В данном случае значение могут иметь характер и функционал аккаунта. Особенно спорными в связи с этим являются аккаунты социальных сетей, которые пользователь создает и ведет в соответствии со своим видением.

Одновременно изменения, внесенные в гражданское законодательство Федеральным законом от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», способствуют возможности признания пользовательского соглашения сделкой, заключенной в письменной форме по российскому праву. Согласно абз. 2 п. 1

ст. 160 ГК РФ в новой редакции письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Поскольку в настоящий момент многие интернет-сервисы используют номер телефона для подтверждения регистрации при создании аккаунта, его использование может рассматриваться как способ, позволяющий определить регистрирующегося пользователя.

Таким образом, договорное направление правового регулирования цифровой смерти на основании пользовательского соглашения является основным в том случае, если национальное законодательство не устанавливает специальных правовых положений. Одновременно в рамках договорного направления остается спорным вопрос о возможности наследования прав и обязанностей пользователя из пользовательского соглашения как договора, а также о возможном фидуциарном характере отношений пользователя и интернет-сервиса.

2. *Аккаунт как самостоятельный вид имущества.* В противовес договорному направлению правовая доктрина некоторых стран идет по пути обоснования имущественных прав лица на информацию в сети Интернет, действующих непосредственно, а не только на основании пользовательского соглашения. Внедоговорное направление обращает внимание на имущественную ценность данных лица в сети Интернет, в том числе объектов интеллектуальной собственности, сообщений, и вводит понятие «цифровой актив».

В США некоторые исследователи высказывались о праве лица на контроль над аккаунтом в сети Интернет, приравнивая его к блоку имущественных прав³⁸. Отмечалось, что информация с аккаунта имеет определенную ценность, в том числе коммерческую, если, например, через социальную сеть распространялись фотографии, видеозаписи, попадающие под охрану интеллектуальной собственности, и договорный режим регулирования не позволяет защитить остающиеся после смерти лица активы, которые должны находиться в наследственной массе. Модельный акт о фидуциарном доступе к цифровым активам США также вводит понятие цифрового актива. Акт позволил фидуциару (уполномоченному на распоряжение имуществом) управлять, помимо традиционных имущественных прав, цифровыми активами, в том числе электронными документами, криптовалютой, а также ограничил доступ фидуциара к электронной

переписке и социальным сетям лица, если только такое лицо прямо не выразило согласие на этот доступ. Цель принятия акта — позволить фидуциару, распоряжающемуся имуществом умершего, также иметь доступ к его цифровым активам, однако сохранить в безопасности более чувствительную информацию о частной жизни лица, если такое лицо не дало непосредственного согласия на доступ к своим данным.

Сфера действия акта ограничивается только цифровыми активами. Под цифровым активом понимаются электронные записи (electronic records), которые принадлежат лицу на праве собственности или затрагивают права и законные интересы лица. Цифровыми могут быть активы, существующие только в электронной форме. Формулировка определения призвана исключить другие виды активов, как, например, содержимое банковского счета, распоряжение которым возможно в режиме онлайн. Определение относится к любой информации, хранящейся в электронной форме, в том числе на персональном компьютере, ином устройстве, на сайте в сети Интернет, а также к виртуальной собственности.

Акт устанавливает различия между цифровыми активами лица. Так, выделяется содержание электронных сообщений, которое включает тему сообщения и его содержание, текстовые сообщения, иные сообщения между частными лицами. Фидуциар в любом случае не может получить доступ к содержанию сообщений, за исключением наличия прямо и непосредственно выраженного согласия лица. Однако фидуциар может получить доступ к каталогу электронных коммуникаций (метаданные: список адресов отправителей и получателей, дата и время отправления сообщений). Такие действия необходимы, например, для проведения поиска активов умершего лица. Если фидуциар находит в контактах банк, он посылает ему запрос о наличии отношений с умершим.

США пошли по пути урегулирования именно имущественных отношений с сохранением конфиденциальности личной информации умершего при отсутствии его воли на раскрытие такой информации. Фактически для цифровых активов лица был создан специальный правовой режим, приближенный к правовому режиму управления имуществом³⁹. Этим обуславливается субъектный состав регулируемых актов отношений. В рамках охватываемых им отношений можно выделить фидуциара, доверителя и поверенного (custodian). При этом поверенным является хранитель информации, т. е. социальная сеть, оператор системы электронной почты и проч. Правомочия

³⁸ См.: Kutler N. Protecting Your Online You: A New Approach to Handling Your Online Persona After Death // Berkley Technology Law Journal. 2011. Vol. 26. No. 4. P. 1641—1670.

³⁹ См.: A summary on the Uniform Fiduciary Access to Digital Assets Act, 2016. URL: <http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/Revised%20UFADAA%20-%20Summary%20-%20March%202016.pdf> (дата обращения: 17.05.2018).

в отношении поверенного согласно акту могут возникать только у лица, являющегося резидентом США либо являвшегося таковым на момент смерти. Акт также не распространяется на использование работником цифровых активов работодателя. Например, в случае если работник имел корпоративную почту, фидуциар не может запросить у работодателя доступ к такой почте, так как отсутствует главный признак поверенного — наличие аккаунта. Под аккаунтом понимается договоренность в соответствии с пользовательским соглашением, на основании которой поверенный осуществляет обработку цифровых активов лица либо предоставляет электронные услуги, товары в электронной форме.

В модельном Акте Канады о фидуциарном доступе к цифровым активам сохранены некоторые положения модельного акта США, однако установлен прямо противоположный с точки зрения принципа автономии воли американскому подход⁴⁰.

Акт Канады, как и американский, распространяет действие на четыре вида фидуциаров: личного представителя, попечителя, юриста по доверенности (attorney), доверительного управляющего (trustee).

Фидуциар имеет право получить доступ к цифровым активам владельца аккаунта при условии, что его полномочия возникли на правовом основании, а также если владелец аккаунта не запретил доступ к своему аккаунту. Право фидуциара на доступ может возникать на основании завещания покойного владельца аккаунта, распоряжения органа по наследству, если это предусмотрено законодательством, а также решения о попечительстве, доверенности, траста, решения суда. Владелец аккаунта может ограничить доступ фидуциара к своему аккаунту после вступления Акта Канады о фидуциарном доступе к цифровым активам в силу, выразив свое намерение в порядке, отдельном от принятия общих условий использования. В случае если владелец аккаунта делал несколько распоряжений в отношении ограничения или открытия доступа фидуциара к его аккаунту, действующим признается последнее из них.

Фидуциар, который по положениям Акта имеет право доступа к аккаунту, может совершать любые действия в отношении цифрового актива, как если бы они осуществлялись владельцем аккаунта при жизни и в полной сознательности, считается имеющим согласие от владельца аккаунта на доступ к цифровому активу, а также считается авторизованным пользователем цифрового актива. Любые положения пользовательского соглашения, ограничивающие право фидуциара на доступ к цифровым активам, считаются ничтожными, вне зависимости от выбора применимого

права. Использование фидуциаром аккаунта и цифровых активов не может считаться нарушением пользовательского соглашения и не должно быть обусловлено получением согласия от какого-либо третьего лица. Если в распоряжении фидуциара находится материальный носитель, с помощью которого возможны хранение, получение, обработка или передача цифрового актива, фидуциар может беспрепятственно получать доступ к любому цифровому активу, доступному с помощью такого материального носителя, и считается его авторизованным пользователем.

Интернет-сервис, который соблюдает положения Акта, освобождается от ответственности за любое действие или бездействие, за исключением случаев недобросовестности.

Канадский исследователь Ф. Л. Вудман выделяет три основных отличия между американским и канадским модельными актами о фидуциарном доступе к цифровым активам⁴¹. Во-первых, канадский акт следует подходу разрешения доступа фидуциару по общему правилу в отличие от США, где введение схожих положений невозможно в силу действия Акта о хранении сообщений. Во-вторых, канадский акт не предоставляет распоряжениям владельца аккаунта в онлайн-форме большую юридическую силу, чем соглашение, выраженному в иных источниках. В-третьих, согласно положениям канадского акта пользовательское соглашение не может ограничивать прав фидуциара, в то время как американский акт дает пользовательскому соглашению определять доступ фидуциара, если владелец аккаунта не даст распоряжений.

Модельные акты о фидуциарном доступе к цифровым активам Канады и США не содержат специальных положений, разъяснявших наличие у фидуциара права уничтожить цифровой актив или аккаунт. В таком случае возможность уничтожения аккаунта зависит от объема полномочий, которыми обладает фидуциар в отношении имущества.

Модельный акт в Канаде, как и в США, не имеет юридической силы и выступает только в качестве предложения провинциям Канады или штатам США принять соответствующие акты. Одновременно модельный акт Канады не был принят ни одной из провинций и поэтому может рассматриваться только как предлагаемое правовое решение.

При отсутствии специальных норм об отнесении аккаунта в интернет-сервисе к имуществу может быть применено широкое толкование понятия «имущество». Законодательство некоторых провинций Канады, например, позволяет обеспечить личных представителей правом доступа к онлайн-аккаунту в силу широкого

⁴⁰ См.: Uniform Law conference of Canada, Uniform Access to Digital Assets by Fiduciaries Act (2016). URL: https://ulcc.ca/images/stories/2016_pdf_en/2016ulcc0006.pdf (дата обращения: 28.04.2020).

⁴¹ См.: Woodman F. L. Fiduciary Access to Digital Assets: A Review of the Uniform Law Conference of Canada's Proposed Uniform Act and Comparable American Model Legislation // Canadian Journal of Law and Technology. 2017. Vol. 15. No. 2. P. 226—227.

толкования законодательства. На основании ст. 20 (1) акта Альберты об управлении имуществом⁴² личный представитель может приобретать во владение и контроль любое имущество, делать с ним все, что покойный мог делать при жизни и в сознательном состоянии, осуществлять любые действия в отношении имущества, которые необходимы для реализации полномочий личного представителя. Аналогично на основании ст. 142 Акта Британской Колумбии о завещаниях, имуществе и наследовании личный представитель обладает всеми полномочиями в отношении имущества, которыми мог обладать покойный при жизни, если иное не указано в законе или завещании⁴³. Существующие положения законодательства Альберты и Британской Колумбии, а также широкое толкование понятия «имущество» позволяют только одному виду фидуциаров — личным представителям — получить доступ к аккаунту после смерти лица⁴⁴.

Итак, признание аккаунта и его содержания самостоятельным объектом имущества возможно либо в силу введения специальных положений в законодательство, либо в силу расширения толкования понятия «имущество».

Имущественный аспект цифровой смерти связан не только с возможностью признания аккаунта имуществом, но и с возможным приданием имущественной оценки персональным данным лица. Предмет исследования настоящей статьи не позволяет в полной мере охватить проблему коммерциализации персональных данных, однако упоминание о такой возможности уместно в той мере, в какой оно отражает рассматриваемый имущественный подход. Персональные данные в случае разрешения вопроса об их коммерциализации также могли бы рассматриваться как цифровые активы. Поскольку факт использования интернет-сервисами данных в коммерческих целях не оставляет сомнения, выдвигаются предложения о признании имущественной ценности за данными, раскрываемыми лицом, в том числе за персональными данными. Согласно проводимым социальным опросам созданию среды доверия между пользователями и цифровыми сервисами способствует закрепление возможности за пользователем сервиса осуществлять контроль за данными⁴⁵. Переданные данные могут получить определенное денежное выражение

в зависимости от того, насколько они полезны. Исходя из этого положения любая услуга в Интернете, полагаемая «бесплатной», в действительности оказывается за передачу данных как встречное представление. Однако такая же ситуация наблюдается и в сфере платных интернет-услуг. В таких условиях обоснованным становится использование моделей активного выбора, предоставляющих возможность заплатить либо деньгами, либо данными⁴⁶.

Отождествление права на защиту персональных данных и имущественного права тем не менее исключает возможность обеспечения надлежащей защиты нематериальных интересов и прав личности. Единая правовая судьба персональных данных скорее должна найти свою реализацию в праве на доступ и управление такими данными. В праве Европейского Союза, например, также наблюдается тенденция к закреплению права на персональные данные, в первую очередь как права осуществлять над ними контроль, что нашло проявление в *data portability* (право на переносимость данных), введенное в Общий Регламент ЕС о защите персональных данных (GDPR)⁴⁷. Право на переносимость данных предполагает создание возможности для любого субъекта персональных данных запросить у оператора персональные данные, обрабатываемые им, получить их в доступном формате, а также дать распоряжение о направлении таких данных другому оператору. Право на переносимость данных получило широкое освещение в исследовательской литературе еще до вступления Регламента в силу⁴⁸.

Хотя внедоговорное направление правового регулирования цифровой смерти в силу сближения с уже знакомым механизмом оборота имущественных прав видится удобным, сложно говорить о возможности создания единого механизма управления информацией разной коммерческой ценности после смерти пользователя. Кроме того, информация, не имеющая коммерческой ценности сама по себе, но обладающая некоторой личной ценностью (переписка с определенным лицом, памятные фотографии и т. п.), остается неохваченной и вопрос о ее оценке может быть достаточно сложным.

⁴⁶ См.: *Malgieri G., Custers B.* Pricing Privacy — the Right to Know the Value of your Personal Data // *Computer Law and Security Review*. 2018. Vol. 34. Iss. 2. P. 289—303.

⁴⁷ *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)* // *Official Journal of the European Union*. L 119, 2016. 4 May. Vol. 59. P. 1—88.

⁴⁸ См.: *Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I.* The Right to Data Portability in the GDPR : Towards User-Centric Interoperability of Digital Services // *Computer Law and Security Review*. 2018. Vol. 34. Iss. 2. P. 193—203.

⁴² См.: Canada, Province of Alberta, *Estate Administration Act*, 2014. URL: <http://www.qp.alberta.ca/documents/Acts/el2p5.pdf> (дата обращения: 28.04.2020).

⁴³ См.: Canada, Province of British Columbia, *Wills, Estate and Succession Act*, 2009. URL: http://www.bclaws.ca/civix/document/id/complete/statreg/09013_01/#section142 (дата обращения: 28.04.2020).

⁴⁴ См.: *Woodman F. L.* Op. cit. P. 193—227.

⁴⁵ См.: *Prince C.* Do Consumers Want to Control their Personal Data? Empirical Evidence // *International Journal of Human-Computer Studies*. 2018. Vol. 110. P. 21—32.

Вопрос о правовом признании цифровых активов одновременно ставит под угрозу личностные аспекты правового регулирования цифровой смерти. Кроме того, само понятие цифрового актива может определяться в разном объеме. Проблемы коммерциализации персональных данных и выделения цифровых активов в качестве самостоятельных объектов гражданских прав характеризуют возможные направления развития рассматриваемого имущественного внедоговорного подхода к правовому регулированию цифровой смерти, однако требуют дополнительного уточнения с точки зрения цивилистики.

Более правильным юридическим решением в случае смерти пользователя было бы создание права доступа наследников к аккаунту в рамках информационного законодательства, что позволит обеспечить наследникам доступ к содержанию аккаунта, оставив за скобками особенности определения границ термина «цифровой актив». Информационно-правовой подход обладает рядом преимуществ. Во-первых, он способствует развитию отраслевых механизмов информационного права, теоретические особенности которого в большей мере получили развитие в российской правовой доктрине. Во-вторых, выделение доступа к информации пользователя в сети Интернет после его смерти в информационном праве позволит также в дальнейшем включить в рассмотрение проблемы цифровой смерти особенности реализации пользователем при жизни права на удаление всей информации из аккаунта, охарактеризовать правовой режим информации об умершем, сохранившейся в государственных информационных системах.

Итак, имущественный аспект правового регулирования цифровой смерти может реализовываться посредством развития договорного направления, поднимающего вопрос о возможности наследования прав и обязанностей из пользовательского соглашения как договора, либо внедоговорного, приравнивающего аккаунт и его содержание к определенному имуществу покойного пользователя. Одновременно формирование правового регулирования цифровой смерти с уклоном в имущественный аспект нивелирует личностный характер отношений пользователя и интернет-сервиса, снижая гарантии защиты его интересов после смерти.

Список литературы

- Albrezzi F. Visiting Digital Tombstones: Unearthing Questions of Digital Personhood, Commemoration and Remembrance Processes. A thesis for the degree of Master of Arts in Culture & Performance Studies. Los Angeles, 2015. 55 p.
- Brudbaker J. R. Death, Identity and the Social Network: Dissertation for the degree of Doctor of Philosophy. Irvine, 2015. 278 p.
- Georges F., Seilles A., Artignan G., Arnaud B., Rodriguez N. et al. Sémiotique et visualisation de l'identité numérique: une étude comparée de Facebook et Myspace. 2009. URL: <https://hal-lirmm.ccsd.cnrs.fr/hal-00410952/document> (дата обращения: 28.04.2020).
- Herbert S. Digital Memorialization: Collective Memory, Tragedy, and Participatory Spaces. A thesis presented to the Faculty of Arts and Humanities. Denver, 2008. 125 p.
- Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I. The Right to Data Portability in the GDPR : Towards User-Centric Interoperability of Digital Services // Computer Law and Security Review. 2018. Vol. 34. Iss. 2.
- Jeng Y.-L. An OpenID Based Authentication Mechanism in a Distributed System Environment // International journal of Computer and Communication Engineering. 2012. No. 3.

Заключение. На основе предложенной классификации отдельных аспектов правового регулирования цифровой смерти можно выделить его тенденции в отдельных странах. Так, США и Франция более склонны к соблюдению личных прав умершего и предоставляют последнему возможность самостоятельным волеизъявлением при жизни определить степень доступности его данных третьим лицам на случай смерти. При этом право наследников на доступ к данным, имеющим имущественную ценность, в достаточной степени остается ограниченным волей самого пользователя. Германия и Канада предлагают правовые решения, в большей мере учитывающие интересы наследников и иных лиц, управляющих имуществом умершего, не уделяя особого внимания автономии воли пользователя.

Правовое регулирование цифровой смерти, т. е. предоставления права доступа к информации покойного в сети Интернет наряду с правом управления такой информацией, может идти либо по пути создания системы приоритетов с предоставлением субъекту права непосредственно выразить волю на раскрытие информации, либо по исключительно имущественному пути, что ставит под угрозу правовые режимы тайн, обычно существующие в отношении действий лица в Интернете. На наш взгляд, на уровне правового регулирования следует в первую очередь говорить о предоставлении права доступа к информации покойного в Интернете, включая право на управление такой информацией при наличии оснований, строго указанных в федеральном законе, а не о наследовании прав и обязательств по пользовательским соглашениям. Установление единого правового режима доступа к информации на случай смерти пользователя — первый шаг на пути к формированию более широкого института цифровой смерти в информационном праве, охватывающего не только особенности координационных правовых отношений на случай смерти пользователя, рассмотренные в настоящей статье, но учитывающего также правовой режим данных пользователя в государственных информационных системах на случай смерти, особенности удаления пользователем информации о себе при жизни.

- Kerr O. S. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It // *The George Washington Law Review*. 2004. Vol. 72. No. 6.
- Kutler N. Protecting Your Online You: A New Approach to Handling Your Online Persona After Death // *Berkley Technology Law Journal*. 2011. Vol. 26. No. 4.
- Malgieri G., Custers B. Pricing Privacy — the Right to Know the Value of your Personal Data // *Computer Law and Security Review*. 2018. Vol. 34. Iss. 2.
- Merzeau L. La présence plutôt que l'identité // *Documentaliste — Sciences de l'Information*, 2010. Vol. 47. No. 1.
- Prince C. Do Consumers Want to Control their Personal Data? Empirical Evidence // *International Journal of Human-Computer Studies*. 2018. Vol. 110.
- Turkle S. Cyberspace and Identity // *Contemporary Sociology*. 1999. Vol. 28. No. 6.
- Turkle S. *Life on the screen: Identity in the Age of the Internet*. New York, 1995.
- Wiszniewski D., Coyne R. Mask and Identity: The Hermeneutics of Self-Construction in the Information Age // *Building Virtual Communities: Learning and change in cyberspace* / K. A. Renninger, W. Shumar (eds.). Cambridge University Press, 2002.
- Woodman F. L. Fiduciary Access to Digital Assets: A Review of the Uniform Law Conference of Canada's Proposed Uniform Act and Comparable American Model Legislation // *Canadian Journal of Law and Technology*. 2017. Vol. 15. No. 2.
- Горохова О. Особенности наследования исключительного авторского права // *Интеллектуальная собственность. Авторское право и смежные права*. 2018. № 12.
- Панарина М. М. Наследование аккаунта в социальных сетях и вопросы цифрового наследования: правовое исследование // *Наследственное право*. 2018. № 3.
- Терещенко Л. К. Модернизация информационных отношений и информационного законодательства: монография. М., 2013.

References

- Albrezzi F. Visiting Digital Tombstones: Unearthing Questions of Digital Personhood, Commemoration and Remembrance Processes. A thesis for the degree of Master of Arts in Culture & Performance Studies. Los Angeles, 2015. 55 p.
- Brudbaker J. R. Death, Identity and the Social Network: Dissertation for the degree of Doctor of Philosophy. Irvine, 2015. 278 p.
- Georges F., Seilles A., Artignan G., Arnaud B., Rodriguez N. et al. Sémiotique et visualisation de l'identité numérique: une étude comparée de Facebook et Myspace, 2009. Pp. 1—13. Available at: <https://hal-lirmm.ccsd.cnrs.fr/hal-00410952/document> (accessed 28.04.2020).
- Gorokhova O. Specifics of Exclusive Copyright Inheritance. *Intellektual'naya sobstvennost'. Avtorskoe pravo i smezhnye prava*, 2018, no. 12, pp. 39—44. (In Russ.)
- Herbert S. Digital Memorialization: Collective Memory, Tragedy, and Participatory Spaces. A thesis presented to the Faculty of Arts and Humanities. Denver, 2008. 125 p.
- Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I. The Right to Data Portability in the GDPR : Towards User-Centric Interoperability of Digital Services. *Computer Law and Security Review*, 2018, vol. 34, iss. 2, pp. 193—203.
- Jeng Y.-L. An OpenID Based Authentication Mechanism in a Distributed System Environment. *International journal of Computer and Communication Engineering*, 2012, no. 3, pp. 250—252.
- Kerr O. S. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. *The George Washington Law Review*, 2004, vol. 72, no. 6, pp. 1208—1243.
- Kutler N. Protecting Your Online You: A New Approach to Handling Your Online Persona After Death. *Berkley Technology Law Journal*, 2011, vol. 26, no. 4, pp. 1641—1670.
- Malgieri G., Custers B. Pricing Privacy — the Right to Know the Value of your Personal Data. *Computer Law and Security Review*, 2018, vol. 34, iss. 2, pp. 289—303.
- Merzeau L. La présence plutôt que l'identité. *Documentaliste — Sciences de l'Information*, 2010, vol. 47, no. 1, pp. 32—33.
- Panarina M. M. Inheritance of an Account in Social Networks and Digital Inheritance Issues: a Legal Research. *Nasledstvennoe pravo*, 2018, no. 3, pp. 27—28. (In Russ.)
- Prince C. Do Consumers Want to Control their Personal Data? Empirical Evidence. *International Journal of Human-Computer Studies*, 2018, vol. 110, pp. 21—32.
- Tereshchenko L. K. Modernization of Informational Relationships and Informational Legislation. Moscow, 2013. 227 p. (In Russ.)
- Turkle S. Cyberspace and Identity. *Contemporary Sociology*, 1999, vol. 28, no. 6, pp. 643—648.
- Turkle S. *Life on the screen: Identity in the Age of the Internet*. New York, 1995. 347 p.
- Wiszniewski D., Coyne R. Mask and Identity: The Hermeneutics of Self-Construction in the Information Age. *Building Virtual Communities: Learning and change in cyberspace*. Ed. by K. A. Renninger, W. Shumar. 2002. Pp. 191—214.
- Woodman F. L. Fiduciary Access to Digital Assets: A Review of the Uniform Law Conference of Canada's Proposed Uniform Act and Comparable American Model Legislation. *Canadian Journal of Law and Technology*, 2017, vol. 15, no. 2, pp. 193—227.

Информация об авторах

Никита Аркадьевич Данилов, руководитель по правовому взаимодействию с органами исполнительной власти ПАО «Мегафон», кандидат юридических наук

Владислав Валерьевич Силкин, аспирант Национального исследовательского университета «Высшая школа экономики»