ЦИФРОВИЗАЦИЯ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

DOI: 10.36724/2072-8735-2020-14-6-27-32

Докучаев Владимир Анатольевич,
МТУСИ, Москва, Россия, ***v.a.dokuchaev@mtuci.ru***

Маклачкова Виктория Валентиновна,
МТУСИ, Москва, Россия, ***v.v.maklachkova@mtuci.ru***

Статьев Вячеслав Юрьевич,
транспортной безопасности, Москва, Россия, ***svu@rnt.ru***

Ключевые слова: *цифровизация, персональные данные, обработка данных, цифровой двойник, цифровой профиль, обезличивание, идентификация, анонимизированные сведения, информационная безопасность, цифровые модели субъекта, большие данные, дополненная реальность*

Необходимость защиты информации конфиденциального характера резко обострилась в условиях пандемии, охватившей все страны в начале 2020 года. Многочисленные случаи утечки персональных данных и информации конфиденциального характера в процессе удалённой работы и дистанционного обучения определяет то внимание, которое в настоящее время уделяется вопросам организации обработки и обеспечения безопасности персональных данных (ПДн), особенно в условиях начала реализации концепции "цифрового профиля гражданина", утверждённой в марте 2019 г. в Российской Федерации. Ключевым моментом при организации работы с ПДн и их защите является идентификация (определение) субъекта персональных данных. С точки зрения российских законов идентификация субъекта персональных данных может осуществляться на основе любой по форме и содержанию информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу. Противоположностью идентификации субъекта ПДн является обезличивание его персональных данных. В результате этого, без использования дополнительной информации, невозможно определить принадлежность ПДн конкретному субъекту персональных данных. Цифровизация всех областей жизнедеятельности российского государства, общества и личности (в том числе политические, экономические, социальные, и другие аспекты) ведёт к сбору всё большего объёма персональных данных о субъекте. В "цифровой экономике" реализуется переход к управлению на уровне "цифровых двойников" (цифровых моделей) в отличие от управления на уровне физических объектов, процессов и личностей в "аналоговой экономике". Это, в свою очередь, порождает разнообразие возможных негативных воздействий на эти "цифровые двойники", возможность реализации которых зависит от конкретных условий использования "цифровых двойников". Можно сделать вывод, что в настоящее время понятие субъект персональных данных начинает выступать в качестве цифрового дополнения (расширения) конкретной физической личности и ее среды обитания, для которой цифровой профиль носит синергетический характер. Поэтому на передний край обеспечения безопасности чего-либо выступает вопрос качества этих цифровых двойников (адекватность, достоверность, полнота, актуальность).

Информация об авторах:
Докучаев Владимир Анатольевич, *д.т.н., профессор, заведующий кафедрой "Сетевые информационные технологии и сервисы" МТУСИ, Москва, Россия*
Маклачкова Виктория Валентиновна, *старший преподаватель кафедры "Сетевые информационные технологии и сервисы" МТУСИ, Москва, Россия*
Статьев Вячеслав Юрьевич, *к.т.н., эксперт "Фонд транспортной безопасности", Москва, Россия*

Для цитирования:
Докучаев В.А., Маклачкова В.В., Статьев В.Ю. Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №6. С. 27-32.

For citation:
Dokuchaev V.A., Maklachkova V.V., Statev V. Yu. (2020) Digitalization of the personal data subject. *T-Comm*, vol. 14, no.6, pp. 27-32. (*in Russian*)

Введение

С развитием информационно-коммуникационных технологий существенно усилились внимание и интерес к проблемам неприкосновенности частной жизни и безопасности персональных данных. Согласно Доктрине информационной безопасности, утвержденной в 2016 г. Указом Президента РФ № 646 [1], одним из национальных интересов в информационной сфере является «обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий...». Из этого следует то внимание, которое в настоящее время уделяется в организациях вопросам организации обработки и обеспечения безопасности персональных данных (ПДн).

Утверждение в марте 2019 г. на заседании президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности концепции «цифрового профиля гражданина» («цифрового двойника») ещё больше повысило остроту проблем, возникающих при работе с ПДн.

Одним из ключевых моментов в области персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – 152-ФЗ) [4] является идентификация (определение) субъекта персональных данных (далее - субъект ПДн). С точки зрения закона идентификация субъекта персональных данных может осуществляться на основе любой по форме и содержанию информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу [5].

Антитезисом идентификации субъекта ПДн является обезличивание его персональных данных. Так обезличивание персональных данных в статье 3 152-ФЗ определяется как «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». В статьях 5 и 6 152-ФЗ выдвигаются требования, что «обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом» и «обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных» соответственно. Можно констатировать, что обезличивание персональных данных и уничтожение персональных данных явления одного порядка.

Отметим, что события конца 2019 года – первой половины 2020 года, произошедшие в мире в связи с пандемией COVID-19, вынудили часть государств, например Венгрию и Великобританию [2], отойти от стандартных процедур обезличивания персональных данных, предусмотренных Общим регламентом защиты персональных данных Европейского союза (GDPR) [3].

В Российской Федерации вопросы обезличивания персональных данных проработаны достаточно подробно в виде приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и соответствующих ему рекомендаций «Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». При этом процесс идентификации (определения) физического лица как субъекта персональных данных имеет весьма размытое описание в нормативных документах

В контексте сказанного необходимо остановиться на вопросе, который, как кажется авторам, является актуальным и не рассмотрен достаточно подробно в настоящий момент, но который непосредственно связан с выполнением требований статьи 18.1 152-ФЗ по реализации оператором оценки «вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона». В настоящий момент каких-либо рекомендаций по возможным подходам к оценке вреда субъектам ПДн не разработано, тем более что этот вред сугубо индивидуален в одних и тех же условиях для различных субъектов ПДн.

Оценка вреда, который может быть причинен субъекту ПДн, может быть сделана только после определения последствий (в терминологии информационной безопасности) [6], связанных с нарушением конфиденциальности, целостности и доступности персональных данных. По сути это, прежде всего, неправомерное ознакомление и несанкционированное распространение персональных данных, ухудшение качества персональных данных и несвоевременность доступа к ним. Вред может быть различным в зависимости от целей, которые ставит перед собой тот, кто хочет воспользоваться последствиями нарушения Федерального закона.

И так, в контексте сказанного, вопрос об оценке потенциального вреда субъекту ПДн можно сформулировать следующим образом: «Кто идентифицирует субъекта ПДн, с какой целью и что является предметом идентификации»?

Цели и предмет идентификации субъекта персональных данных

Идентификацией субъекта ПДн может заниматься оператор персональных данных или некоторое третье лицо, которое законным или незаконным образом получило доступ к информации о субъекте ПДн. И, если цель идентификации субъекта ПДн со стороны оператора персональных данных очевидна и непосредственно связана с целью обработки персональных данных, то цель идентификации субъекта ПДн со стороны третьего лица не является очевидной, особенно если она носит деструктивный характер. Особого рассмотрения требует предмет идентификации, который определяется исходя из цели идентификации, и может иметь достаточно разнообразное и своеобразное проявление. Тут все зависит от того, кто осуществляет идентификацию субъекта ПДн, так как само понятие субъект персональных данных как физическое лицо с совокупностью своих признаков (прямых или косвенных) существует только в его понимании. Например, это могут быть физические параметры тела субъекта ПДн, это могут быть сведения о заболеваниях членов семьи субъекта ПДн, это могут быть сведения о предпочтениях субъекта ПДн в еде и одежде, это могут быть сведения о распорядке дня субъекта ПДн и т.п. В такой постановке, ис-

ходя из определения персональных данных в статье 3 152-ФЗ, идентификация субъекта есть процесс формирования его информационной модели заданной тематической направленности типа досье.

Исследование заданного вопроса начнем с рассмотрения обобщенной схемы среды жизнедеятельности современной личности.

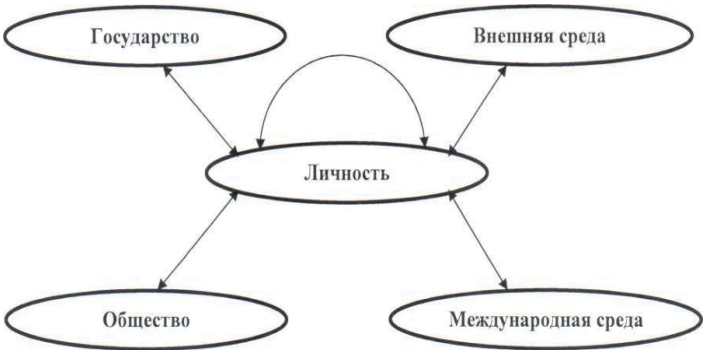

Рис. 1. Обобщенной схемы среды жизнедеятельности современной личности

Данная схема в общем виде показывает, что в процессе своей жизнедеятельности личность (физическое лицо - субъект персональных данных) может вступать в различного рода отношения с государством, обществом, внешней средой, международной средой и другой личностью (далее - объекты взаимоотношений).

В данном случае под государством понимается политическая форма организации общества во главе с правительством и его органами, осуществляющими управление обществом, охрану его экономической и социальной структуры [7], а общество в широком смысле - это совокупность исторически сложившихся форм совместной деятельности людей [8].

Внешнюю среду можно определить как совокупность природной и техногенной среды обитания личности. Международная среда – это совокупность форм организации функционирования международных сообществ, отдельных иностранных государств и соответствующих им обществ.

Идентификация субъекта персональных данных и «цифровой двойник»

Возвращаясь к вопросу идентификации субъекта ПДн по совокупности доступной о нем информации, следует отметить, что в рамках приведенной схемы отношений личности с объектами взаимоотношений осуществляется обработка персональных данных, в процессе которой может быть осуществлена прямая или косвенная идентификация конкретного субъекта ПДн (личности). При этом необходимо иметь в виду, что возникающие отношения между объектом взаимоотношений и личностью могут носить односторонний характер, т.е. только один из участников этого процесса является его активным участником.

Например, государство в лице соответствующих структур может исследовать деятельность личности в части налоговых платежей, а личность может исследовать деятельность другой личности в части легитимности продажи ею некоторой собственности. В этом смысле проведение идентификации субъекта ПДн с деструктивными намерениями по отношению к личности носит односторонний характер.

Прямая идентификация субъекта ПДн может быть осуществлена по нормативно закрепленным признакам (совокупности персональных данных) такой однозначной идентификации. В качестве таких признаков могут выступать:

– глобальные идентификаторы (электронная цифровая подпись, СНИЛС для РФ или, например, персональный банковский код для физических лиц henkilötunnus в Финляндии);

– совокупность паспортных данных (общегражданский паспорт, дипломатический паспорт, загранпаспорт гражданина, паспорт моряка и т.п.);

– совокупность данных различного рода удостоверений (удостоверение работника Прокуратуры, удостоверение члена Совета Федерации, удостоверение члена Государственной Думы, удостоверение судьи, удостоверение военнослужащего, водительское удостоверение и т.п.);

– совокупность данных документов регистрационного характера (вид на жительство, разрешение на временное проживание для лиц без гражданства, приглашение на въезд в страну, сертификат электронной подписи и т.п.).

При прямой идентификации субъекта ПДн определяющая совокупность персональных данных носит устойчивый характер и слабо зависит от временного и пространственного факторов. Напротив, косвенная идентификация субъекта ПДн может иметь дело с переменной совокупностью персональных данных, связанной с временным и пространственным факторами.

Косвенная идентификация субъекта персональных данных носит ассоциативный характер в рамках указанных отношений и связана с различными сведениями, определяющими его физические, экономические, финансовые, социальные, политические, религиозные, медицинские параметры и различного рода предпочтения, наклонности и интересы. Данная идентификация может осуществляться как самостоятельно, так и совместно с прямой идентификацией. В общем случае она не требует наличия юридически значимых признаков субъекта ПДн как физического лица, и вообще при таком виде идентификации субъект ПДн как физическое лицо может не интересовать того, кто осуществляет эту идентификацию (объект взаимоотношений), так как в данном случае первичным предметом идентификации являются указанные выше признаки.

Данный вид идентификации поддерживается различного рода аналитическими моделями и является основой построения цифрового двойника (цифрового профиля) конкретного физического лица. Все дальнейшие отношения объекта взаимоотношений с личностью могут выстраиваться с ее цифровым двойником, так как для реализации целевой функции объекта взаимоотношений в рамках отношений с личностью ему более ничего не требуется.

Косвенная идентификация лежит в основе концепции Больших Данных, которая в настоящее время активно прорабатывается применительно к сфере персональных данных. Так создание цифрового профиля предусмотрено нацпроектом «Цифровая экономика», в рамках федеральной программы «Цифровое государственное управление» к 2024 г.

должна быть создана платформа для идентификации граждан, в рамках которой предполагается наличие цифрового профиля физического лица, обсуждается проект закона о цифровом профиле россиян. При этом поднимается вопрос о необходимости анонимизации, обезличивании сведений о физическом лице. Это упрощает решение вопросов с обработкой персональных данных, так как законы различных стран о защите персональных данных не рассматривают анонимизированные сведения как персональные данные.

Однако проведенные исследования в этой области показывают, что якобы анонимные сведения о физическом лице позволяют с помощью некоторой модели искусственного интеллекта идентифицировать это лицо с точностью до 99,8%. Так наличие 15 определенных анонимных показателей различной тематической направленности позволяют практически однозначно определить конкретное физическое лицо, что в соответствии с 152-ФЗ переводит эти анонимизированные сведения в разряд персональных данных [9]. Если рассмотреть Интернет как совокупность данных, которую можно интерпретировать как большие данные, то интересна в этом смысле информация, размещенная на портале Роскомнадзора [10].

Студентам РГУ нефти и газа им. И.М. Губкина и МГУ им. М.В. Ломоносова в ходе дебатов на тему защиты персональных данных было дано задание по одной лишь фотографии студента, размещенной в Интернете, идентифицировать человека и его родственников, выяснив их фамилии, адреса, телефоны и т.д. В течение 15 минут участники эксперимента, используя поисковые системы, страницы социальных сетей, блогов и форумов, нашли всю необходимую информацию, которая позволила идентифицировать человека и его близких родственников.

Целью прямой идентификации является соотнесение субъекта персональных данных как физического лица с юридически значимыми сведениями (персональными данными) некоторого документа в бумажном или электронном виде, что позволяет реализовывать указанные отношения объекта взаимоотношений с этим лицом со значимой долей легитимности. При этом характер этих отношений (конструктивный или деструктивный) не важен.

Цель косвенной идентификации носит более сложный характер и может быть как конструктивной, так и деструктивной. Косвенная идентификация может быть направлена на:

– повышение эффективности деятельности объекта взаимоотношений в рамках сложившихся отношений с личностью;

– повышение качества сложившихся отношений и (или) формирование новых отношений для личности со стороны объекта взаимоотношений и, как следствие, повышение эффективности деятельности самого объекта взаимоотношений;

– замену прямой идентификации субъекта ПДн его косвенной идентификацией для проведения таргетированных воздействий на субъекта ПДн, возможно негативной направленности, имеющих физический, моральный, материальный, финансовый или иной характер, с потенциальной возможностью изменения отношений этой личности с объектами взаимоотношений;

– проведение таргетированных атак на цифрового двойника личности для нарушения его конфиденциальности, целостности и доступности, следствием чего может быть требуемое изменение отношений этой личности с объектами взаимоотношений.

Основу косвенной идентификации составляют модели и методы анализа данных, которые позволяют соотнести ассоциативные данные с субъектом ПДн. Эти модели и методы определяют потенциальную возможность эффективной идентификации субъекта ПДн. Однако ее реализация зависит от цели идентификации, используемых ассоциативных данных и методов их обработки, возможностей объекта взаимоотношений, т.е. процесс идентификации носит вероятностный характер.

В связи с этим, возвращаясь к вопросу об оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства, необходимо применять риск-ориентированный подход в вопросах идентификации субъекта персональных данных. В этом смысле необходимо говорить о риске нанесения вреда, т.е. о событии риска и ущербе от его наступления. Под событием риска в данном случае понимается идентификация субъекта ПДн в некотором разрезе его цифрового профиля, а под ущербом понимаются некоторые потенциальные негативные последствия этой идентификации (риск реализации некоторых деструктивных воздействий на субъекта ПДн). Например, утечка персональных данных в составе ФИО, СНИЛС (прямая идентификация) может привести к рискам реализации негативных воздействий на субъект ПДн в части его пенсионных накоплений. Очевидно, что таких рисков может быть несколько применительно к конкретной совокупности ассоциативных данных о личности.

Из сказанного следует, что для информационных систем обработки персональных данных наряду с моделями угроз и нарушителя безопасности персональных данных, которые являются исходными документами для организации системы защиты персональных данных, необходимо разрабатывать модель последствий для субъекта ПДн в случае реализации актуальных угроз, обозначенных в модели угроз.

Заключение

В настоящее время осуществляется цифровизация всех областей жизнедеятельности современного государства, общества и личности, включая экономические, социальные, политические и прочие аспекты. Всё это ведёт к увеличению рисков безопасности субъекта ПДн, например, об этом свидетельствует информация в СМИ об утечке данных нарушителей самоизоляции в Москве [11].

Создаются «цифровые двойники» (цифровые модели) физических объектов, физических процессов, процессов принятия решений, а также физических субъектов-личностей этих объектов и процессов. Осуществляется переход от управления на уровне физических объектов, процессов и личностей к управлению на уровне их цифровых двойников.

На передний край обеспечения безопасности чего-либо выступает вопрос качества этих цифровых двойников (адекватность, достоверность, полнота, актуальность). Если ранее различного рода угрозы (негативные воздействия) реализовывались по отношению к физическим объектам, процессам и личностям, то в условиях глобальной цифровизации нега-

тивные воздействия реализуются по отношению к их цифровым двойникам. После этих воздействий искаженные (разрушенные) цифровые модели редуцируются на физическую среду современного государства, общества и личности, одновременно нарушая различные виды безопасности.

Вопрос качества цифровых двойников даже при отсутствии негативных воздействий на них связан с такими факторами, как:

– объем знаний о моделируемых объектах, процессах и их субъектах;

– наличие скрытых структурных и поведенческих характеристик у моделируемых объектов, процессов и субъектов;

– собственные ошибки цифрового моделирования;

– наличие различного рода ресурсов для осуществления цифрового моделирования.

Для снижения влияния указанных факторов используются технологии Больших Данных, искусственного (добавленного) интеллекта, программной и аппаратной роботизации.

Развитие технологий цифровизации и сфер их применения в различных областях жизнедеятельности современного государства, общества и личности порождает значительное разнообразие множества негативных воздействий на их цифровые модели. Причем в каждый текущий момент это множество не имеет полного описания, что в практике программирования отражено в виде тезиса «исправляется всегда предпоследняя ошибка». Потенциальная возможность реализации указанных негативных воздействий зависит от конкретных условий использования цифровых двойников.

Изложенный подход к вопросам идентификации субъекта персональных данных подводит к мысли, что, по сути, понятие «субъект персональных данных» в современных условиях начинает выступать в качестве цифрового дополнения (расширения) конкретной физической личности и ее среды обитания, для которой цифровой профиль носит синергетический характер. Характеристики цифрового профиля могут являться синтетическими понятиями типа индекса интеллектуального развития и быть неизвестны самой личности (сам человек о себе ничего не знает). Поэтому вопросы адекватности цифрового профиля конкретной личности приобретают первостепенное значение с учетом перехода из физической реальности в дополненную цифровую реальность.

Литература

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Сайт Президента РФ. http://kremlin.ru/acts/bank/41460 (дата обращения: 09.05.2020).
2. Hungarian government suspends EU data protection rights. Сайт “EURACTIV.com”. [Электронный ресурс]. URL: https://www.euractiv.com/section/digital/news/hungarian-government-suspends-eu-data-protection-rights/ (дата обращения: 10.05.2020).
3. Global Data Protection Regulation. EU GDPR Portal. https://www.eugdpr.org/ (дата обращения: 09.05.2020).
4. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» Сайт Президента РФ. http://www.kremlin.ru/acts/bank/24154 (дата обращения: 09.05.2020).
5. *Докучаев В.А., Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Идентификация субъекта – ключевой момент в процессе обработки персональных данных // Сборник трудов XIV Международной отраслевой научно-технической конференции «Технологии информационного общества». 2020. С. 273-274.
6. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Классификация угроз безопасности персональных данных в информационных системах // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №1. С. 56-60.
7. Большой толковый словарь русского языка: А-Я / РАН. Ин-т лингв. исслед.; Сост., гл. ред. канд. филол. наук С. А. Кузнецов. СПб.: Норинт, 1998. 1534 с. ISBN 5-7711-0015-3.
8. Большой Энциклопедический Словарь, 2-е изд. Универсальное справочное издание. М.: изд. "Большая Российская Энциклопедия", 1998. 1456 с.
9. "Коммерсантъ" от 24.07.2019. Мнимая анонимность [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4040585 (дата обращения: 09.05.2020).
10. Студентам в ходе дебатов на тему защиты персональных данных удалось собрать в интернете информацию о человеке по одной фотографии. Сайт Роскомнадзора, 03.12.2019 [Электронный ресурс]. URL: https://https://pd.rkn.gov.ru/press-service/subject1/news4782/ (дата обращения: 09.05.2020).
11. "Коммерсантъ" от 18.05.2020. Прокуратура проверяет утечку данных нарушителей самоизоляции [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4348076 (дата обращения: 18.05.2020).

DIGITALIZATION OF THE PERSONAL DATA SUBJECT

Vladimir A. Dokuchaev, *MTUCI, Moscow, Russia,* ***v.a.dokuchaev@mtuci.ru***
Victoria V. Maklachkova, *MTUCI, Moscow, Russia,* ***v.v.maklachkova@mtuci.ru***
Vyacheslav Yu. Statev, *Transport Safety Fund, Moscow, Russia,* ***svu@rnt.ru***

Abstract
The need to protect confidential information has intensified sharply due the pandemic that swept all countries in early 2020. The numerous cases of leakage of personal data and confidential information in the process of remote work and distance learning determines the attention that is currently being paid to the organization of processing and ensuring the security of personal data, especially in the context of the beginning of the implementation of the concept of "digital citizen profile", approved in March 2019 in the Russian Federation. The key point in the organization of work with personal data and their protection is the identification (determination) of the personal data subject. From the point of view of Russian laws, the identification of the personal data subject can be carried out on the basis of any form and content of information relating to a directly or indirectly identified or identifiable individual. The opposite of the identification of the personal data subject is the depersonalization of his personal data. As a result of this, without the use of additional information, it is impossible to determine the ownership of personal data to a specific personal data subject. Digitalization of all activities of life of the Russian state, society and the individual (including political, economic, social, and other aspects) leads to the collection of an increasing amount of personal data about the natural person. In the "digital economy", a transition to management at the level of "digital twins" (digital profiles) is being implemented, as opposed to management at the level of physical objects, processes and personalities in the "analog economy". This, in turn, gives rise to a variety of possible negative impacts on these "digital twins" the possibility of which depends on the specific conditions of use of "digital twins". It can be concluded that at present, the concept of the personal data subject begins to act as a digital supplement (extension) or as augmented reality of a personal data subject of a specific physical person and his (her) environment, for which the digital profile is synergistic. Therefore, the issue of the quality of these "digital twins" (adequacy, reliability, completeness, relevance) is at the forefront of ensuring the security of something.

Keywords: *digitalization, personal data, data processing, personal data subject, digital twin, digital profile, depersonalization, identification, anonymous information, information security, subject's digital models, big data, augmented reality.*

References

1. Decree of the President of the Russian Federation of December 5, 2016 No. 646 "On the approval of the Doctrine of information security of the Russian Federation." Site of the President of the Russian Federation. http://kremlin.ru/acts/bank/41460 (date accessed: 05/09/2020).
2. Hungarian government suspends EU data protection rights. Сайт "EURACTIV.com". [Электронный ресурс]. - URL: https://www.euractiv.com/section/digital/news/hungarian-government-suspends-eu-data-protection-rights/ (дата обращения: 10.05.2020).
3. Global Data Protection Regulation. EU GDPR Portal. https://www.eugdpr.org/ (дата обращения: 09.05.2020).
4. Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" Site of the President of the Russian Federation. http://www.kremlin.ru/acts/bank/24154 (date accessed: 05/09/2020).
5. Dokuchaev V.A., Dokuchaev V.A., Maklachkova V.V., Statiev V.Yu. (2020). Subject identification is a key point in the processing of personal data. In the collection: Technologies of the information society. *Proceedings of the XIV International Branch Scientific and Technical Conference*. 2020. P. 273-274.
6. Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. (2020). Classification of personal data security threats in information systems. *T-Comm*, vol. 14, no.1, pp. 56-60. (in Russian)
7. Comprehensive explanatory dictionary of the Russian language: A-Z / RAS. Institute of ling. research.; Comp., Ch. ed. Cand. philol. Sciences S.A. Kuznetsov. SPb.: Norint, 1998. 1534 p. ISBN 5-7711-0015-3.
8. Big Encyclopedic Dictionary, 2nd ed., 1456 p., Moscow., Ed. "Great Russian Encyclopedia". 1998.
9. "Kommersant" dated 07.24.2019. Imaginary anonymity [Electronic resource]. - URL: https://www.kommersant.ru/doc/4040585 (date of access: 05/09/2020).
10. During the debate on the protection of personal data, students managed to collect information about a person on the Internet from one photo. Roskomnadzor website, 03.12.2019 [Electronic resource]. - URL: https: // https://pd.rkn.gov.ru/press-service/subject1/news4782/ (date accessed: 05/09/2020).
11. "Kommersant" dated 05/18/2020. The prosecutor's office checks the data leakage of self-isolation violators [Electronic resource]. URL: https://www.kommersant.ru/doc/4348076 (date of access: 18.05.2020).

Information about authors:
Vladimir A. Dokuchaev, *DSc (Technical), Professor, Head of the Department "Network Information Technologies and Services" MTUCI, Moscow, Russia*
Victoria V. Maklachkova, *DSc (Mathematical), Senior Researcher, Professor of the Department of "Network Information Technologies and Services", MTUCI, Moscow, Russia*
Vyacheslav Yu. Statev, *PhD, expert, Transport Safety Fund, Moscow, Russia*