DOI: 10.17803/1729-5920.2021.178.9.088-101

А. Н. Мочалов*

Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности[1]

Аннотация. В статье рассматриваются основные угрозы правам человека в связи с введением в Российской Федерации цифровых профилей. Наибольшим рискам подвержены право на неприкосновенность частной жизни и право на достоинство. Кроме того, повышается риск дискриминации. Анализируя текущее правовое регулирование цифрового профиля, автор приходит к выводу, что оно не отвечает критерию правовой определенности и создает повышенные риски вторжения государства и частных структур в сферу частной жизни человека. Несмотря на то что в настоящее время цифровые профили граждан представляют собой только свод официальной информации, содержащейся в некоторых государственных информационных системах и публичных реестрах, в будущем, по мнению автора, данная инфраструктура может быть использована для профилирования людей, углубленного анализа, мониторинга и прогнозирования их поведения, как это делается уже сегодня некоторыми другими государственными и негосударственными организациями.
В основе правового регулирования цифрового профиля должны лежать специальные гарантии прав человека, связанные со сбором и обработкой имеющейся в распоряжении государства персональной информации о гражданах. К числу таких гарантий автор относит, в частности, установление в законе перечня сведений, которые не могут входить в состав цифрового профиля гражданина или быть иным образом связанными с ним, перечня недопустимых целей использования цифровых профилей, а также установление обязанности операторов в доступной форме доводить до субъектов информацию о фактах и юридических последствиях профилирования, о принципах и логических схемах, лежащих в основе профилирования.
Ключевые слова: цифровой профиль; профилирование; персональные данные; права человека; гарантии; частная жизнь; неприкосновенность частной жизни; цифровая экономика; национальная система управления данными.
Для цитирования: *Мочалов А. Н.* Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica. — 2021. — Т. 74. — № 9. — С. 88–101. — DOI: 10.17803/1729-5920.2021.178.9.088-101.

Digital Profile: Main Risks for Constitutional Human Rights in the face of Legal Uncertainty[2]

Artur N. Mochalov, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Constitutional Law, Ural State Law University
ul. Komsomolskaya, d. 21, Ekaterinburg, Russia, 620137
artm84@gmail.com

Abstract. The paper considers the main threats to human rights in connection with the introduction of digital profiles in the Russian Federation. Rights such as the right to privacy and the right to dignity are most at risk. In addition, the risk of discrimination increases. Analyzing the current legal regulation of the digital profile, the

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16204.
[2] The reported study was funded by RFBR according to the research project № 18-29-16041.

* *Мочалов Артур Николаевич,* кандидат юридических наук, доцент, доцент кафедры конституционного права Уральского государственного юридического университета
Комсомольская ул., д. 21, г. Екатеринбург, Россия, 620137
artm84@gmail.com

author concludes that it does not meet the criterion of legal certainty and creates increased risks of intrusion of the state and private structures into the sphere of a person's private life. Despite the fact that currently digital profiles of citizens are only a set of official information contained in some state information systems and public registers, according to the author, in the future, this infrastructure can be used for profiling people, in-depth analysis, monitoring and forecasting their behavior, as is already done today by some other states and non-governmental organizations.

The legal regulation of the digital profile should be based on special guarantees of human rights in connection with the collection and processing of personal information about citizens available to the state. Among such guarantees, the author includes, in particular, the establishment in the law of a list of information that cannot be part of a digital profile of a citizen or be otherwise related to it, a list of unacceptable purposes for using digital profiles, as well as the establishment of the obligation of operators to inform subjects in an accessible form about the facts and legal consequences of profiling, about the principles and logical schemes underlying profiling.

Keywords: digital profile, profiling, personal data, human rights, guarantees, private life, privacy, digital economy, national data management system.

Cite as: Mochalov AN. Tsifrovoy profil: osnovnye riski dlya konstitutsionnykh prav cheloveka v usloviyakh pravovoy neopredelennosti [Digital Profile: Main Risks for Constitutional Human Rights in the face of Legal Uncertainty]. *Lex russica*. 2021;74(9):88-101. DOI: 10.17803/1729-5920.2021.178.9.088-101. (In Russ., abstract in Eng.).

Национальным проектом «Цифровая экономика Российской Федерации» предусмотрено формирование «цифрового государственного управления», существенным элементом которого должны стать цифровые профили граждан и юридических лиц. Согласно паспорту национального проекта[3], до конца 2024 г. должна быть создана платформа идентификации, включающая в себя наряду с такими инструментами, как биометрическая идентификация и облачная квалифицированная электронная подпись, цифровые профили гражданина и юридического лица[4]. Инфраструктура цифрового профиля будет представлять собой «платформу, обеспечивающую обмен информацией между государством, гражданами, а также коммерческими и некоммерческими организациями, в том числе с согласия гражданина»[5].

Инфраструктура цифрового профиля создается в рамках эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах. Этот эксперимент, в свою очередь, является частью еще более масштабного проекта по формированию национальной системы управления данными (далее — НСУД), концепция создания и функционирования которой была утверждена распоряжением Правительства РФ от 03.06.2019 № 1189-р (далее — Концепция). Согласно Концепции, формирование НСУД предполагает установление единых требований к управлению государственными данными и приведение их в соответствие с этими требованиями.

Порядок проведения эксперимента регулируется положением, утвержденным постановлением Правительства РФ от 03.06.2019 № 710[6] (далее — Положение; Постановление № 710). Срок эксперимента изначально был установлен с 1 июля 2019 г. по 31 марта 2020 г., однако затем несколько раз продлевался, и теперь датой его окончания значится 31 декабря 2021 г. Предполагается, что по окончании эксперимента на смену подзаконному регули-

[3] Паспорт национального проекта «Национальная программа "Цифровая экономика Российской Федерации"» (утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // СПС «КонсультантПлюс».

[4] Первоначально в соответствии с ранее действовавшим паспортом национальной программы «Цифровая экономика Российской Федерации» от 24.12.2018 срок создания инфраструктуры цифрового профиля был определен до конца 2023 г.

[5] Паспорт федерального проекта «Информационная инфраструктура» (утвержден президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // СПС «КонсультантПлюс».

[6] Постановление Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // СПС «КонсультантПлюс».

рованию должен прийти федеральный закон, который определит порядок функционирования инфраструктуры цифрового профиля и использования данных, содержащихся в цифровых профилях граждан и организаций. Проект федерального закона «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» (законопроект № 747513-7, далее — законопроект)[7] был внесен в Государственную Думу 5 июля 2019 г., однако по состоянию на май 2021 г. его рассмотрение приостановлено в связи с отрицательным заключением ответственного комитета.

В статье я приведу некоторые соображения о конституционно-правовых рисках, связанных с введением в действие инфраструктуры цифрового профиля и повышением связанности государственных данных о физических лицах. Прежде всего, речь пойдет о рисках нарушения конституционных прав и свобод человека и гражданина в условиях правовой неопределенности. Как будет показано далее, создание цифровых профилей позволит обрабатывать и использовать данные о гражданах на качественно новом уровне, что сопряжено с повышенным риском вмешательства государства и частных субъектов в сферу частной жизни человека.

За последние несколько лет отечественными учеными был опубликован ряд научных статей, направленных как на юридическое осмысление цифровых профилей и обеспечение безопасности составляющих их сведений[8], так и на рассмотрение проблем защиты персональных данных в цифровом мире в целом[9], в том числе в контексте распространения технологии «больших данных»[10]. В то же время российское законодательство в этой сфере по-прежнему серьезно отстает от достигнутого уровня технологического развития и не обеспечивает адекватных гарантий прав человека при использовании современных методов обработки данных, в том числе при профилировании лиц. В заключение будут предложены отдельные направления совершенствования законодательной базы в части закрепления таких гарантий.

1. О понятии и содержании цифрового профиля. Ни один из названных выше документов не содержит определения цифрового профиля. Определить данное понятие попытались авторы упомянутого законопроекта: «совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации» (п. 3 ст. 1 законопроекта). Из Постановления № 710 также можно сделать вывод, что цифровой профиль — это не просто совокупность сведений, а определенным образом упорядоченный массив официальных данных о гражданине или юридическом лице, достоверность которых подтверждена компетентными органами государства. Дефиниция «инфраструктуры цифрового профиля» приведена в пп. «а» п. 2 Положения. Из этой нормы следует, что указанная инфраструктура призвана обеспечивать в рамках Единой системы идентификации и аутентификации (далее — ЕСИА) доступ граждан, а по их инициативе либо с их согласия — также определенных организаций к сведениям, используемым для оказания государственных и муниципальных услуг (либо сформированным в результате их предоставления) и осуществления государственных и муниципальных функций.

Перечень сведений, образующих цифровой профиль гражданина, содержится в приложении к Положению и включает почти сорок позиций. В основном это анкетные данные (паспортные данные, адрес места жительства, идентификационный номер налогоплательщика и т. д.) и сведения из публичных реестров (например, о принадлежащей недвижимости). Но есть в нем и информация, которая обычно считается более «чувствительной».

---

7 URL: https://sozd.duma.gov.ru/bill/747513-7 (дата обращения: 09.06.2021).

8 *Жарова А. К.* Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55–61.

9 *Солдатова В. И.* Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. № 2. С. 33–43 ; *Талапина Э. В.* Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права Российской академии наук. 2018. Т. 13. № 5. С. 117–150.

10 *Савельев А. И.* Проблемы применения законодательства о персональных данных в эпоху «больших данных» (big data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

Например, это сведения из электронной трудовой книжки (к которым в соответствии со ст. 66.1 Трудового кодекса РФ относятся в том числе сведения о переводах и увольнении, об основаниях и причинах расторжения трудового договора), сведения о доходах и уплаченных налогах и т. д. Попадут в цифровые профили и собираемые Банком России сведения о деловой репутации отдельных лиц (учредителей банков, негосударственных пенсионных фондов, членов их органов управления и т. д.). В свою очередь, они включают информацию из целого ряда источников: начиная с Картотеки арбитражных дел и Единого федерального реестра сведений о банкротстве и заканчивая перечнем террористов, который ведет Росфинмониторинг[11].

Существующий перечень сведений, предоставляемых в составе цифрового профиля, охватывает далеко не всю имеющуюся в распоряжении государства и местных органов информацию о гражданах и полученных ими государственных и муниципальных услугах. Так, например, в настоящее время в цифровые профили не включаются сведения о полученных гражданином государственных документах об образовании или о зарегистрированных на его имя объектах интеллектуальной собственности. Можно предположить, что по мере совершенствования НСУД структура цифрового профиля также будет расширяться за счет привлечения новых информационных ресурсов. Кроме того, пока в приложении к Положению говорится о сведениях, образующих цифровые профили только граждан. Но в скором времени аналогичный подход будет применен и к организациям.

Реализация принципа связанности данных, лежащего в основе цифрового профиля, позволит заинтересованному пользователю (самому субъекту, а также в определенных случаях государственным органам, органам местного самоуправления, организациям) в любой момент извлекать и обрабатывать необходимые данные в требуемом объеме. В частности, инфраструктура цифрового профиля, согласно Положению, должна обеспечивать следующие функциональные возможности:

— сохранение, автоматизированное обновление и автоматизированное предоставление гражданину по его запросу необходимых сведений о нем;
— организация доступа отдельных организаций (банков, страховщиков, операторов связи, микрофинансовых организаций и т. д.) к сведениям о клиенте — физическом лице по его инициативе или с его согласия в случае обращения с заявлением или за заключением договора;
— автоматизированное использование необходимых сведений о гражданине при его обращении за предоставлением государственных или муниципальных услуг;
— мониторинг гражданином доступа организаций к сведениям о нем, содержащимся в ЕСИА и в иных государственных и муниципальных информационных системах, и т. д.

Введение цифровых профилей призвано обеспечить интероперабельность государственных информационных ресурсов и согласованность содержащихся в них данных. В настоящее время количество таких ресурсов настолько велико, что часто происходит дублирование одной и той же информации, ее тиражирование разными операторами. В результате несвоевременной актуализации информации возникают противоречия между сведениями, содержащимися в разных информационных системах. Итогом является риск «ограничения и даже ущемления прав граждан в ситуации, когда такая система технически не позволяет гражданину совершить определенное действие, предусмотренное законодательством»[12]. Другим несомненным преимуществом введения цифровых профилей является предоставление возможности субъектам контролировать использование данных о себе, а также управлять этими данными. Наконец, цифровые профили должны расширить доступ частного сектора к инфраструктуре государственных информационных систем, в частности ЕСИА. Мгновенный доступ поставщиков услуг к достоверным официальным данным о гражданине или организации упростит заключение и исполнение контрактов в Интернете, избавит от необходимости проведения рутинных формальных процедур по предоставлению и проверке информации и подтверждающих документов, снизит риски злоупотреблений и

[11] См.: положение Банка России от 27.12.2017 № 625-П «О порядке согласования Банком России назначения (избрания) кандидатов на должности в финансовой организации…» // СПС «КонсультантПлюс».

[12] *Афанасьев С. Д.* Формирование национальной системы управления данными: конституционно-правовые аспекты // Конституционное и муниципальное право. 2019. № 12. С. 9–14.

повысит уровень доверия между участниками правоотношений.

2. Риски нарушения конституционных прав и свобод человека. Инфраструктура цифрового профиля создаст не только новые возможности для управления данными и развития цифровой экономики, но и повышенные риски для человека, связанные с вмешательством в сферы, традиционно относящиеся к его частной жизни и охраняемые ст. 24 Конституции РФ.

В научной литературе выделяется три уровня цифрового профиля[13]. На первом уровне осуществляется генерация данных из источников, на которых пользователи сами способны управлять информацией, в том числе определять круг лиц, получающих доступ к ней. На втором уровне генерируются данные, собираемые автоматически, в том числе передаваемые электронными устройствами (например, данные о местоположении лица, об устройствах, с которых пользователь выходит в Сеть, о семантике поисковых запросов, о профессиональных связях и т. д.). Субъект уже не может в полной мере контролировать передачу и использование такой информации. Наконец, на третьем уровне создаются производные данные на основе анализа тех данных, которые были получены на первых двух уровнях. При этом сам субъект уже полностью лишен возможности управлять производными данными о себе. Но именно эти данные позволяют осуществлять так называемое профилирование субъекта, в том числе получать путем вычислений и построения корреляционных статистических закономерностей информацию, не всегда очевидную даже для самого субъекта, но весьма точно раскрывающую его характер, образ жизни, мировоззрение, привычки, предпочтения и т. д. На основе таких данных возможно проведение мониторинга поведенческой активности человека и прогнозирование его действий.

Обеспокоенность, связанную с профилированием граждан, еще в 2013 г. выразил Комитет министров Совета Европы в Рекомендации CM/Rec(2010)13[14], отметив, что профильные характеристики, присваиваемые субъекту данных, «делают возможным создание новых персональных данных, не являющихся идентичными тем, которые были переданы указанным субъектом контролеру». По этой причине метод профилирования создает «значительный риск для прав и свобод человека»: люди могут «попадать в определенные категории, причем зачастую не зная об этом», а «профилирование отдельного лица может привести к неоправданному лишению его права на доступ к тем или иным товарам и услугам, тем самым нарушая принцип недопустимости дискриминации». Определение профилирования (создания профиля) физического лица содержится в Общем регламенте Европейского Союза о защите персональных данных (General Data Protection Regulation — GDPR). Это автоматизированное использование персональных данных в целях определения, оценки и анализа определенных индивидуальных аспектов физического лица, в том числе его производственных показателей, экономического положения, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, местоположения или передвижения.

В России цифровой профиль гражданина — в том виде, в каком он существует сегодня, — не является результатом или инструментом профилирования человека по смыслу GDPR. Скорее, это его «цифровой отпечаток», содержащий исключительно официальные сведения первого уровня. Они предназначены для идентификации сведений о лице в государственных информационных системах, но сами по себе малопригодны для оценки индивидуальных характеристик и поведения человека (хотя уже на их основе можно сформировать предварительное представление о надежности, платежеспособности и деловой репутации лица).

Однако следует отметить, что пока цифровой профиль в нашей стране — это лишь эксперимент, задачей которого является апробация

---

[13] *Жарова А. К.* Указ. соч.
Данная структура в целом отражает существование трех групп персональных данных, выделяемых в документах ОЭСР: предоставляемые данные (volunteered data), наблюдаемые данные (observed data) и прогнозные данные (inferred data) (см.: *Савельев А. И.* На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4. С. 174–195).

[14] Рекомендация CM/Rec(2010)13 Комитета министров странам-членам по вопросам защиты частных лиц в связи с автоматизированной обработкой персональных данных в контексте профилирования граждан (утверждена Комитетом министров 23.11.2010) // URL: https://www.refworld.org.ru/category,COI,COEMINISTERS,,,5513f93e4,0.html (дата обращения: 09.06.2021).

его возможностей на примере автоматизации некоторых рутинных процессов. Государство располагает огромным объемом других сведений о гражданах, которые остаются за рамками цифровых профилей, но обладают колоссальным потенциалом для профилирования и категорирования людей, анализа и прогнозирования их поведения. Поэтому использование цифровых профилей (и в целом НСУД) именно для профилирования граждан и мониторинга их поведенческой активности — это, скорее всего, дело ближайшего будущего. По крайней мере, было бы наивным полагать, что государство откажется от такой возможности использования данных о лицах. Правовое регулирование цифрового профиля следует выстраивать с учетом этой перспективы.

В настоящее время перечень сведений, предоставляемых с использованием инфраструктуры цифрового профиля гражданина, закреплен в приложении к Положению. Формально он является исчерпывающим и включает в себя лишь малую часть информации о гражданах, имеющейся в распоряжении органов государства. Однако само Положение носит подзаконный характер, поэтому его изменение не требует прохождения законодательной процедуры. Только в результате внесения поправок в ноябре 2020 г. и апреле 2021 г. этот перечень вырос почти в два раза и, очевидно, продолжит расширяться. Ни Постановление № 710, ни Концепция, ни даже внесенный в Государственную Думу законопроект не содержат каких-либо ограничений, связанных с отнесением той или иной информации к цифровому профилю конкретного человека. Не существует для этого ограничений и в действующих федеральных законах. Говоря о повышении связанности данных, содержащихся в государственных информационных ресурсах, следует отметить, что Концепция вообще не делает каких-либо исключений или различий в отношении тех или иных категорий данных. Положение, в свою очередь, также предельно широко говорит о предназначении инфраструктуры цифрового профиля: для получения сведений, необходимых для предоставления государственных или муниципальных услуг или осуществления государственных или муниципальных функций, в том числе о результатах предоставления соответствующих услуг. При таком регулировании государство практически ничем не ограничено в связывании в цифровой профиль любых имеющихся у него данных о лице.

Это опасение имеет под собой основания. Наряду с созданием инфраструктуры цифрового профиля в настоящее время реализуются и другие мероприятия по расширению возможностей использования ЕСИА и аккумулированию широкого набора сведений о гражданах в государственных информационных ресурсах.

Так, постановлением Правительства РФ от 27.03.2021 № 453 был дан старт эксперименту по использованию ЕСИА для идентификации и аутентификации пользователей социальных сетей и ресурсов поиска сотрудников и работы, а также сторон договоров, заключаемых посредством интернет-платформ и агрегаторов. Эксперимент, если его результаты будут признаны успешными, вполне может перерасти в повсеместную практику. Очевидно, что действия пользователей, совершенные в Сети после идентификации через ЕСИА, оставляют цифровые следы в самой ЕСИА. Как минимум это информация о ресурсах, на которых пользователь зарегистрировался или осуществил вход через ЕСИА. При этом не существует ограничений на сбор информации о любых других следах, оставленных пользователем на таких ресурсах, включая просмотренные страницы, сделанные заказы, поисковые запросы и т. д. Для биометрической идентификации и аутентификации граждан, в том числе в отношениях с госорганами, банками, при обращении к нотариусу, уже сегодня активно используется Единая биометрическая система (ЕБС), данные из которой синхронизируются с ЕСИА.

В рассматриваемом контексте вызывает неоднозначную оценку и аккумулирование государством электронных чеков. В начале 2021 г. Федеральная налоговая служба запустила сервис хранения электронных чеков «Мои чеки онлайн»[15]. Согласно пресс-релизу ФНС, сервис позволит пользователю иметь полную информацию о своих покупках в одном месте, а в будущем — автоматически рассчитывать сумму налогового вычета при покупке лекарств[16]. Обратной стороной этой инициативы является

[15] В России создадут сервис хранения электронных чеков // URL: https://ria.ru/20210224/cheki-1598781491.html (дата обращения: 09.06.2021).

[16] ФНС разрабатывает сервис для хранения электронных чеков // URL: https://www.nalog.gov.ru/rn77/news/activities_fts/10592783/ (дата обращения: 09.06.2021).

практически не регламентированный законом доступ государства к обширной информации о покупках, совершаемых гражданами, в том числе о времени их совершения, предмете, суммах, продавцах и т. д. Учитывая, что абонентский номер телефона, указываемый пользователем при совершении онлайн-платежа, может быть однозначно соотнесен с конкретным физическим лицом (в силу требования п. 1 ст. 44 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», предусматривающего возможность заключения договора на оказание услуг подвижной радиотелефонной связи с абонентом при условии представления им достоверных сведений о себе[17]), сведения из электронных чеков вполне могут оказаться связанными с цифровыми профилями конкретных граждан и использоваться для анализа их поведения, потребительских предпочтений, расходов и т. д., а также для прогнозирования поведения как определенного человека, так и других людей, обладающих сходными характеристиками.

Наконец, в государственных информационных ресурсах содержатся и иные сведения, которые могут быть однозначно соотнесены с определенными гражданами, в том числе полученные с использованием технологий автоматической видеофиксации нарушений, распознавания лиц[18], контроля перемещения граждан (в частности, для отслеживания нарушений условий карантина и изоляции в условиях распространения новой коронавирусной инфекции[19]), геномной и дактилоскопической регистрации и т. д. На государственные данные, в свою очередь, могут накладываться сведения, характеризующие индивидуальные особенности взаимодействия конкретного человека с электронными устройствами для выхода в Сеть (время и периодичность выхода в Интернет, скорость нажатия клавиш, угол наклона смартфона и т. д.), а также сведения, размещенные человеком в открытых профилях в социальных сетях и на других сайтах (например, на сайтах поиска работы, объявлений, знакомств). Совокупность всех этих данных, технологически взаимосвязанных между собой, позволит обрабатывать информацию об индивидах на качественно ином уровне, позволяющем получать путем вычислений знания, характеризующие личность каждого отдельно взятого человека, моделировать и прогнозировать его поведение.

Справедлива следующая закономерность: чем больше персональных данных о лице агрегируется и подвергается обработке, тем выше степень вмешательства в частную жизнь такого лица и, соответственно, величина риска, связанного с нарушением его прав[20]. Поэтому связывание огромного числа информации о человеке в централизованный ресурс и ее обработка без надлежащего законодательного регулирования, в том числе без четко определенных законом ограничений, представляют серьезный вызов индивидуальным правам и свободам, в первую очередь — праву на уважение частной жизни и праву на достоинство. Согласно ст. 21 Конституции РФ, ничто не может служить основанием для умаления человеческого достоинства. Вместе с тем оно может оказаться умаленным как в силу самого факта получения государством или частным субъектом сведений, составляющих приватную сферу индивида, так и в результате дискриминации: если, например, лицу в результате анализа его персональной информации будет отказано в предоставлении той или иной услуги (например, в выдаче кредита) или в удовлетворении его просьбы или требования. Опасность дискриминации связана, в частности, с возможными ошибками при автоматизированной обработке персональных данных, в том числе ошибками в алгоритмах и программ-

[17] С 1 июня 2021 г. вводится возможность внесения в ЕСИА сведений об абонентских номерах подвижной радиотелефонной связи и об идентификаторах пользовательского оборудования (Федеральный закон от 30.12.2020 № 533-ФЗ «О внесении изменений в Федеральный закон “О связи”»). Включение таких сведений в ЕСИА пока будет осуществляться самими гражданами добровольно (п. 7 ст. 45 Федерального закона «О связи»), однако не исключено, что в будущем это может приобрести обязательный характер.

[18] В Москве заработала одна из крупнейших в мире систем видеонаблюдения с функцией распознавания лиц // URL: https://www.mos.ru/news/item/30105073/ (дата обращения: 09.06.2021).

[19] Минкомсвязь создает систему отслеживания за гражданами, нарушившими карантин // URL: https://digital.ac.gov.ru/news/4539/ (дата обращения: 09.06.2021).

[20] *Савельев А. И.* Проблемы применения законодательства о персональных данных в эпоху «больших данных» (big data). // Право. Журнал Высшей школы экономики. 2015. № 1. С. 52.

ных кодах, а также с возможностью неверной интерпретации результатов такой обработки.

Приведенные выше опасения нельзя считать надуманными. В Китае уже несколько лет действует государственная программа социального рейтингования граждан путем присвоения им баллов. Система социального рейтинга основана на сборе и анализе огромных массивов данных о гражданах, начиная от уровня образования и заканчивая сделанными ими покупками в онлайн-магазинах[21]. Граждане зарабатывают или теряют баллы в зависимости от поведения: оплаты кредитов, нарушений правил дорожного движения, активности в Интернете и т. д. Для лиц с низким рейтингом существуют «наказания»: например, им могут не продать билет на самолет или ночной поезд и даже отказать в социальном обеспечении[22]. В западном мире тоже есть примеры профилирования индивидов государством на основе автоматизированной обработки персональных данных, например для выявления лиц, склонных к совершению общественно опасных поступков. Так, чикагская полиция еще в 2013 г. запустила программу по предупреждению незаконного использования оружия, основываясь на анализе профилей граждан из группы риска[23].

В России профилирование пользователей уже сегодня активно используется частными субъектами: банками, интернет-провайдерами, администрациями социальных сетей. К примеру, по информации портала Bankiros.ru, один из российских операторов сотовой связи активно предлагает банкам услуги по выявлению потенциально недобросовестных клиентов и вероятности просрочки ими платежей по кредитам, а также по проверке достоверности персональных данных, сообщенных клиентом. Для оценки клиента используется скоринговая система, анализирующая финансовое поведение пользователя (независимо от того, является ли он абонентом данного оператора) по более чем 400 метрикам (частота оплаты услуг связи, геоаналитика, вид и модель используемых устройств и т. д.)[24]. Действующее законодательство не предусматривает механизма информирования граждан ни о фактах проведения в отношении них профилирования, ни об используемых в нем принципах и логических схемах, ни и о возможных последствиях совершаемых ими действий, попадающих под мониторинг. Не закреплено и право оспаривать результаты мониторинга или требовать их раскрытия. Институт профилирования по-прежнему не известен российскому законодательству, в связи с чем особенностей и условий использования персональных данных для целей профилирования, а также специфических гарантий прав субъектов при их профилировании в России не существует.

В свете данной проблемы существенное значение приобретает вопрос не только о составе данных, образующих цифровые профили, но и о целях использования этих данных, а также о том, кому и в каком объеме они могут быть предоставлены. Пока регулирование данного вопроса также не обладает необходимой правовой определенностью. Причем, в отличие от Положения, предусматривающего исчерпывающий перечень случаев обращения к цифровым профилям граждан, законопроект не конкретизирует основания предоставления информации из цифровых профилей «по запросам организаций», оставляя, видимо, пространство для подзаконного нормотворчества. Представляется, что именно в законе (а не в подзаконном акте) должны определяться как круг лиц, имеющих возможность получения сведений из цифрового профиля, так и закрытый и ясно определенный перечень целей, с которыми эта информация может передаваться и использоваться.

Должен быть четко определен и объем сведений о гражданине, предоставляемых по запросам пользователей инфраструктуры цифрового профиля в зависимости от цели. Действующее Положение не определяет его, ограничиваясь лишь указанием на цели предоставления и на необходимость проявления

---

[21] См.: *Петров А. А.* Китайский цифровой профиль или скоринговая система социального доверия // Chronos. 2020. № 8. С. 11–24.

[22] Как работает система социального доверия в Китае // URL: https://tass.ru/opinions/5225841 (дата обращения: 09.06.2021).

[23] Data Is Power: Profiling and Automated Decision-Making in GDPR // URL: https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf (дата обращения: 09.06.2021).

[24] 150 рублей за штуку. Как МТС «сливает» своих клиентов банкам и коллекторам // URL: https://bankiros.ru/news/mts-banki-i-kollektory-2391 (дата обращения: 09.06.2021).

инициативы или согласия гражданина на предоставление сведений. Логичным было бы предположить, что в каждом конкретном случае из цифрового профиля должны предоставляться только сведения, минимально необходимые для совершения конкретной процедуры, за которой обратился субъект, или для заключения конкретного договора. Однако вполне вероятно, что организации — пользователи инфраструктуры будут строить взаимодействие с клиентами таким образом, чтобы получать от них согласие на доступ к максимальному объему сведений из цифрового профиля. В отсутствие специального законодательного регулирования они постараются использовать для этого весь арсенал методов, от навязывания услуг, требующих предоставления дополнительной информации, до особого структурирования пользовательских интерфейсов на сайтах, «заставляющих» граждан соглашаться на предоставление заведомо большего объема данных (например, если на странице, где гражданин заполняет заявление, по умолчанию будут предварительно проставлены галочки в чекбоксах напротив всех возможных видов данных в расчете на то, что далеко не каждый пользователь проверит этот перечень и снимет лишние галочки).

Отсутствие правовой определенности в этом вопросе может привести к тому, что у банков, операторов связи и других частных структур окажутся чрезмерно большие наборы данных о гражданах (в том числе такие сведения, которые человек не стал бы предоставлять, если бы заполнял заявления или договоры традиционным способом, без обращения к цифровому профилю). Вполне ожидаемо, что эти данные впоследствии будут объединяться с информацией, содержащейся в негосударственных информационных системах, и использоваться для профилирования клиентов в коммерческих целях. Причем, оперируя данными, полученными из цифровых профилей граждан, организации будут ссылаться на то, что доступ к ним был добровольно предоставлен самими субъектами.

Конституционной гарантией, направленной на недопущение чрезмерного расширения состава цифрового профиля гражданина и его использования для целей, несовместимых с правами человека, можно считать конституционный запрет сбора, хранения и использования информации о частной жизни лица без его согласия (ч. 1 ст. 24 Конституции РФ). Однако широкая и довольно пространная трактовка понятия «частная жизнь»[25], как и отсутствие должной правовой регламентации использования персональных данных для целей профилирования, оставляют государству большие возможности для определения того, какие сведения следует относить к сфере частной жизни, а какие нет, а также осуществления сбора и обработки таких сведений под предлогом защиты публичных интересов, например в связи с необходимостью обеспечения национальной безопасности. В результате данные о гражданах могут использоваться государством и частными структурами не только в законных целях, но и, напротив, для нарушения их прав и дискриминации (например, для слежки за представителями политической оппозиции и оказания давления на них).

Часть 3 ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает императивный запрет на объединение баз данных, если содержащиеся в них персональные данные будут обрабатываться в целях, несовместимых между собой. Данная норма при ее буквальном толковании неприменима к цифровому профилю, поскольку сведения, содержащиеся в цифровых профилях граждан, не консолидируются в единую сводную базу данных, а продолжают храниться в различных государственных информационных системах и будут извлекаться из них по мере необходимости. Однако, как верно замечает С. Е. Чаннов, опираясь на более ранние исследования других ученых, «даже если фактически базы данных не объединяются целиком, объем данных, передаваемых в центр персонализации, позволяет считать это их объединением», поскольку результатом в этом случае является одномоментный доступ пользователя к необходимым базам данных, содержащимся в разных информационных системах[26]. Возможность одномоментного доступа к разнообразной ин-

[25] Конституционный Суд РФ определяет частную жизнь как «область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит непротивоправный характер» (определение от 28.06.2012 № 1253-О).

[26] *Чаннов С. Е.* Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. 2018. № 9. С. 50–51.

формации из цифрового профиля гражданина с использованием централизованной инфраструктуры влечет за собой еще один существенный риск: в случае несанкционированного доступа к цифровым профилям злоумышленники смогут завладеть слишком большим объемом данных о субъектах, в том числе получить данные личного характера.

Гарантии прав субъектов при автоматизированной обработке их персональных данных получили отражение на международном уровне — в Конвенции о защите физических лиц при автоматизированной обработке персональных данных[27] (далее — Конвенция). В числе базовых принципов, устанавливаемых Конвенцией, — законная и справедливая основа, наличие законной цели обработки, адекватность и относимость к делу и т. д. Российская Федерация, будучи участником данного международного договора, закрепила указанные принципы в национальном законодательстве, главным образом в Федеральном законе «О персональных данных». В 2018 г. Конвенция подверглась ревизии, обусловленной ростом объема обрабатываемой информации о физических лицах, повышением скорости и удешевлением ее автоматизированной обработки, массовым распространением новых технологий обработки персонализированной информации, в том числе технологии «больших данных», создающей повышенные угрозы неприкосновенности частной жизни человека. В числе нововведений — расширение перечня принципов автоматизированной обработки персональных данных. К названным выше принципам добавляются честность и прозрачность обработки. Несмотря на то что изменения в Конвенцию, внесенные Протоколом от 10.10.2018[28], еще не вступили в силу, их, безусловно, следует принимать во внимание в целях правовой регламентации цифрового профиля.

Необходимо сделать акцент на принципах законной основы и законной цели автоматизированной обработки персональных данных. Они предполагают достаточную правовую определенность в вопросе о том, какие данные, кем, каким образом и в связи с чем подлежат обработке. Однако, как следует из предыдущего анализа, существующее в России регулирование цифрового профиля вряд ли можно назвать соответствующим этому критерию. Складывающаяся ситуация крайне неоднозначна и с точки зрения ч. 3. ст. 55 Конституции РФ, согласно которой любое ограничение прав и свобод человека (а обработка персональной информации о человеке, в том числе ее связывание или объединение в цифровой профиль, бесспорно, является ограничением) допустимо только на основании федерального закона и только для достижения конституционно значимых целей.

3. О гарантиях прав человека в связи с введением цифровых профилей. Таким образом, введение цифровых профилей требует серьезной доработки законодательной базы, прежде всего в части установления гарантий соблюдения прав человека при обработке его персональной информации.

Прежде всего, требуют законодательного закрепления специальные гарантии прав и свобод человека от вероятных негативных последствий связывания персональных данных, имеющихся в распоряжении государства. Эти гарантии должны учитывать не только текущий состав сведений, образующих цифровой профиль, но весь массив государственных данных о гражданах, которые потенциально могут быть включены в их цифровые профили или быть с ними связаны и которые могут использоваться путем автоматизированной обработки для профилирования человека и мониторинга его поведения.

Во-первых, в федеральном законе должны быть закреплены более определенные гарантии неприкосновенности частной жизни человека в связи с введением цифровых профилей в развитие общей нормы, содержащейся в ч. 1 ст. 24 Конституции РФ. В основе содержания этих гарантий должен лежать принцип пропорциональности: в цифровой профиль не должна включаться информация, использование которой способно привести к неоправданному вмешательству государства в сферу частной жизни индивида или создать чрезмерные риски такого вмешательства, а также повысить риски утечки особо «чувствительной» информации о человеке. В частности, должен существовать законодательный запрет на включение в цифровые профили такой информации, как

[27] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28 января 1981 г.) // СПС «КонсультантПлюс».

[28] Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (г. Страсбург, 10 октября 2018 г.) // СПС «КонсультантПлюс».

сведения о фактах записи к врачу или обращения за медицинской помощью, о судимости, о привлечении к административной ответственности, о фактах идентификации или аутентификации лица на сайтах с использованием ЕСИА, о действиях, совершенных им на таких сайтах. Также представляется необходимым определить в законе, какие государственные данные, относящиеся к человеку, в принципе должны продолжить храниться изолированно от других данных и не иметь прямой технологической связанности с ними (например, данные, содержащиеся в государственных системах геномной или дактилоскопической регистрации, данные из систем видеонаблюдения).

Что касается информации, содержащейся в онлайн-чеках, геолокационных данных, цифровых следов и других данных о человеке, непосредственно затрагивающих его частную жизнь, то их хранение в государственных информационных системах и порядок использования нуждаются в законодательном регулировании, гарантирующем сохранение такой информации в тайне и недопустимость ее произвольного использования. Регулирование здесь должно основываться на риск-ориентированном подходе и быть направленным на «ограничение нежелательного воздействия на пользователя, не обусловленного его согласием на использование его персональных данных и иной связанной с ним информации ограниченного доступа»[29]. Решением могло бы быть, например, установление в законе требования хранить такие сведения в обезличенном виде с возможностью деанонимизации информации самим субъектом, к которому она относится, либо на основании судебного решения. Также следует ограничить срок хранения указанной информации. Такой подход уже был применен Судом ЕС, отменившим решением от 08.04.2014 Директиву ЕС 2006/24/ЕС. Суд посчитал незаконным расширенный сбор и долгосрочное хранение метаданных о пользователях — получателях электронных услуг, усмотрев в этом непропорциональное ограничение основополагающих прав граждан[30].

Во-вторых, законодательные гарантии должны быть направлены на однозначное урегулирование вопроса о том, кто и с какими целями может использовать сведения, доступ к которым организован через инфраструктуру цифрового профиля, при этом особый акцент должен быть сделан на гарантиях при осуществлении профилирования субъектов. В числе гарантий должно быть указание в законе на недопустимые цели использования данных, полученных из цифрового профиля. К таким целям следует отнести, в частности, определение политических предпочтений лица, его философских взглядов или религиозных убеждений; получение информации об интимной жизни лица; организацию преследования или дискриминации человека по политическим мотивам или в связи с его убеждениями, расовой или этнической принадлежностью, членством в общественных объединениях, участием в публичных мероприятиях или высказанным мнением.

Ориентиром для закрепления гарантий в связи с профилированием лиц может служить GDPR. Согласно этому документу, субъект данных должен быть проинформирован о наличии профиля и его последствиях. При этом каждый субъект должен иметь право знать и получать сведения в отношении целей, для которых обрабатываются его персональные данные, получателей этих данных, а также логической схемы, значения и последствий любой их автоматизированной обработки, если она основана на профилировании. Если персональные данные обрабатываются в целях адресного маркетинга, субъект должен иметь право на возражение против такой обработки.

Ясное, совершаемое в доступной форме информирование субъектов об использовании их данных, в том числе о возможных последствиях такого использования, приобретает исключительно большое значение. Статья 9 Конвенции в редакции Протокола 2018 г. предусматривает право любого лица получать по запросу в разумные сроки и без излишних задержек или расходов всю доступную информацию об обработанных данных, их происхождении и сроке хранения, а также о причинах обработки данных. До тех пор пока контролер не представит законные основания для обработки персональ-

[29] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики (подготовлена некоммерческой организацией «Фонд развития центра разработки и коммерциализации новых технологий»). М., 2020. С. 17.

[30] См.: Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / под ред. А. С. Дупан (Гутниковой). М. : Издательский дом Высшей школы экономики, 2016. С. 210.

ных данных, лицо вправе заявлять возражения, в том числе по личным причинам, против обработки своих персональных данных. Указанное регулирование направлено на реализацию внесенных в Конвенцию Протоколом 2018 г. новых принципов обработки персональных данных: честности и прозрачности.

В-третьих, посредством законодательного регулирования следует исключить случаи доступа субъектов к избыточному объему сведений о лице, а также установить ответственность для тех, кто, злоупотребляя доверием граждан, будет получать доступ к избыточным сведениям из цифрового профиля или использовать полученные сведения для последующего профилирования без явно выраженного согласия лица. Например, можно установить обязанность организаций при проектировании пользовательских интерфейсов для заполнения заявлений или заключения договоров четко разграничивать данные, предоставление которых является обязательным, и данные, отсутствие которых не является обязательным для совершения испрашиваемого действия. При этом лицо должно быть четко проинформировано, к каким конкретно сведениям из цифрового профиля предоставление доступа не является обязательным. Отсутствие согласия на предоставление доступа к таким данным не должно влечь за собой отказ в рассмотрении его заявления или предоставлении ему услуги или иным образом ставить его в менее выгодное положение в сравнении с теми, кто такое согласие дал.

Отчасти решение данной проблемы предусматривается в проекте федерального закона «О внесении изменения в статью 14.8 Кодекса Российской Федерации об административных правонарушениях», внесенного Правительством РФ в Государственную Думу 1 июня 2021 г. (законопроект № 1184517-7)[31]. Документ предусматривает административную ответственность за неправомерный отказ в заключении договора с потребителем в случае непредоставления им персональных данных, если такие персональные данные не требуются в соответствии с законом. Тем не менее это регулирование носит точечный характер и не решает всего комплекса возникающих в связи с использованием цифрового профиля проблем.

В-четвертых, следует ограничить возможность использования данных, получаемых из цифровых профилей, с любыми другими целями, за исключением тех, ради которых доступ к этим данным был предоставлен, а также использования таких данных в целях профилирования гражданина или в иных коммерческих целях, а также в целях мониторинга его поведения, если согласие на это не было прямо выражено субъектом персональных данных. Указанные ограничения в целом вытекают из существующего регулирования, содержащегося в Федеральном законе «О персональных данных». Тем не менее применительно к профилированию лиц и использованию для обработки персональных данных технологий «больших данных» их необходимо конкретизировать. В частности, согласие на обработку персональных данных для целей профилирования следовало бы получать отдельно, с одновременным информированием гражданина в доступной форме о целях, логической схеме и возможных последствиях профилирования и разъяснением его права на обжалование решения, принятого на основании автоматизированной обработки его данных посредством профилирования. Логические схемы, используемые при профилировании (неважно, осуществляемом ли государством или частными субъектами), должны относиться к общедоступной информации и ни в коем случае не скрываться под режимами государственной или коммерческой тайны. Исключение может составлять профилирование, осуществляемое в рамках оперативно-розыскной и иной правоохранительной деятельности, но и оно должно осуществляться строго в рамках установленных юридических процедур.

В-пятых, за гражданами должна быть в любом случае сохранена возможность совершения любых действий, связанных с реализацией конституционных прав и свобод и получением любых услуг, без обращения к цифровому профилю. Использование цифрового профиля не должно становиться для лица единственным допустимым средством реализации своих прав.

При закреплении в законе гарантий соблюдения прав человека при обработке сведений из его цифрового профиля, в том числе при установлении запретов и ограничений на включение определенной информации в цифровые профили или использование ее с определенными целями, важным представляется установление баланса между интересами граждан, публичными интересами и коммерческими

[31] URL: https://sozd.duma.gov.ru/bill/1184517-7 (дата обращения: 09.06.2021).

интересами негосударственных структур. Очевидно, что и государство, и частные субъекты будут стремиться извлечь максимальную выгоду от доступа к информации персонального характера. Обработка такой информации, в том числе ее анализ на основе технологии «больших данных», является существенной частью цифровой экономики и цифрового государственного управления. Правовое регулирование, гарантируя соблюдение прав человека и устанавливая понятные для всех сторон правила использования персональных данных и иной связанной с конкретным человеком информации, в то же время не должно создавать неоправданные барьеры для операторов, делать всякое использование ими такой персонализированной информации невозможным или крайне затруднительным.

БИБЛИОГРАФИЯ

1. *Афанасьев С. Д.* Формирование национальной системы управления данными: конституционно-правовые аспекты // Конституционное и муниципальное право. — 2019. — № 12. — С. 9–14.
2. *Жарова А. К.* Вопросы обеспечения безопасности цифрового профиля человека // Юрист. — 2020. — № 3. — С. 55–61.
3. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / под ред. А. С. Дупан (Гутниковой). — М. : Издательский дом Высшей школы экономики, 2016. — 344 с.
4. *Петров А. А.* Китайский цифровой профиль или скоринговая система социального доверия // Chronos. — 2020. — № 8. — С. 11–24.
5. *Савельев А. И.* На пути к концепции регулирования данных в условиях цифровой экономики // Закон. — 2019. — № 4. — С. 174–195.
6. *Савельев А. И.* Проблемы применения законодательства о персональных данных в эпоху «больших данных» (big data) // Право. Журнал Высшей школы экономики. — 2015. — № 1. — С. 43–66.
7. *Солдатова В. И.* Защита персональных данных в условиях применения цифровых технологий // Lex russica. — 2020. — № 2. — С. 33–43.
8. *Талапина Э. В.* Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права Российской академии наук. — 2018. — Т. 13. — № 5. — С. 117–150.
9. *Чаннов С. Е.* Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. — 2018. — № 9. — С. 48–54.

Материал поступил в редакцию 10 июня 2021 г.

REFERENCES

1. Afanasyev SD. Formirovanie natsionalnoy sistemy upravleniya dannymi: konstitutsionno-pravovye aspekty [Formation of a national data management system: Constitutional and legal aspects]. *Konstitutsionnoe i munitsipalnoe pravo [Constitutional and municipal law].* 2019;12:9-14. (In Russ.)
2. Zharova AK. Voprosy obespecheniya bezopasnosti tsifrovogo profilya cheloveka [Questions of ensuring the security of a person's digital profile]. *Yurist [Lawyer].* 2020;3:55-61. (In Russ.)
3. Dupman (Gutnikova) AS, editor. Novaya paradigma zashchity i upravleniya personalnymi dannymi v Rossiyskoy Federatsii i zarubezhnykh stranakh v usloviyakh razvitiya sistem obrabotki dannykh v seti Internet [A new paradigm of personal data protection and management in the Russian Federation and foreign countries in the context of the development of data processing systems on the Internet]. Moscow: Higher School of Economics Publishing House; 2016. (In Russ.)
4. Petrov AA. Kitayskiy tsifrovoy profil ili skoringovaya sistema sotsialnogo doveriya [Chinese digital profile or scoring system of social trust]. *Chronos*. 2020;8:11-24. (In Russ.)
5. Savelev AI. Na puti k kontseptsii regulirovaniya dannykh v usloviyakh tsifrovoy ekonomiki [Towards the concept of data regulation in the digital economy]. *Zakon [Law].* 2019;4:174-195. (In Russ.)

6. Savelev AI. Problemy primeneniya zakonodatelstva o personalnykh dannykh v epokhu «bolshikh dannykh» (big data) [Problems of application of the legislation on personal data in the era of "big data" (big data)]. *Pravo. Zhurnal Vysshey shkoly ekonomiki [Law. Journal of the Higher School of Economics]*. 2015;1:43-66. (In Russ.)
7. Soldatova VI. Zashchita personalnykh dannykh v usloviyakh primeneniya tsifrovykh tekhnologiy [Protection of Personal Data in Digital Environment]. *Lex Russica*. 2020;1(2):33-43. (In Russ.)
8. Talapina EV. Zashchita personalnykh dannykh v tsifrovuyu epokhu: rossiyskoe pravo v evropeyskom kontekste [Personal data protection in the digital age: Russian Law in the European context*]. Trudy Instituta gosudarstva i prava Rossiyskoy akademii nauk*. 2018;13(5):117-150. (In Russ.)
9. Channov SE. Pravovye ugrozy pri ispolzovanii informatsionnykh sistem v gosudarstvennom upravlenii [Legal threats in the use of information systems in public administration]. *Administrativnoe pravo i protsess [Administrative law and procedure]*. 2018;9:48-54. (In Russ.)