УДК 004.91
DOI 10.33764/2618-981X-2022-6-197-203

Организация защиты персональных данных в государственных и муниципальных информационных системах

О. А. Поликанина[1], А. Н. Поликанин[1], А. В. Шабурова[1]*
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Polikanina-OA2021@sgugit.ru

Аннотация. На сегодняшний день проблема утечки персональных данных из государственных и муниципальных информационных систем является актуальной и, по мнению авторов, связана с тем, что в информационных системах органов власти общедоступные сведения и сведения ограниченного доступа не разграничены между собой техническими и организационными средствами защиты. В определенных жизненных ситуациях сведения ограниченного доступа могут быть выданы ненадлежащим лицам вместе с общедоступными данными. Решение данной проблемы необходимо начать с установления классификации персональных данных в зависимости от степени тяжести ущерба, который может быть нанесен гражданину, вследствие распространения указанных сведений. В статье авторы предлагают выделить следующие категории персональных данных: «открытые», «ограниченного доступа», «закрытые» в зависимости от необходимой степени их защиты.

Ключевые слова: персональные данные, государственные и муниципальные информационные системы, сведения ограниченного доступа

Organization of personal data protection in state and municipal information systems

O. A. Polikanina[1], A. N. Polikanin[1], A. V. Shaburova[1]*
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: polikanina-olga@yandex.ru

Abstract. Today the problem of leakage of personal data from state and municipal information systems is relevant and, according to the authors, is related to the fact that in the information systems of authorities, publicly available information and restricted access information are not differentiated between each other by technical and organizational means of protection. In certain life situations, restricted access information may be issued by an improper person together with publicly available data. The solution to this problem should begin with the establishment of a classification of personal data depending on the severity of the damage that may be inflicted on a citizen as a result of the dissemination of this information. In the article, the authors propose to distinguish the following categories of personal data: "open", "restricted access", "closed", depending on the necessary degree of their protection.

Keywords: personal data, state and municipal information systems, restricted access information

Введение

По данным компании SearchInform увеличение количества инцидентов, связанных с утечкой персональных данных (далее – ПДн), с 2017 по 2019 г.г. составило порядка 20-23 % ежегодно [1, 2, 3]. В 2020 г. данный показатель вырос до

33 %. Проведенные компанией SearchInform исследования в 2020 –2021 г.г. говорят о том, что основная доля таких утечек 38-40 % приходится на государственные и муниципальные структуры, которые обрабатывают огромные массивы достоверных, документально подтвержденных ПДн. Согласно исследованиям компании SearchInform отмечено стабильное увеличение из года в год слива (утечки) ПДн из баз данных (дата-цетров) информационных систем органов государственной власти и органов местного самоуправления [4,5].

К ПДн относится любая личная информация, которая позволяет идентифицировать субъекта. Сам термин не является новым, вместе с тем развитие сетей связи и автоматизированной обработки данных с использованием информационных систем позволили централизованно собирать, обрабатывать, передавать большие массивы ПДн. Потери ПДн нередки в работе организаций, в том числе государственных и муниципальных органов власти, осуществляющих обработку таких данных (далее – Операторы ПДн), и зачастую связаны с недобросовестным отношением к защите ПДн.

В этой связи вопросы безопасности обработки и защиты ПДн приобретают все более острый характер, ведь злоумышленники с помощью ПДн могут выследить человека, спланировать преступление против него, выдать себя за другое лицо, совершить посягательство на личную жизнь либо имущество, совершить иное противоправное деяние.

В группе риска оказываются ПДн, обрабатываемые в государственных и муниципальных информационных системах, поскольку при обращении в органы власти, например, для регистрации прав на недвижимое имущество субъект предоставляет данные строго в соответствии с документами (ФИО, СНИЛС, дата рождения, паспортные данные, адрес регистрации и т.д.). В связи с этим остро встает вопрос гарантий со стороны государства обеспечения доступности, целостности и конфиденциальности обрабатываемых ПДн.

Классификация персональных данных

В России отношения в области ПДн регулируются Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – «Закон о ПДн») [6], Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым Кодексом РФ, Приказами ФСБ, ФСТЭК России, Роскомнадзора, другими нормативными актами, которые накладывают правила, ограничения и запреты на обработку ПДн и имеют нюансы, разобраться в которых бывает не просто даже опытному специалисту. Операторы ПДн часто по-разному интерпретируют данный закон, содержащий общие формулировки, включая само понятие ПДн.

По мнению компании SearchInform, одной из причин сложившейся ситуации является отсутствие конкретного перечня ПДн, так как в 2006 г. при разработке «Закона о ПДн» данное направление было малоизученным, количество ПДн, предоставляемых гражданами, незначительным и составляло небольшой поток данных, поэтому законодатель не был озабочен вопросами категорирования ПДн, что оставило простор для их толкования.

Проанализировав «Закон о ПДн» (в редакции от 01.03.2021), установлено, что в настоящее время в нем выделены только специальные категории ПДн и биометрические ПДн. Первые касаются национальной принадлежности, политических, религиозных взглядов, здоровья. Вторые характеризуют биологические и физиологические особенности человека, на основе которых можно установить его личность. Закон все больше уходит в сторону того, что ответственность за ПДн перекладываются на субъекта, который сам принимает решение и дает согласие на их обработку, и Оператора ПДн, который должен обеспечить необходимую защиту ПДн.

Требования по защите ПДн при обработке в информационных системах (далее – ИСПДн) определены постановлением Правительства РФ от 01.11.2012 №1119 [7]. Уровень защищенности ПДн устанавливается в зависимости от типа угроз и категории ПДн, которые обрабатываются в информационной системе: специальные категории ПДн; биометрические ПДн; общедоступные ПДн, полученные из общедоступных источников ПДн; иные категории ПДн.

Вместе с тем понятие «общедоступные» ПДн исключено из «Закона о ПДн» еще в 2011 году. С 01.03.2021 введено понятие ПДн, разрешенные субъектом ПДн для распространения неограниченному кругу лиц. «Иные» категории ПДн вообще не раскрываются в законе, государство не берет на себя обязательства проработать вопросы их категорирования и защиты.

Одновременно в законе выделены особенности обработки ПДн в государственных и муниципальных ИСПДн. В таких системах могут быть установлены особенности учета ПДн, в том числе с использованием различных способов обозначения принадлежности ПДн к конкретному субъекту.

В случае отзыва субъектом согласия на обработку ПДн органы государственной власти и местного самоуправления вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, когда обработка ПДн необходима для исполнения полномочий таких органов. Следовательно, ответственность за сохранение и безопасность ПДн, обрабатываемых в государственных и муниципальных ИСПДн, несут непосредственно сами органы власти и их должностные лица, государственные и муниципальные служащие.

Проведенный анализ показывает, что классификация ПДн в зависимости от степени важности и обеспечения безопасности закреплена на законодательном уровне в общем, так сказать, «крупными мазками». Для установления категорий ПДн проведем аналогию с разграничением секретных сведений в Законе РФ от 21.07.1993 №5485-1 «О государственной тайне» (далее – «Закон о гостайне») [8].

В связи с государственной значимостью в «Законе о гостайне» дан подробный перечень и основания отнесения сведений к государственной тайне, целый раздел посвящен защите государственной тайны (органы защиты, организация допуска, ответственность и т.п). Самое главное в законе закреплены степени секретности сведений: «особой важности», «совершенно секретно», «секретно» в зависимости от степени тяжести ущерба, который может быть нанесен безопасности страны в результате распространения таких сведений. Сведения «особой важности» имеют более высокую степень допуска к ним должностных лиц, более

жесткие запреты и ограничения при работе с такими сведениями и требуют максимальных затрат на их охрану. Сведения «секретно» имеют меньше ограничений по допуску, таким образом, ресурсов на их охрану затрачивается меньше. Больше людей допускаются к нижнему уровню секретности, и, соответственно, меньше к высшему уровню.

Поскольку структура ПДн разнородна и нет смысла защищать все данные одинаково деление ПДн на категории в зависимости от степени тяжести возможного ущерба для гражданина в результате их распространения позволит по разному организовать защиту ПДн.

Анализ ведомственных нормативных актов, включая Федеральный закон от 13.07.2015 №218-ФЗ «О государственной регистрации недвижимости» (далее – «Закон о недвижимости») [9, 10], показывает, что в информационной системе органа регистрации прав хранятся, обрабатываются и передаются одновременно общедоступные сведения, сведения ограниченного доступа (конфиденциальные) и закрытые (запрещенные для выдачи) сведения о правообладателях и объектах недвижимого имущества на всей территории РФ.

Проблема категорирования ПДн является актуальной для государственной информационной системы регистрации недвижимого имущества, в связи с этим, предлагаем установить три категории ПДн в зависимости от степени тяжести ущерба и необходимой степени их защиты: «открытые», «ограниченного доступа», «закрытые».

К «открытым» предлагается отнести общедоступные ПДн, которые предоставляются по запросам любых лиц и подлежат открытому опубликованию на сайте ведомства в сети Интернет. «Открытые» данные представляются интернет порталами различных систем власти в общий доступ для дальнейшей обработки в информационных системах, следовательно, общедоступные сведения должны иметь минимальный уровень защиты в ИСПДн.

К сведениям «ограниченного доступа» предлагается отнести конфиденциальные ПДн, которые предоставляются по запросам законодательно определенных лиц. Утечка таких данных может нанести крупный материальный либо моральный ущерб гражданину. Такие сведения должны иметь более высокий уровень защиты, доступ к ним может иметь ограниченный круг лиц в организации с установленной формой, порядком доступа и персональной ответственностью за утечку данных.

К «закрытым» предлагается отнести ПДн лиц, подлежащих государственной защите, и их близких, в отношении которых принято решение о наложении запрета на выдачу сведений согласно Федеральному закону от 20.04.1995 №45-ФЗ. Обработка «закрытых» ПДн потребует от организации обеспечения максимальной, в том числе криптографической защиты, установления ответственности вплоть до уголовной в случае утечки «закрытых» ПДн и степени ущерба, понесенного субъектом.

Предлагаемые категории ПДн сопоставлены с категориями сведений, разграниченными в «Законе о недвижимости», и со степенями секретности, установленными «Законом о гостайне» (табл. 1).

Таблица 1

Категории персональных данных

Категории ПДн «Закон о ПДн»	Категории сведений «Закон о недвижимости»	Степени секретности «Закон о гостайне»
«Открытые» (общедоступные)	Общедоступные сведения, в том числе размещаемые на официальном сайте для просмотра неограниченным кругом лиц	«Секретно»
«Ограниченного доступа» (специальные, биометрические)	Сведений, доступ к которым ограничен ч.13 ст. 62 «Закона о недвижимости»	«Совершенно секретно»
«Закрытые»	Сведения о лицах, подлежащих государственной защите, выдача которых запрещена ч. 1.2 ст. 62 «Закона о недвижимости»	«Особой важности»

В дальнейшем деление ПДн на категории позволит осуществить рациональный подход к организации защиты ПДн, установить необходимые уровни защищенности ПДн при их обработке, выбрать обоснованные меры и средства защиты информации для каждого уровня и обеспечить защиту данных, в том числе от утечки.

Результаты

Учитывая, что современные базы данных хранятся на серверах, которые размещаются в центрах обработки данных, для реализации дифференцированного подхода к разным категориям ПДн должен предоставляться доступ разной степени защиты.

Поскольку «открытые» сведения являются общедоступными, то к ним, соответственно, должны применяться минимальные требования по защите. Для получения доступа к «открытым» данным пользователю достаточно пройти идентификацию по логину и паролю.

Для защиты сведений «ограниченного доступа» (ОД) должны применяться более жесткие организационные и технические меры. Например, кодирование конфиденциальных данных. Доступ к сведениям с кодом ОД должен быть привязан к биометрическим данным пользователя и осуществляться с использованием биометрического идентификатора путем запроса и проверки идентификатора биометрических данных исполнителя. Компьютер должен иметь защищенный канал связи биометрики, чтобы злоумышленник не имел возможности перехватить биометрические данные и воспользоваться ими для получения доступа к сведениям «ограниченного доступа».

«Закрытые» сведения также вносятся в базу данных с присвоением установленного кода ЗД. Кроме биометрического терминала для идентификации пользователей, имеющих доступ к сведениям с кодом ЗД, потребуются дополнительные меры защиты к помещению и компьютеру, на котором будет осуществляться

обработка таких данных, а также специальный канал с криптографической защитой передачи данных (шифрование данных при передаче).

В числе организационных мер следует регламентировать порядок доступа в организации к сведениям с кодами ОД и ЗД. Определить должностных лиц, имеющих специальный допуск и несущих персональную ответственность, а также установленную на законодательном уровне гражданско-правовую, административную, уголовную ответственность за разглашение, ненадлежащее предоставление либо нарушение требований по защите ПДн, отнесенных к сведениям «ограниченного доступа» и «закрытым» сведениям, включая утечку (слив) таких данных. В качестве компенсирующих мер работникам должна быть установлена надбавка, иные привилегии за обработку особых категорий персональных данных.

Заключение

На сегодняшний день государственные и муниципальные органы, действуя как Операторы ПДн, обнаруживают невысокую компетенцию в вопросах организации защиты ПДн. По информации Роскомнадзора, государственные и муниципальные учреждения часто нарушают права субъектов ПДн, что подтверждается в ходе проверок и косвенно свидетельствует о дефиците компетентных специалистов.

Правильно построенный процесс обработки данных является гарантом безопасности персональных данных, составляющих основу частной жизни граждан, репутации и личной безопасности.

Деление ПДн на категории позволит не защищать все данные одинаково, так как это требует огромных ресурсов и повышает риск утечки информации, а применять различные организационные и технические меры защиты информации в государственных и муниципальных ИСПДн в зависимости от установленной категорий ПДн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 2017: Исследование уровня информационной безопасности российских компаний [Электронный ресурс] / SearchInform. – Электрон. дан. – М., 2022. – Режим доступа : https://searchinform.ru/research-2017/.

2. Исследование уровня информационной безопасности в компаниях России и мира за 2018 год [Электронный ресурс] / SearchInform. – Электрон. дан. – М., 2022. – Режим доступа : https://searchinform.ru/research-2018/.

3. Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год [Электронный ресурс] / SearchInform. – Электрон. дан. – М., 2022. – Режим доступа : https://searchinform.ru/research-2019/.

4. Глобальное исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год [Электронный ресурс] / SearchInform. – Электрон. дан. – М., 2022. – Режим доступа : https://searchinform.ru/survey/global-2020/.

5. Глобальное исследование уровня информационной безопасности в компаниях России и СНГ за 2021 год [Электронный ресурс] / SearchInform. – Электрон. дан. – М., 2022. – Режим доступа : https://searchinform.ru/survey/global-2021/.

6. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».

7. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : постановление Правительства Рос. Федерации от 01.11.2012 № 1119. – Доступ из справ.-правовой системы «КонсультантПлюс».

8. О государственной тайне [Электронный ресурс] : федер. закон от 21.07.1993 № 5485-1. – Доступ из справ.-правовой системы «КонсультантПлюс».

9. О государственной регистрации недвижимости [Электронный ресурс] : федер. закон от 13.07.2015 № 218-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об установлении порядка предоставления сведений Единого государственного реестра недвижимости и порядка уведомления заявителей о ходе оказания услуги по предоставлению сведений, содержащихся в Едином государственном реестре недвижимости [Электронный ресурс] : Приказ Федеральной службы государственной регистрации, кадастра и картографии от 08.04.2021 № П/0149. – Доступ из справ.-правовой системы «КонсультантПлюс».