

О. А. Поликанина¹, А. Н. Поликанин¹ А. В. Шабурова¹*

Методический подход для организации разграничений доступа к сведениям в информационной системе персональных данных

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

* e-mail: Polikanina-OA2021@sgugit.ru

Аннотация. С 01 марта 2023 года вступили в силу изменения в Федеральный закон от 13.07.2015 №218-ФЗ «О государственной регистрации недвижимости» в части защиты персональных данных. Вопросы доступности, целостности и конфиденциальности персональных данных, обрабатываемых в информационной системе, становятся все более актуальными. В настоящее время общедоступные сведения и сведения ограниченного доступа, в том числе персональные данные, не разграничены между собой техническими и организационными средствами защиты. В статье авторы предлагают организовать защиту данных в зависимости от категории: «открытые», «ограниченного доступа», «закрытые». Деление на категории осуществляется в зависимости от степени тяжести ущерба, который может быть нанесен субъекту, в результате распространения сведений. Такой подход позволит избежать применения избыточных мер защиты «открытых» данных, вместе с тем организация защиты сведений ограниченного доступа потребует больших затрат, при этом количество пользователей, допущенных к обработке, будет значительно меньше.

Ключевые слова: персональные данные, информационная система персональных данных, сведения ограниченного доступа, разграничение прав доступа

О. А. Polikanina¹, А. N. Polikanin¹, А. V. Shaburova¹*

Methodical Approach to Organize Access to Information in the Personal Data Information System

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: polikanina-olga@yandex.ru

Abstract. On March 1, 2023, amendments to the Federal Law of July 13, 2015 № 218-FZ “On State Registration of Real Estate” came into force regarding the protection of personal data. The issues of availability, integrity and confidentiality of personal data processed in the state information system are becoming more and more relevant. At present, public and restricted information, including personal data, is not separated from each other by technical and organizational means of protection. In the article, the authors propose to organize data protection depending on the category: “open”, “limited access”, “closed”. The division into categories is carried out depending on the severity of the damage that can be inflicted on the subject as a result of the dissemination of information. This approach will avoid the use of excessive measures to protect "open" data, however, the organization of the protection of restricted access information will be expensive, while the number of users allowed for processing will be much smaller.

Keywords: personal data, the personal data information system, restricted access information, access rights differentiation

Введение

С 01 марта 2023 года вступили в силу изменения в Федеральный закон от 13.07.2015 №218-ФЗ «О государственной регистрации недвижимости» (далее – Закон о недвижимости) в части защиты персональных данных (далее – ПДн).

Закон о недвижимости дополнен статьей 36.3 Правила внесения в государственный реестр недвижимости (далее – реестр недвижимости) записи о возможности предоставления ПДн правообладателя объекта недвижимости. ПДн владельца недвижимости (фамилия, имя, отчество, дата рождения) могут быть предоставлены третьим лицам только при наличии *согласия* правообладателя или лица, в пользу которого зарегистрированы ограничения права (обременения) объекта недвижимости.

Вместе с тем частью 6 статьи 36.3 Закон о недвижимости предусмотрено, что ПДн гражданина, независимо от наличия записи о возможности их предоставления, указываются в Выписке из реестра недвижимости по запросам нотариусов, правоохранительных органов, судебных приставов, арбитражных управляющих, судов, залогодержателей, иных лиц, указанных в законе [1].

В этой связи вопросы обеспечения доступности, целостности и конфиденциальности сведений, обрабатываемых в информационной системе персональных данных (далее – ИСПДн) Росреестра имеют большое практическое значение и становятся всё более актуальными [2].

В настоящее время все сведения реестра недвижимости защищаются одинаково, при этом при предоставлении сведений ограниченного доступа возникают ошибки информационной системы либо конкретного исполнителя, которые приводят к негативным последствиям, одним из которых является утечка ПДн в госсекторе [3,4,5].

Целью исследования является выработка методического подхода для организации разграничений доступа к сведениям в ИСПДн в зависимости от установленной категории данных. Для достижения поставленной цели в статье решены следующие задачи:

- проанализирован существующий порядок доступа к сведениям в ИСПДн;
- выполнена классификация данных, обрабатываемых в ИСПДн;
- выработан авторский подход к разграничению прав доступа к сведениям в ИСПДн в зависимости от категории обрабатываемых данных и должности исполнителя.

Методы и материалы

Законом о недвижимости установлено, что сведения реестра недвижимости предоставляются по запросам любых лиц и подлежат размещению на официальном сайте ведомства [6], за исключением сведений, доступ к которым ограничен федеральным законом, к таким сведениям относятся ПДн правообладателя объекта недвижимости.

В случае принятия решения о наложении запрета на выдачу сведений о защищаемых лицах и их близких, объектах государственной охраны и членах их семей сведения о таких лицах не предоставляются, за исключением случаев, предусмотренных федеральными законами либо указом Президента РФ [1].

Таким образом, законодательно сведения реестра недвижимости разделены на три группы: общедоступные, имеющие ограниченный доступ и запрещенные для выдачи.

В настоящее время порядок доступа к сведениям в ИСПДн не разграничен, пользователи с ролью Предоставление сведений имеют равный доступ ко всем данным. Авторизация пользователей при входе в ИСПДн осуществляется по паре логин/пароль или с использованием электронной подписи (далее – ЭП), что не гарантирует 100% достоверную идентификацию должностного лица. Иными словами, зная логин и пароль либо имея доступ к ЭП, любой сотрудник может войти в систему и получить доступ к информации, включая ПДн правообладателей объектов недвижимости.

Кроме того, пользователи с ролью Предоставление сведений технически могут формировать для выдачи любые сведения, как общедоступные, так и конфиденциальные, при этом сведения автоматически удостоверяются ЭП организации, а не конкретного должностного лица.

Обработка данных осуществляется в одинаковых условиях (помещениях) с использованием компьютеров, оснащенных одними и теми же техническими средствами защиты. Особая организация рабочих мест специалистов, обрабатывающих конфиденциальную информацию и запрещенные для выдачи сведения, отсутствует.

Существующий порядок доступа пользователей к сведениям в ИСПДн Росреестра представлен в табл. 1.

Таблица 1

Порядок доступа пользователей к сведениям в ИСПДн

Организация доступа пользователя	Общедоступные сведения	Сведения, ограниченного доступа	Сведения, на которые наложен запрет
Создание учетной записи (регистрация пользователя в системе)	+	+	+
Настройка ролей	+	+	+
Вход в систему Логин/пароль	+	+	+
Вход в систему ЭП на съемном носителе	+	+	+
Биометрическая идентификация			
Выделенное защищенное помещение			
Аттестованное АРМ пользователя			
Поиск запрашиваемой информации в БД только открытые данные	+	+	+
Поиск запрашиваемой информации в БД, включая сведения ограниченного доступа	+	+	+
Поиск запрашиваемой информации в БД, включая закрытые данные	+	+	+
Идентификация субъекта на получение запрашиваемых сведений		+	+
Предоставление сведений удостоверенных обезличенной ЭП организации	+	+	+

Организация доступа пользователя	Общедоступные сведения	Сведения, ограниченного доступа	Сведения, на которые наложен запрет
Предоставление сведений удостоверенных ЭП исполнителя			
Передача данных по защищенному каналу (криптографическому)	+	+	+

Таким образом, существующий порядок доступа в ИСПДн обеспечивает сотрудникам с ролью Предоставление сведений одинаковые права на просмотр, обработку и выдачу любых сведений реестра недвижимости, включая ПДн правообладателей объектов недвижимости.

Результаты

В связи с вступлением в силу Федерального закона от 14.07.2022 №266-ФЗ о внесении изменений в Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» [7] ПДн правообладателя объекта недвижимости исключены из общедоступных сведений, предоставляемых ранее по запросам любых лиц, следовательно, меры по защите ПДн должны быть усилены.

В предыдущих публикациях авторами было предложено разделить сведения реестра недвижимости на три категории: «открытые», «ограниченного доступа» и «закрытые» в зависимости от степени тяжести ущерба, который может быть нанесен субъекту в результате утечки данных [8].

Для дальнейшей организации защиты данных в зависимости от категории в первую очередь необходимо определить круг лиц, имеющих доступ к разным категориям сведений, в соответствии с занимаемой должностью. К «закрытым» сведениям разрешить доступ лиц не ниже начальника структурного подразделения. К сведениям «ограниченного доступа» могут быть допущены заместитель начальника и ведущие специалисты отдела. «Открытые» сведения доступны всем сотрудникам.

Авторский подход к разграничению прав доступа в зависимости от категории сведений и занимаемой должности представлен в табл. 2.

Таблица 2

Группы разграничения доступа

Должность	Шт. ед.	Открытые	Ограниченного доступа	Закрытые
Директор	1	+	+	+
Заместитель директора	1	+	+	+
Начальник отдела	1	+	+	+
Зам. начальника отдела	1	+	+	
Ведущий инженер	5	+	+	
Инженер 1 категории	4	+		
Инженер 2 категории	4	+		

Таким образом, чем выше уровень закрытости сведений, тем меньше сотрудников в организации должны быть допущены к их обработке, при этом персональная ответственность и занимаемая должность должны быть выше у лиц, осуществляющих обработку конфиденциальной информации, в том числе ПДн правообладателей объектов недвижимости.

Опираясь на авторский подход для организации разграничений доступа к сведениям, исходя из занимаемой должности, немало важным фактором является предложенное деление сведений на 3 категории: «открытые», «ограниченного доступа» и «закрытые».

Используя метод системного исследования функций объекта с целью поиска баланса между затратами и эффективностью [9], предлагаем доступ пользователей в ИСПДн разграничить по категориям сведений, предусмотрев дополнительные меры защиты при работе с конфиденциальными данными.

В целях достоверного распознавания должностного лица, имеющего права на работу со сведениями «ограниченного доступа» и/или «закрытыми», для входа в ИСПДн дополнительно применять биометрическую идентификацию и аутентификацию пользователя. Автоматизированное рабочее место пользователя необходимо обеспечить средствами защиты конфиденциальной информации от несанкционированного доступа. Проход в помещение, в котором ведется обработка ПДн, предоставить исключительно лицам, допущенным к работе со сведениями ограниченного доступа.

Поскольку Законом о недвижимости установлен круг лиц, которым могут быть предоставлены сведения «ограниченного доступа», исполнитель должен лично проверять полномочия заявителя, нести персональную ответственность за выдачу сведений надлежащему лицу, заверяя их своей ЭП.

Обработка «закрытых» данных должна осуществляться в специально оборудованном помещении на аттестованном компьютере, оснащенный средствами криптографической защиты. Доступ к «закрытым» данным должны иметь минимальное количество должностных лиц.

Предлагаемый подход к организации разграничений доступа к сведениям в ИСПДн Росреестра представлен в табл. 3.

Таблица 3

Организация разграничений доступа пользователей в ИСПДн
в зависимости от категории данных

Организация доступа пользователя	Откры- тые	Ограниченного до- ступа	Закры- тые
Создание учетной записи	+	+	+
Настройка ролей	+	+	+
Вход в систему Логин/пароль	+		
Вход в систему ЭП на съемном носителях		+	+
Биометрическая идентификация		+	+
Выделенное защищенное помещение			+
Аттестованное АРМ пользователя			+

Организация доступа пользователя	Откры- тые	Ограниченного до- ступа	Закры- тые
Поиск запрашиваемой информации в БД только открытые данные	+	+	+
Поиск запрашиваемой информации в БД, включая сведения ограниченного доступа		+	+
Поиск запрашиваемой информации в БД, включая закрытые данные			+
Идентификация субъекта на получение запрашиваемых сведений		+	+
Предоставление сведений удостоверенных обезличенной ЭП организации	+		
Предоставление сведений удостоверенных ЭП исполнителя		+	+
Передача данных по защищенному каналу (криптографическому)		+	+

Предлагаемый подход к организации доступа в ИСПДн в зависимости от категории сведений позволит разграничить меры защиты информации и повысить эффективность защиты сведений ограниченного доступа, включая ПДн, обеспечив дополнительные организационно-технических мероприятий и персональную ответственность сотрудников за утечку данных, при этом количество пользователей, допущенных к обработке конфиденциальной информации, число автоматизированных рабочих мест и помещений, требующих применения дорогостоящих средств защиты, будет минимальным.

Заключение

Организация защиты данных реестра недвижимости в зависимости от установленной категории сведений: «открытые», «ограниченного доступа», «закрытые» имеет большое практическое значение и позволит:

1) избежать применения избыточных организационных мер и технических средств защиты «открытых» данных, доступ к которым имеет максимальное количество пользователей в организации, разрешенных для опубликования на официальном сайте ведомства, так как утечка таких сведений может нанести минимальный ущерб гражданину, юридическому лицу либо государству;

2) разрешить доступ к конфиденциальным данным должностным лицам, начиная от ведущего специалиста и выше, сократив количество пользователей, допущенных к обработке, поскольку организация защиты таких сведений потребует дополнительных мер, включая биометрическую идентификацию пользователей и больших затрат, а исполнители будут нести персональную ответственность за ненадлежащее предоставление и утечку сведений, включая ПДн правообладателей;

3) ограничить доступ к «закрытым» данным, разрешив их обработку минимальному числу лиц в организации, начиная от начальника структурного подразделения и выше, так как для организации защиты потребуется специально выделенное помещение с аттестованным АРМ пользователя, а в случае утечки «за-

крытых» данных должностные лица могут быть привлечены к ответственности вплоть до уголовной в зависимости от степени причиненного ущерба [10, 11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О государственной регистрации недвижимости [Электронный ресурс] : федер. закон от 13.07.2015 № 218-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
2. 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».
3. Исследование уровня информационной безопасности в компаниях России за 2022 год [Электронный ресурс] // SearchInform: [сайт]. [2023]. URL: <https://searchinform.ru/survey/global-2022/> (дата обращения 10.05.2023).
4. Исследование осведомленности и отношения государственных служащих к проблемам защиты персональных данных [Электронный ресурс] // SearchInform: [сайт]. [2022]. URL: <https://searchinform.ru/survey/zaschita-persdannyh-v-gossektore-2021/> (дата обращения 10.05.2023).
5. Глобальное исследование уровня информационной безопасности в компаниях России и СНГ за 2021 год [Электронный ресурс] // SearchInform: [сайт]. [2021]. URL: <https://searchinform.ru/survey/global-2021/> (дата обращения 10.05.2023).
6. Об установлении состава сведений, содержащихся в Едином государственном реестре недвижимости, подлежащих размещению на официальном сайте Федеральной службы государственной регистрации, кадастра и картографии в информационно-телекоммуникационной сети Интернет, и порядка их размещения [Электронный ресурс] : приказ Росреестра от 30.08.2021 № П/0375. Доступ из справ.-правовой системы «КонсультантПлюс».
7. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
8. Поликанина О.А., Поликанин А.Н., Шабурова А.В. Организация защиты персональных данных в государственных и муниципальных информационных системах // Интерэкспо Гео-Сибирь. 2022. Т.6. С. 197–203.
9. Никитина Е. Б. Функционально-стоимостный анализ [Электронный ресурс] : учеб. пособие // Пермский государственный национальный исследовательский университет: [сайт]. [2021]. URL: <http://www.psu.ru/nauka/elektronnye-publikatsii/uchebnye-posobiya-i-metodicheskie-materialy/e-b-nikitina-funktsionalno-stoimostnyj-analiz> (дата обращения 10.05.2023).
10. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Технические, организационные и кадровые аспекты управления информационной безопасностью: учеб. пособие для вузов. М. : Гор. линия–Телеком, 2013. 214 с.
11. Курило А. П., Милославская Н. Г., Сенаторов М. Ю. Основы управления информационной безопасностью : учеб. пособие для вузов. М. : Гор. линия–Телеком, 2013. 244 с.

© О. А. Поликанина, А. Н. Поликанин, А. В. Шабурова, 2023