Информатика

Материалы международной научно-практической конференции «Наука, технологии и информация в библиотеках (LIBWAY-2018)»

УДК 024:004.056
ББК 78.37с
DOI 10.20913/1815-3186-2018-4-101-105

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ «ЦИФРОВОГО» ГРАЖДАНИНА В БИБЛИОТЕКЕ

© З. В. Родионова, Л. К. Бобров, И. П. Медянкина, 2018

Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск, Россия; e-mail: rodionova_z@ngs.ru

В статье анализируются основные аспекты защиты персональных данных в условиях перехода функционирования современной библиотеки в цифровую среду. Представлен алгоритм категорирования информационных систем персональных данных для библиотечной сферы. Выполнен обзор наиболее частых нарушений законодательства в области защиты персональных данных сотрудниками библиотек.

Ключевые слова: персональные данные читателя, информационная система персональных данных библиотеки, цифровая среда, цифровой гражданин, информатизация библиотеки

Для цитирования: *Родионова З. В., Бобров Л. К., Медянкина И. П.* Защита персональных данных «цифрового» гражданина в библиотеке // Библиосфера. 2018. № 4. С. 101–105. DOI: 10.20913/1815-3186-2018-4-101-105.

Personal data protection of a «digital» citizen in a library

Z. V. Rodionova, L. K. Bobrov, I. P. Medyankina

Novosibirsk State University of Economics and Management, Novosibirsk, Russia; e-mail: rodionova_z@ngs.ru

The article analyzes main aspects of personal data protection in the context of modern library transition to the digitized environment. It represents the algorithm of classifying personal data information system in the library sphere. Authors review the most frequent law violation in the field of personal data protection by the library staff.

Keywords: user personal data, personal data of library information system, digital environment, digital citizen, library informatization

Citation: *Rodionova Z. V., Bobrov L. K., Medyankina I. P*. Personal data protection of a «digital» citizen in a library. *Bibliosphere. 2018. № 4. P. 101–105.* DOI: 10.20913/1815-3186-2018-4-101-105.

Благодаря информационным системам у библиотек появилась возможность анализировать информацию о предпочтениях читателя, изучать их роль и место в книжном деле, создавать так называемую «концепцию читателя» [1], что условно может послужить источником информации о личной жизни читателя, его религиозных и философских убеждениях, состоянии здоровья и др. Ситуация усугубляется тем, что процесс трансформации информационных массивов в цифровую форму, а также повсеместная информатизация библиотек превратили и самого читателя в «цифрового» гражданина. Осуществляя обработку сведений о своих читателях и сотрудниках, а именно сбор, систематизацию, накопление, хранение, уточнение и использование персональных данных (ПДн), библиотеки подпадают под действие Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных». Несмотря на то, что отечественное законодательство в области защиты ПДн формируется с 2001 г., многие аспекты его применения до сих пор не учтены, а права граждан продолжают нарушаться, в том числе и в библиотеках. В статье представлены результаты анализа сложившейся ситуации и предложены возможные пути ее решения.

Современные реалии таковы, что все библиотеки Российской Федерации являются операторами ПДн. При предоставлении услуг библиотека, как правило, обрабатывает следующие категории ПДн читателя: фамилия, имя, отчество, дата рождения, адрес, образование, профессия, паспортные данные (серия, номер, дата выдачи, организация, выдавшая паспорт, адрес по месту регистрации), адрес по месту фактического проживания, данные документа об образовании: серия и номер, дата выдачи, наименование образовательного учреждения, квалификация по документу; контактная информация (номер домашнего телефона, номер рабочего телефона, номер мобильного телефона, e-mail). Данный перечень не претендует на полноту и, с точки зрения авторов, будет существенно расширен в ближайшем будущем.

Основные положения защиты персональных данных библиотеки. Анализ развития современных библиотек в информационном пространстве позволяет сделать выводы о том, что ПДн «цифрового» гражданина, как правило, циркулируют в следующих системах, на сервисах и ресурсах:

- автоматизированная библиотечно-информационная система, обеспечивающая комплексную авто-

матизацию библиотечных процессов (комплектование, каталогизацию и систематизацию литературы, создание и ведение электронного каталога и электронных баз данных, учет читателей, библиотечного фонда и др.);

- библиотечный портал;
- библиотечный блог в интернете и группы (сообщества) в социальных сетях;
- «облачные» библиотеки, оказывающие услуги в интернете через облачные технологии и облачные сервисы;
- центр обработки данных (специализированный центр, который обладает мощными программно-техническими и телекоммуникационными возможностями);
- электронная библиотека (информационная система, обеспечивающая создание и хранение документов в электронном виде с возможностью доступа к ним через средства вычислительной техники, в том числе в информационных сетях, например, НЭБ, ИС ЭКБСОН, WDL и др.);
- информационно-телекоммуникационная инфраструктура;
- другие информационные системы, сервисы и ресурсы библиотек.

Как правило, самые большие объемы информации о ПДн «цифрового» гражданина обрабатываются в информационных системах персональных данных (ИСПДн), к которым относятся автоматизированные библиотечные системы (обработка карточки пользователя (читателя)). Наиболее популярными системами этого класса являются ALEPH, LIBER, TINLIB, VTLS, МАРК-SQL, ИРБИС, «1С: Библиотека» и др.

Для определения технических требований по защите персональных данных, обрабатываемых в библиотечных информационных системах (БИС), необходимо установить уровень указанной ИСПДн в соответствии с Постановлением Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119. За исходные значения были приняты следующие средние параметры БИС [2] (таблица).

Согласно упомянутому выше Постановлению Правительства РФ и в соответствии со значениями указанных параметров может быть установлен второй уровень ИСПДн для типовой БИС. Ко второму уровню ИСПДн относятся информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Небольшим библиотекам, менее 100 000 читателей, имеет смысл отказаться от использования фотографий на читательских билетах и проведения видеосъемки, что позволит избежать обработки биометрических ПДн, тем самым понизив уровень ИСПДн библиотеки.

В связи с тем, что БИС, как правило, имеют модульную систему, при категорировании ИСПДн важно учесть тот фактор, что информационной системе в целом присваивается уровень, соответствующий наиболее высокому уровню входящего в нее модуля.

В Постановлении Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119 приведен следующий список требований по организации защиты ИСПДн второго уровня:

1. Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2. Обеспечение сохранности носителей персональных данных.

3. Утверждение руководителем организации оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

Исходные данные для классификации ИСПДн типовой библиотеки

Initial data to classify personal data information systems of a common library

Признак классификации	Значение признака	Примечание
Актуальные угрозы безопасности ПДн	Угрозы второго типа	Наличие актуальных угроз, связанных с присутствием недокументированных (недекларированных) возможностей в прикладном программном обеспечении. На сегодняшний день на рынке программного обеспечения не представлены БИС, имеющие сертификат Федеральной службы по техническому и экспортному контролю об отсутствии недекларированных возможностей
Категория ПДн	Биометрические персональные данные	Использование видеонаблюдений; фотографии в карточке пользователя (читателя)
Число субъектов персональных данных	Любое	В связи с обработкой биометрических персональных данных параметр «число субъектов персональных данных» не влияет на определение уровня защищенности и может быть как более 100 000, так и менее
Обработка ПДн работников	Не ведется	Обработка ПДн сотрудников, как правило, ведется в другой ИСПДн, но бывают исключения (например, Марк SQL)

4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

5. Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

6. Доступ к содержанию электронного журнала сообщений должен быть возможен исключительно для должностных лиц (работников) организации оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Большая часть перечисленных требований относится к организационной защите ПДн и не требует больших финансовых вложений, но временные затраты на поддержание в актуальном состоянии созданной организационной системы защиты будут значительными. Четвертый пункт имеет непосредственное отношение к технической защите, реализация таких защитных механизмов, как правило, дорогостояща и в условиях недостаточного финансирования библиотек практически не осуществима. Детализация требований четвертого пункта приведена в приказе «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. ФСТЭК № 21.

Некоторые БИС предлагают инструменты обезличивания ПДн, которые позволяют существенно сократить затраты на техническую защиту, так как требуется обеспечить безопасность только одной рабочей станции, той, посредством которой происходит дешифровка ПДн. Описанную схему можно реализовать, например, с помощью автоматизированного рабочего места «Центр регистрации читателей» в БИС ИРБИС.

Помимо защиты ПДн, которые обрабатываются в ИСПДн, большое значение имеет организационная защита обработки ПДн без использования средств автоматизации. Основные организационные меры по защите ПДн [3]:

- поддержание в актуальном состоянии информации об операторе ПДн в реестре операторов ПДн Роскомнадзора. Издание приказа о создании комиссии по защите ПДн;
- разработка/поддержание в актуальном состоянии положения об обработке и защите персональных данных (автоматизированный режим обработки или традиционный, на бумажных носителях);
- издание/поддержание в актуальном состоянии приказа руководителя об утверждении списка сотрудников, допущенных к работе с ПДн, и их персональной ответственности за защиту персональных данных;
- сбор согласий на обработку персональных данных с пользователей библиотек (сбор, систематизацию, накопление, хранение, уточнение, использование, обезличивание, блокирование, уничтожение);
- перечень персональных данных пользователей, обрабатываемых библиотекой-оператором (в том числе их категория, объем и сроки хранения);
- внесение изменений в положения о структурных подразделениях, должностные инструкции работников, имеющих отношение к обработке персональных данных;
- внесение изменений в правила пользования библиотекой.

Обзор нарушений законодательства о защите персональных данных сотрудниками библиотеки. Контроль и надзор за выполнением требований по защите ПДн выполняют так называемые регуляторы: Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций), ФСТЭК (Федеральная служба по техническому и экспортному контролю), ФСБ (Федеральная служба безопасности), Прокуратура РФ.

Самые обширные полномочия по контролю и надзору в сфере защиты ПДн имеет Роскомнадзор, который «…обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям Федерального закона “О персональных данных” и принятых в соответствии с ним нормативных правовых актов» (Постановление Правительства РФ «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» от 16 марта 2009 г. № 228).

Основными предметами проверки Роскомнадзора являются: деятельность по обработке ПДн, документы, характер информации в которых предполагает или допускает включение в них ПДн, ИСПДн. В полномочия регулятора входит также

- проверка актуальности информации, указанной в уведомлении об обработке ПДн, которое было передано библиотекой в Роскомнадзор;
- ограничение доступа к ПДн, в случае нарушений законодательства при их обработке;
- обращение в суд с исковыми заявлениями и представление интересов граждан, чьи права в области защиты ПДн были нарушены;
- привлечение к административной ответственности лиц, виновных в нарушении законодательства в области защиты ПДн.

Роскомнадзор осуществляет три вида проверок: плановые, внеплановые и мероприятия систематического наблюдения. Плановые проверки проводятся на основании ежегодного плана, который в обязательном порядке публикуется на сайте регулятора в середине декабря текущего года. С 2009 по 2017 г. было проведено 37 плановых проверок в библиотеках РФ; количество внеплановых проверок на сайте не публикуется и остается неизвестным. Внеплановые проверки проводятся, если истек срок исполнения оператором ранее выданного предписания об устранении выявленного нарушения (обычно после плановой проверки); если в службу поступило обращение от граждан, юридических лиц, индивидуальных предпринимателей о нарушении законодательства в области ПДн; по приказу руководителя Роскомнадзора или руководителя территориального управления.

Как показывают отчеты Роскомнадзора, количество жалоб граждан, а соответственно и внеплановых проверок, существенно растет с каждым годом, например, в 2011 г. в службу поступило 2607 жалоб, в 2017 г. – 36 495 [4]. Самыми масштабными по количеству проверяемых операторов ПДн являются мероприятия систематического наблюдения, которые включают в себя проверку сайта оператора. Так, например, в 2017 г. было проведено 868 плановых проверок, 60 внеплановых и 2129 мероприятий систематического наблюдения [4].

ФСТЭК и ФСБ осуществляют проверку технических аспектов защиты ПДн, ФСБ определяет меры по защите ИСПДн, при использовании в них средств криптографической защиты, а ФСТЭК – меры по всем остальным вопросам обеспечения безопасности. В процессе проведения проверок Роскомнадзор, ФСТЭК и ФСБ вправе привлечь органы прокуратуры в случае такой необходимости.

Рассмотрим наиболее частые нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (и принятых на его основе подзаконных актов), которые допускают библиотеки.

По данным Роскомнадзора (https://rkn.gov.ru/), на первом месте – представление уведомления об обработке персональных данных, содержащего недостоверные сведения. Важно отметить, что не все библиотеки подали такое уведомление, а это само по себе серьезное нарушение. Например, в Новосибирске 223 библиотеки, а в реестре Роскомнадзора всего 65 уведомлений от библиотек на всю Новосибирскую область. Такое уведомление целесообразно обновлять в следующих случаях: изменилось название и/или местонахождение организации; у библиотеки появились новые услуги, которые потребовали расширения перечня целей обработки ПДн или категорий ПДн; изменился ответственный за обработку ПДн в организации и/или его контактная информация; изменилось местонахождения базы данных. Анализировать информацию, содержащуюся в уведомлении, на предмет необходимости ее актуализации желательно хотя бы раз в три месяца.

Следующее нарушение – это несоответствие содержания письменного согласия субъекта персональных данных на обработку ПДн требованиям законодательства Российской Федерации [5, 6]. Форму и содержание согласия на обработку ПДн читателя определяет ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Так как библиотеки обрабатывают биометрические ПДн, то допустимы только письменная форма согласия или согласие в форме электронного документа, подписанного, в соответствии с федеральным законом, электронной подписью. Такие формы согласия должны включать в себя, в частности:

1. Фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2. Фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3. Наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4. Цель обработки персональных данных;

5. Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7. Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8. Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9. Подпись субъекта персональных данных.

Отсутствие хотя бы одного из перечисленных разделов является нарушением, как собственно и бессрочная обработка ПДн. Персональные данные читателя подлежат уничтожению, как только достигнута цель их обработки.

К серьезным и частым нарушениям Роскомнадзор относит отсутствие в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных. Сотрудник библиотеки, чья фамилия указана в уведомлении об обработке ПДн, должен знать об этом факте, иметь достаточное образование для обучения других сотрудников организации и проведения проверок. Библиотека должна разработать, опубликовать и довести до сведения всех сотрудников положение об обработке персональных данных.

По закону лица, виновные в нарушении требований законодательства в области защиты ПДн, несут гражданскую, уголовную, административную и дисциплинарную ответственность. Предусмотрены следующие виды наказаний: лишение свободы на срок до пяти лет, штраф до 200 000 рублей, лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

Выводы

Высокие темпы автоматизации библиотечной сферы требуют обратить пристальное внимание на вопросы защиты персональных данных читателей. Необходимость повышения уровня контроля в библиотеках над соблюдением норм безопасности при обработке ПДн и обеспечение условий их обработки не вызывает сомнений. Библиотекам следует защитить своих

читателей от различных неправомерных действий, связанных с обработкой ПДн. Кроме того, в ближайшее время может произойти расширение перечня категорий, обрабатываемых персональных данных, что повлечет за собой повышение уровня требований к защите.

Список источников

1. *Аскарова В. Я.* Читатель как объект профессиональной рефлексии // Чтение в XXI веке: традиции и тенденции: материалы Всерос. науч.-практ. конф. (Екатеринбург, 29–30 мая 2014 г.). Екатеринбург, 2014. С. 21–28.
2. *Бобров Л. К.*, Родионова З. В. Защита информационных ресурсов библиотеки на основе анализа бизнес-процессов // Научно-техническая информация. Серия 1, Организация и методика информационной работы. 2016. № 1. С. 21–29.
3. Обработка персональных данных пользователей в библиотеках : метод. рекомендации / Амур. обл. науч. б-ка им. Н. Н. Муравьева-Амурского ; сост. Л. Ф. Куприенко. Благовещенск, 2012. 38 с.
4. Публичный доклад Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. 2017. URL: http://rkn.gov.ru/docs/doc_2326.pdf (дата обращения: 30.08.2018).
5. *Безнедельный С. А.*, *Родионова З. В.* Проблема защиты персональных данных в медицинских учреждениях // Информационные технологии в прикладных исследованиях. Новосибирск, 2013. С. 215–219.
6. *Пестунова Т. М.*, *Родионова З. В.*, Отто Е. Н. Повышение эффективности управления работой с персональными данными на основе анализа бизнес-процессов // Вестник СибГУТИ. 2016. № 1. С. 23–29.

References

1. Askarova V. Ya. A reader as an object of professional reflection. *Chtenie v XXI veke: traditsii i tendentsii : materialy Vseros. nauch.-prakt. konf. (Ekaterinburg, 29–30 maya 2014 g.)*. Ekaterinburg, 2014, 21–28. (In Russ.).
2. Bobrov L. K., Rodionova Z. V. Protecting the library information resources based on business processes analysis. *Nauchno-tekhnicheskaya informatsiya. Seriya 1, Organizatsiya i metodika informatsionnoi raboty*, 2016, 1, 21–29. (In Russ.).
3. *Obrabotka personal'nykh dannykh pol'zovatelei v bibliotekakh : metod. rekomendatsii* [Processing users' personal data in libraries : method. recommendations]. Comp. L. Kuprienko. Blagoveshchensk, 2012. 38 p. (In Russ.).
4. *Publichnyi doklad Federal'noi sluzhby po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii. 2017* [Public report of the Federal Service for Supervision of Communications, Information Technology and Mass Communications. 2017]. URL: http://rkn.gov.ru/docs/doc_2326. pdf (accessed 30.08.2018).
5. Beznedel'nyi S. A., Rodionova Z. V. The problem of personal data protection in medical institutions. *Informatsionnye tekhnologii v prikladnykh issledovaniyakh*. Novosibirsk, 2013, 215–219. (In Russ.).
6. Pestunova T. M., Rodionova Z. V., Otto E. N. Improving the efficiency of managing personal data based on business processes analysis. *Vestnik SibSUTI*, 2016, 1, 23–29. (In Russ.).

Материал поступил в редакцию 22.10.2018 г.

Сведения об авторах: *Родионова Зинаида Валерьевна – кандидат технических наук, доцент НГУЭУ «НИНХ»,*
Бобров Леонид Куприянович – доктор технических наук, профессор, НГУЭУ «НИНХ»,
Медянкина Ирина Петровна – кандидат технических наук, НГУЭУ «НИНХ»