УТВЕРЖДЕН
приказом Государственного
учреждения культуры
Краснодарского края
«Краснодарская краевая
универсальная научная
библиотека им. А.С. Пушкина»
от 21.11. 2011 года №112-П

# ПОЛИТИКА

государственного бюджетного учреждения культуры Краснодарского края "Краснодарская краевая универсальная научная библиотека им. А.С.Пушкина" в отношении обработки и защиты персональных данных

## 1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со статьями 18.1, 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПД), Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и является локальным актом государственного бюджетного учреждения культуры Краснодарского края "Краснодарская краевая универсальная научная библиотека им. А.С.Пушкина" (далее Библиотека), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПД), оператором которых является Библиотека.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД в Библиотеке, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Библиотекой как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до ее утверждения.

## 2. Основания обработки и состав персональных данных, обрабатываемых в Библиотеке

2.1. Обработка ПД в Библиотеке осуществляется в связи с выполнением законодательно возложенных на Библиотеку функций, по оказанию библиотечно-информационных услуг.

Кроме того, обработка ПД в Библиотеке осуществляется в ходе трудовых и

иных непосредственно связанных с ними отношений, в которых Библиотека выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Библиотекой своих прав и обязанностей как юридического лица.

2.2. В рамках осуществления функции Библиотека обрабатывает категории ПД: фамилия, имя, отчество, год рождения, дата рождения, место рождения, семейное положение, образование, профессия, место работы или учебы.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Библиотека выступает в качестве работодателя, обрабатываются ПД лиц, претендующих на трудоустройство в Библиотеку, работников Библиотеки (далее - Работники) и бывших Работников.

2.4. В связи с реализацией своих прав и обязанностей, Библиотекой обрабатываются ПД физических лиц, а также граждан, письменно обращающихся в Библиотеку по вопросам её деятельности.

2.5. Специальные категории персональных данных, а также биометрические персональные данные Библиотекой не обрабатываются.

2.6. ПД получаются и обрабатываются Библиотекой на основании федеральных законов и письменного согласия субъекта ПД.

2.7. В целях исполнения возложенных на Библиотеку функций Библиотека в установленном порядке вправе поручить обработку ПД третьим лицам.

В договоры с лицами, которым Библиотека поручает обработку ПД, включаются условия, обязывающие таких лиц соблюдать предусмотренные Законом о ПД и Политикой правила обработки ПД.

2.8. Библиотека предоставляет обрабатываемые ПД государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПД.

2.9. В Библиотеке не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в Библиотеке, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Библиотекой ПД уничтожаются или обезличиваются.

2.10. При обработке ПД обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки.

## 3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПД при их обработке в Библиотеке является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПД, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПД Библиотека руководствуется следующими принципами:

1) законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;

2) системность: обработка ПД в Библиотеке осуществляется с учетом всех

взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;

3) комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Библиотеки и других имеющихся в Библиотеке систем и средств защиты;

4) непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Библиотеке с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД;

8) минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Библиотеки, а также объема и состава обрабатываемых ПД;

10) эффективность процедур отбора кадров: кадровая политика Библиотеки предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;

11) наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

12) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

## 4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Библиотеке ПД имеют лица, уполномоченные приказом, а также лица, чьи ПД подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПД полномочия по реализации каждой определенной законодательством функции Библиотеки закрепляются за соответствующими структурными подразделениями.

Доступ к ПД, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Библиотеки, могут иметь только Работники этого структурного подразделения. Работники

допускаются к ПД, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПД осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Библиотеки. Допуск Работников к обработке ПД осуществляется согласно перечню типовых полномочий, утверждаемых приказом Библиотеки. Соответствующие полномочия вносятся в должностные обязанности Работников.

Допущенные к обработке ПД Работники под роспись знакомятся с документами Библиотеки, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

4.4. Порядок доступа субъекта ПД к его ПД, обрабатываемым Библиотекой, осуществляется в соответствии с Законом о ПД и определяется локальным актом Библиотеки.

## 5. Реализация Политики

5.1. Библиотека принимает необходимые и достаточные меры для защиты обрабатываемых ПД от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПД в отделах Библиотеки несет заведующий отдела регистрации читателей и начальник отдела кадров.

Ответственный за организацию обработки ПД в Библиотеке, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Библиотеке требований нормативных правовых актов и локальных актов Библиотеки в области обработки и защиты ПД;

2) доводить до сведения Работников положения нормативных правовых актов и локальных актов Библиотеки в области обработки и защиты ПД;

3) организовывать прием и обработку обращений и запросов субъектов ПД или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Библиотека осуществляет обработку ПД без использования средств автоматизации.

5.4. При обработке ПД без использования средств автоматизации Библиотека, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПД, реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПД от информации, не содержащей ПД;

2) раздельную обработку и хранение каждой категории ПД (фиксация на отдельных материальных носителях ПД, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПД, установленным требованиям;

5) сохранность материальных носителей ПД;

6) условия хранения, исключающие несанкционированный доступ к ПД, а также смешение ПД (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПД.

5.6. Для каждой информационной системы формируется модель угроз безопасности ПД и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу.

Пересмотр моделей угроз осуществляется:

а) в плановом порядке для существующих информационных систем – не реже одного раза в три года;

б) в случае существенных изменений в инфраструктуре или порядке обработки ПД - в течение трех месяцев с даты фиксации изменений;

в) в случае создания новой информационной системы (выделения части из существующей) - в течение одного месяца с даты создания (выделения).

5.7. Ввод в эксплуатацию информационной системы оформляется актом ввода в эксплуатацию и сопровождается аттестацией или декларированием соответствия информационной системы требованиям по безопасности ПД.

5.8. В целях обеспечения управления информационной безопасностью ПД в Библиотеке создается система защиты ПД.

Объектами защиты системы защиты ПД являются информация, обрабатываемая Библиотекой и содержащая ПД, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.9. Система защиты ПД реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку локальных актов Библиотеки по вопросам обработки и защиты ПД, контроль за исполнением в Библиотеке требований нормативных правовых актов и локальных актов Библиотеки в области обработки и защиты ПД, а также внесение соответствующих изменений в имеющиеся локальные акты;

2) оформление письменных обязательств Работников о неразглашении ПД;

3) доведение до сведения Работников информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПД;

4) обеспечение наличия в положениях о структурных подразделениях Библиотеки и должностных обязанностях Работников требований по соблюдению установленного порядка обработки и защиты ПД;

5) разработку и введение в действие внутренних регулятивных документов Библиотеки по обеспечению информационной безопасности информационной системы;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление Работников с положениями нормативных правовых актов и внутренних регулятивных документов Библиотеки в области обработки и

защиты ПД, а также обучение Работников правилам обработки и защиты ПД;

8) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

а) физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию обработки ПД, в том числе хранения и передачи информации как внутри Библиотеки, так и при взаимодействии с государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

10) установление правил доступа на объекты, в помещения, применению в этих целях систем охраны и управления доступом;

11) формирование участков (выделение в отдельные виртуальные локальные компьютерные сети технических средств) администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и информационной системы в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Библиотеке (включая условия хранения документов в архиве), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Библиотеки в области обработки и защиты ПД;

14) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

15) организацию необходимых мероприятий с Работниками, а также собеседование с лицами, претендующими на работу в Библиотеке, изучение их биографии и проверку предоставляемых сведений;

16) обучение Работников требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

а) при стратегическом планировании архитектуры информационной системы;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

19) применение следующих компонентов программно-технических мер защиты:

а) защищенных средств (систем) обработки информации, содержащей ПД;

б) системы криптографической защиты информации при ее передаче по каналам связи;

в) межсетевых экранов для логического разделения подсетей и защиты от

несанкционированного доступа из внешних (открытых) информационных систем;

г) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

5.10. Для всех критичных в отношении обеспечения целостности и доступности ПД функций информационной системы разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал проходят процедуру обновления. Работники проходят обучение необходимым действиям по обеспечению целостности и доступности ПД в нештатных ситуациях.

## 6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПД реализуются в Библиотеке в следующих направлениях:

1) предотвращение утечки информации, содержащей ПД, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПД информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) обеспечение безопасного межсетевого взаимодействия;

5) обеспечение безопасного доступа к сетям международного информационного обмена;

6) анализ защищенности информационной системы;

7) обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПД по каналам связи;

8) обнаружение вторжений и компьютерных атак;

9) осуществления контроля за реализацией системы защиты ПД.

6.2. Мероприятия по обеспечению безопасности ПД включают в себя:

1) разграничение доступа пользователей информационной системы и обслуживающих её Работников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

2) регистрацию действий пользователей и обслуживающих её Работников, контроль несанкционированного доступа и действий пользователей и обслуживающих Работников, а также третьих лиц;

3) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

4) предотвращение внедрения в информационную систему вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

5) ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПД, а также хранятся носители информации, содержащие ПД;

6) размещение технических средств, позволяющих осуществлять обработку ПД, в пределах охраняемой территории;

7) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПД;

8) учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

9) резервирование технических средств, дублирование массивов и носителей информации;

10) реализацию требований по безопасному межсетевому взаимодействию ИС;

11) межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

12) обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПД;

13) периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационную систему;

14) активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

15) анализ защищенности информационной системы с применением специализированных программных средств (сканеров безопасности);

16) централизованное управление системой защиты ПД.

6.3. С целью поддержания состояния защиты ПД на надлежащем уровне в Библиотеке осуществляется внутренний контроль за эффективностью системы защиты ПД и соответствием порядка и условий обработки и защиты ПД установленным требованиям.

Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав систему защиты;

2) контроль соблюдения требований по обеспечению безопасности ПД (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПД, требований договоров).

6.4. В целях осуществления внутреннего контроля в Библиотеке проводятся периодические проверки условий обработки ПД. Проверки осуществляются ответственным за организацию обработки ПД в Библиотеке либо комиссией, образуемой директором.