Министерство культуры и туризма Рязанской области

Государственное бюджетное учреждение культуры Рязанской области
«Рязанская областная детская библиотека»

ПРИКАЗ

01.11.2017 № 18

г. Рязань

Об обеспечении безопасности персональных данных

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в целях обеспечения защиты персональных данных работников и пользователей Государственного бюджетного учреждения культуры Рязанской области «Рязанская областная детская библиотека»

ПРИКАЗЫВАЮ:

1. Отменить действие Положения об обработке и защите персональных данных работников ГУК Рязанская ОДБ, утвержденное приказом директора от 11.01.2010г. № 2.
2. Отменить действие Положения об обработке и защите персональных данных читателей ГУК Рязанская ОДБ, утвержденное приказом директора от 11.01.2010г. № 2.
3. Утвердить Политику ГБУК РО «Рязанская ОДБ» в отношении обработки персональных данных (Приложение №1)
4. Утвердить Положение об обработке и защите персональных данных работников ГБУК РО «Рязанская ОДБ» (Приложение №2)
5. Утвердить Положение об обработке и защите персональных данных читателей ГБУК РО «Рязанская ОДБ» (Приложение №3)
6. Утвердить Список сотрудников ГБУК РО «Рязанская ОДБ», допущенных к работе с персональными данными работников (Приложение №4)
7. Утвердить Список сотрудников ГБУК РО «Рязанская ОДБ», допущенных к работе с персональными данными читателей (Приложение №5)
8. Сотрудники, указанные в Списках и допущенные к работе с персональными данными работников и читателей ГБУК РО «Рязанская ОДБ», должны неукоснительно соблюдать требования соответствующих нормативных документов и несут персональную ответственность за:
- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с базой персональных данных работников.
- нарушение установленного законом порядка, сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- неправомерный доступ к компьютерной информации, содержащей персональные данные работников или читателей ГБУК РО «Рязанская ОДБ».
9. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Т.Н. Окружная

Министерство культуры и туризма Рязанской области

Государственное бюджетное учреждение культуры Рязанской области
«Рязанская областная детская библиотека»

ПРИКАЗ

01.11.2017 № 18

г. Рязань

Об обеспечении безопасности персональных данных

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в целях обеспечения защиты персональных данных работников и пользователей Государственного бюджетного учреждения культуры Рязанской области «Рязанская областная детская библиотека»

ПРИКАЗЫВАЮ:

1. Отменить действие Положения об обработке и защите персональных данных работников ГУК Рязанская ОДБ, утвержденное приказом директора от 11.01.2010г. № 2.
2. Отменить действие Положения об обработке и защите персональных данных читателей ГУК Рязанская ОДБ, утвержденное приказом директора от 11.01.2010г. № 2.
3. Утвердить Политику ГБУК РО «Рязанская ОДБ» в отношении обработки персональных данных (Приложение №1)
4. Утвердить Положение об обработке и защите персональных данных работников ГБУК РО «Рязанская ОДБ» (Приложение №2)
5. Утвердить Положение об обработке и защите персональных данных читателей ГБУК РО «Рязанская ОДБ» (Приложение №3)
6. Утвердить Список сотрудников ГБУК РО «Рязанская ОДБ», допущенных к работе с персональными данными работников (Приложение №4)
7. Утвердить Список сотрудников ГБУК РО «Рязанская ОДБ», допущенных к работе с персональными данными читателей (Приложение №5)
8. Сотрудники, указанные в Списках и допущенные к работе с персональными данными работников и читателей ГБУК РО «Рязанская ОДБ», должны неукоснительно соблюдать требования соответствующих нормативных документов и несут персональную ответственность за:
- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с базой персональных данных работников.
- нарушение установленного законом порядка, сбора, хранения, использования или распространения информации о гражданах (персональных данных);
- неправомерный доступ к компьютерной информации, содержащей персональные данные работников или читателей ГБУК РО «Рязанская ОДБ».
9. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Т.Н. Окружная

Приложение №1
к приказу директора
ГБУК РО «Рязанская ОДБ»
от 01.11.2017 № 18

Политика
ГБУК РО «Рязанская ОДБ»
в отношении обработки персональных данных

1. Общие положения

1.1 Термины и определения

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (Обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2 Назначение и правовая основа документа

Политика ГБУК РО «Рязанская ОДБ» (далее Библиотека) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационно безопасности, которыми руководствуется Библиотека в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики является Конституция РФ, Гражданский, Уголовный и Трудовой кодексы, ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства РФ, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Библиотеки позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. Объекты защиты

Основными объектами системы безопасности персональных данных в Библиотеки являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные сотрудников и пользователей Библиотеки;
- процессы обработки персональных данных в информационной система персональных данных Библиотеки, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

3. Цели и задачи обеспечения безопасности персональных данных.

3.1 . Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных Библиотеки является:

- Библиотека, как собственник информационных ресурсов;
-руководство и сотрудники Библиотеки, в соответствии с возложенными на них функциями;
- физические лица (граждане) – читатели (пользователи) Библиотеки;
- физические лица (граждане), состоящие с Библиотекой в гражданско-правовых отношениях;

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- современного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
-разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

3.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Библиотеки от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Библиотеки, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждения авторства) персональных данных, хранимых и обрабатываемых в информационных системах Библиотеки и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

3.3. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Библиотеки должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационно безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Библиотеки;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативных тенденций;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидации последствий нарушения безопасности информации;
- защиту от вмешательства в процессе функционирования информационных систем Библиотеки посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Библиотеки (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутенфикации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в информационных системах Библиотеки программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передачи по каналам связи.

3.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решения перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационных систем Библиотеки (информация, задач, документов, каналов связи, серверов, автоматизированных мест);
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Библиотеки по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Библиотеки;
- четким знанием и строгим соблюдением всеми пользователями информационных система Библиотеки требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Библиотеки;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Библиотеки;
- применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов Библиотеки требований по обеспечению безопасности информации;
- юридической защитой интересов Библиотеки при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4. Основные принципы построения системы безопасности персональных данных

Построением системы, обеспечения безопасности персональных данных Библиотеки, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
- законность;
- системность;
- компетентность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

4.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Библиотеки в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных актов по безопасности информации РФ. С применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи системы Библиотеки должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

4.2. Системность

Системный подход к построению системы защиты информации в Библиотеке предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Библиотеки, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласование применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.4. Непрерывность защиты

Обеспечением безопасности персональных данных – процесс, осуществляемый руководством Библиотеки, ответственным за организацию обработки персональных данных и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупностью средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Библиотеки и каждый сотрудник Библиотеки должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной

деятельности Библиотеки и ее эффективность зависти от участия руководства Библиотеки в обеспечении информационной безопасности персональных данных.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п). Перерыв в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

4.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных системы в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развития самой защищаемой информационной системы. Это позволяет учесть требования безопасности при проектировании архитектуры и, в конечном счете, обладающие достаточным уровнем защищенности.

4.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных система Библиотеки и системы ее защиты с учетом

4.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Библиотеки. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативного воздействия или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

4.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом,

чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен представляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.10. исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критических операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Библиотеки. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможность скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

4.11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Библиотеки. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных за организацию обработки персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в Библиотеки является высокая культура работы с информацией. Руководство Библиотеки несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Библиотеки. Все сотрудники Библиотеки должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает большие возможности для нарушения безопасности или не обнаружения фактов ее нарушения.

4.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Библиотекой своей деятельности. В числе таких изменений входят:

- изменения организационной и штатной структуры Библиотеки;

- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретной структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.14. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малоприятных ему операций.

4.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономически целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

4.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Библиотеки (ответственными за организацию обработки персональных данных)

4.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и

должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками Библиотеки должны немедленно доводиться до сведения руководителя Библиотеки и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

5. Меры, методы и средства обеспечения требуемого уровня защиты информационных ресурсов

Все меры обеспечения безопасности информационных систем Библиотеки подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные);

5.1.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Библиотеки.

5.1.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Библиотеке. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Библиотеки в целом. Морально-этические нормы бывают как неписанные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

5.1.3. Технологические меры защиты

К данному виду меры защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

5.1.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае реализации угроз безопасности или снизить размер потерь в случае их реализации.

5.2. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечивать ее выполнение, выделяя необходимые ресурсы и контролирую состояние дел.

5.3. Регламентация доступа в помещение

Компоненты информационных систем Библиотеке должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.)

По окончанию рабочего дня, помещения, в которых размещаются компоненты информационных систем Библиотеки, должны запираться на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

5.4. Регламентация допуска сотрудников к использованию информационных ресурсов.

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Все сотрудники библиотеки и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных.

5.5. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов.

В целях поддержания режима информационной безопасности аппаратного программная конфигурация автоматизированных рабочих мест сотрудников Библиотеки, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

в компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.6. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем Библиотеки, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической документацией, определяющей требования и порядок обработки персональных данных в Библиотеке.

5.7. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем Библиотеки

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Библиотеки.

5.8. Средства обеспечения безопасности

Для обеспечения информационной безопасности Библиотеки используются следующие средства защиты:

- физические средства;
-технические средства;
- средства идентификации и аутенфикации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационных систем Библиотеки, независимо от их вида и формы представления информации в них.

5.9. Контроль эффективности систем защиты

Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных,
Разрушение средств информатизации. Контроль может производиться привлекаемыми для этой цели организациям, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Приложение №2
к приказу директора
ГБУК РО «Рязанская ОДБ»
от 01.11.2017г. № 18

Положение
об обработке и защите персональных данных работников
ГБУК РО «Рязанская ОДБ»

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных работников ГБУК РО «Рязанская ОДБ» от несанкционированного доступа.

1.2. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и определяет порядок сбора, хранения, передачи и любого другого использования персональных данных в соответствии с законодательством Российской Федерации.

2. Понятие и состав персональных данных.

2.1. Для целей настоящего Положения используются следующие понятия:
- Работник - физическое лицо, состоящее в трудовых отношениях с работодателем.
- Работодатель - Государственное бюджетное учреждение культуры Рязанской области «Рязанская областная детская библиотека» (ГБУК РО «Рязанская ОДБ»).
- Персональные данные - любая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
- Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
- Использование персональных данных - действия (операции) с персональными данными, совершаемые работодателем в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

- Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.
- Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
2.2. К персональным данным относятся:
- Сведения, содержащиеся в документе, удостоверяющем личность работника;
- Информация, содержащаяся в трудовой книжке работника;
- Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- Сведения, содержащиеся в документах воинского учета;
- Сведения об образовании, квалификации или наличии специальных знаний или подготовки;
-Информация медицинского характера, в случаях, предусмотренных законодательством;
- Сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- Сведения о доходах;
- Сведения о семейном положении работника;

3. Получение и обработка персональных данных работника

3.1. Получение персональных данных.
- Все персональные данные работника следует получать лично у работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
3.2. Хранение персональных данных работников осуществляется кадровой службой, бухгалтерией, на бумажных и электронных носителях.
3.3. В кадровой службе персональные данные хранятся на бумажных носителях в личных карточках по форме Т-2 и личных делах. Кадровая служба обеспечивает их защиту от несанкционированного доступа и копирования.
3.4. В бухгалтерии персональные данные хранятся в электронном виде, в программе 1С: «Зарплата и кадры». Бухгалтерия обеспечивает их защиту от несанкционированного доступа и копирования.
3.5. Уничтожение персональных данных.
- Персональные данные работников хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.
- Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

4. Права и обязанности работников и работодателя по обеспечению защиты персональных данных.

4.1. В целях обеспечения защиты персональных данных, хранящихся в личных делах работников, работники имеют право:
- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
- при отказе работодателя или уполномоченного им лица исключить или исправить персональные данные работника - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;
- дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;
- требовать от работодателя или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие работодателя или уполномоченного им лица при обработке и защите персональных данных работника.
4.2. Для защиты персональных данных работников работодатель обязан:
- за свой счет обеспечить защиту персональных данных работника от неправомерного их использования или утраты в порядке, установленном законодательством РФ;
- ознакомить работника и его представителей с настоящим Положением и их правами в области защиты персональных данных под расписку;
- осуществлять передачу персональных данных работника только в соответствии с настоящим Положением и законодательством Российской Федерации;
- предоставлять персональные данные работника только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;
- обеспечить работнику свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;
- по требованию работника предоставить ему полную информацию о его персональных данных и обработке этих данных;
- Работодатель не вправе получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать персональные данные работника о его личной жизни только с письменного согласия работника;
- Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.
4.3. Работники обязаны:
- сообщать работодателю обо всех изменениях в персональных данных в письменной форме в двухнедельный срок с момента внесения изменений в соответствующие документы работника;

5. Передача персональных данных работника

5.1. Передача персональных данных работников в пределах ГБУК РО «Рязанская ОДБ».
5.1.1. Право доступа к персональным данным работника имеют (Приложение №4):
- директор;
- заместитель директора по координации;
- заместитель директора по автоматизации;
- кадровая служба;
- бухгалтерия;
- руководители отделов.
5.1.2. Право доступа к персональным данным других работников определяется приказом руководителя организации. Работники должны быть ознакомлены с указанным приказом под роспись.
5.1.3. Руководитель кадровой службы вправе передавать персональные данные Работника в бухгалтерию в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.
5.2. Передача персональных данных работников третьим лицам и сторонним организациям.
- Работодатель вправе передавать персональные данные Работника третьим лицам и сторонним организациям только при наличии письменного согласия работника. При отсутствии письменного согласия работника передача персональных данных производится исключительно в целях предупреждения угрозы жизни и здоровья работника, а также в других случаях, установленных законодательством.
- При передаче персональных данных Работника лица, получающие данную информацию, должны быть предупреждены представителем работодателя о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, от этих лиц должно быть получено письменное подтверждение соблюдения этого условия.

6. Ответственность за разглашение персональных данных

6.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке,

установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Согласовано:
Заместитель директора по координации .....
Заместитель директора по автоматизации .....
Главный бухгалтер .....
Начальник отдела кадров .....
Ведущий юрисконсульт .....

Согласно требованиям ст. 88 ТК РФ работодатель обязан осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись. Таким актом, например, может являться приказ по организации, утверждающий список работников организации, допущенных к работе с персональными данными:

Приложение №3
к приказу директора
ГБУК РО «Рязанская ОДБ»
от 01.11.2017г. № 18

Положение
об обработке и защите персональных данных читателей
ГБУК РО «Рязанская ОДБ»

1. Общие положения

1.1. Настоящее Положение регулирует правоотношения, возникающие в процессе сбора, хранения, использования и уничтожения персональных данных пользователей и служащих библиотеки.

1.2. Целью настоящего Положения является соблюдение прав пользователей на неприкосновенность частной жизни, личную и семейную тайну при обработке его персональных данных.

1.3. Настоящее положение разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.4. Основные понятия используемые в настоящем Положении:

- персональные данные - любая информация, относящаяся к определенному физическому лицу (пользователю библиотеки), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

2. Принципы обработки персональных данных читателей

2.1. Сбор персональных данных читателей библиотекой осуществляется с целью:

- повышения оперативности и качества обслуживания читателей, организации адресного, дифференцированного и индивидуального их обслуживания, обеспечения сохранности библиотечного имущества.

2.2. Персональные данные читателей обрабатываются библиотекой на основании ст. 5 и ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и с их письменного согласия, подтверждаемого собственноручной подписью читателя, либо его законного представителя в Договоре и регистрационной карточке.

2.3. Источником персональных данных служит регистрационная карточка читателя, заполняемая им лично или с его слов библиотекарем при оформлении в библиотеку и удостоверяемая собственноручной подписью пользователя.

2.4. Персональные данные читателей являются конфиденциальной информацией, не подлежащей разглашению, и не могут быть использованы библиотекой или ее сотрудниками для целей, не перечисленных в п. 2.1 настоящего Положения.

2.5. Разглашение персональных данных читателя или их части допускается только в случаях предусмотренных действующим законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации, либо с отдельного письменного согласия читателя.

Перечень персональных данных вносимых в регистрационную карточку пользователя (Приложение №2):

- Фамилия, имя и отчество читателя;
- Паспортные данные (серия, номер, орган выдавший, дата выдачи);
- Сведения о регистрации по месту жительства и временной регистрации по месту пребывания
- Место работы/учебы

3. Условия обработки персональных данных читателей

3.1. Персональные данные читателей хранятся в отделе обслуживания в сейфе на бумажном носителе (регистрационная карточка).

3.2. Право доступа к персональным данным читателей имеют:

- администрация;
- сотрудники отделов обслуживающих читателей (Приложение №5).

3.3. Работники отделов обслуживания вправе передавать персональные данные читателя работникам администрации в объеме необходимом для исполнения ими служебных обязанностей и согласно их должностным инструкциям, а также в случаях, установленных законодательством.

3.4. Директор библиотеки может передавать персональные данные читателя третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья читателя и иных случаях, установленных действующим законодательством.

3.5. При передаче персональных данных читателя директор ГБУК РО «Рязанская ОДБ» предупреждает лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требует от этих лиц письменное подтверждение соблюдения этого условия.

3.6. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных читателей, определяются должностными инструкциями.

3.7. Персональные данные читателя уточняются ежегодно при первом посещении читателем библиотеки в году, следующем за годом регистрации, либо годом последнего уточнения персональных данных. В случае изменения персональных данных библиотека переоформляет регистрационную карточку читателя, уничтожает регистрационную карточку с неверными данными.

3.8. Срок обработки персональных данных библиотекой – в течение двухлетнего срока с момента последней перерегистрации читателя. По истечении срока обработки персональные данные на бумажном носителе (регистрационная карточка, формуляр) уничтожаются.

4. Права читателей

4.1. Читатель имеет право на получение при обращении в библиотеку следующей информации:

- подтверждение факта обработки персональных данных библиотекой, а также цель такой обработки;
- способы обработки персональных данных, применяемые библиотекой;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для читателя может повлечь за собой обработка его персональных данных.

4.2. Обработка персональных данных в целях информирования читателя о новых услугах библиотеки, новых поступлениях литературы, проводимых в библиотеке мероприятиях путем осуществления прямых контактов с ним с помощью средств связи допускается только при условии предварительного согласия читателя выраженного в письменной форме и прекращается немедленно по его письменному требованию.

4.3. Если читатель считает, что библиотека осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, читатель вправе обжаловать действия или бездействие библиотеки в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

4.4. Читатель имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5. Обязанности библиотеки в отношении обработки персональных данных читателей

5.1. Библиотека при обработке персональных данных принимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, копирования, распространения персональных данных, а также от иных неправомерных действий.

5.2. Библиотека осуществляет передачу персональных данных читателя только в соответствии с настоящим Положением и законодательством РФ.

5.3. Библиотека обязана в порядке, предусмотренном п.п. 4.1-4.3 настоящего Положения, сообщить читателю информацию о наличии его персональных данных, а также предоставить возможность ознакомления с ними при обращении читателя в течение десяти рабочих дней с даты получения запроса.

5.4. Библиотека обязана внести по требованию читателя необходимые изменения, блокировать его персональные данные по предоставлении читателем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему читателю и обработку которых осуществляет библиотека, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах библиотека уведомляет читателя или его законного представителя и третьих лиц, которым персональные данные этого читателя были переданы.

5.5. В случае выявления недостоверных персональных данных или неправомерных действий с ними библиотека при обращении или по запросу читателя осуществляет блокирование персональных данных,

относящихся к соответствующему читателю, с момента такого обращения на период проверки.

5.6. В случае подтверждения факта недостоверности персональных данных библиотека на основании документов, представленных читателем или его законным представителем, уточняет персональные данные и снимает их блокирование.

5.7. В случае выявления неправомерных действий с персональными данными, библиотека в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений библиотека в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных библиотека уведомляет читателя или его законного представителя.

5.8. По истечении двухлетнего срока с момента последней перерегистрации читателя библиотека прекращает обработку персональных данных, уничтожает (в случае прямого отказа от пользования библиотекой) его персональные данные на бумажном носителе (регистрационную карточку). Уничтожение и обезличивание персональных данных производятся только при условии, что читатель не имеет задолженности перед библиотекой. В противном случае, персональные данные блокируются, уничтожаются и обезличиваются только после снятия задолженности.

6. Ответственность библиотеки и ее сотрудников

6.1. Защита прав читателей, установленных настоящим Положением и законодательством РФ, осуществляется судом, в целях пресечения неправомерного использования персональных данных читателя, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального ущерба.

6.2. В случае нарушения норм, регулирующих обработку, хранение, передачу и защиту персональных данных читателя библиотекой и иными лицами, они несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение №4
к приказу директора
ГБУК РО «Рязанская ОДБ»
от 01.11.2017г. № 18

Список лиц, допущенных к работе с персональными данными работников

N п/п	Должность	Фамилия, имя, отчество	Подпись
1	Директор	Окружная Т.Н.	
2	Заместитель директора по координации	Вайло С.С.	
3	Заместитель директора по автоматизации	Лебедева О.Н.	
4	Главный бухгалтер	Кульчицкая Т.В.	
5	Ведущий инженер по охране труда	Бизюкин С.В.	
6	Ведущий экономист	Вьюшкова Л.М.	
7	Бухгалтер I категории	Прошлякова Т.Н.	
8	Начальник отдела кадров	Тарасова И.А.	
9	Заведующий отделом обслуживания	Ляблина Л.В.	
10.	Заведующий отделом формирования и хранения фонда	Амелина О.Н.	
11.	Заведующий методико-библиографическим отделом	Королева О.Е.	

Приложение № 5
к приказу директора
ГБУК РО «Рязанская ОДБ»
от 01.11.2017г. № 18

Список лиц, допущенных к работе с персональными данными читателей

№	Должность	Фамилия, имя, отчество	Название отдела	Подпись
1	Главный библиотекарь	Федорова З.Г.	Отдел формирования и хранения фонда	
2	Главный библиотекарь	Шушунова М.А.	Отдел формирования и хранения фонда	
3	Ведущий библиотекарь	Суркова И.А.	Отдел формирования и хранения фонда	
4	Главный библиотекарь	Воронина Р.А.	Отдел обслуживания	
5	Библиотекарь 1 категории	Куликова Н.И.	Отдел обслуживания	
6	Библиотекарь II категории	Мирошник Ю.В.	Отдел обслуживания	
7	Главный библиотекарь	Зорькина С.А.	Отдел обслуживания	
8	Ведущий библиотекарь	Светикова Е.Ю.	Отдел обслуживания	
9	Ведущий библиотекарь	Сучкова Е.В.	Отдел обслуживания	
10	Заведующий отделом	Королева О.Е.	Методико-библиографический отдел	
11	Ведущий библиограф	Грачева Т.А.	Методико-библиографический отдел	
12	Заведующий отделом	Ляблина Л.В.	Отдел обслуживания	
13	Ведущий библиотекарь	Осипова С.В.	Отдел обслуживания	
14	Главный библиотекарь	Крыкова Е.Н	Отдел обслуживания	
15	Главный библиотекарь	Чечева И.Б.	Отдел обслуживания	
16	Ведущий библиотекарь	Половая Е.П	Отдел обслуживания	
17	Главный библиотекарь	Клюйкова И.М.	Отдел обслуживания	
18	Ведущий библиотекарь	Стельмах Г.В.	Отдел обслуживания	
19	Ведущий библиотекарь	Савова Н.Ю.	Отдел обслуживания	
20	Библиотекарь II категории	Краюшкина М.Н.	Отдел обслуживания	
21	Заведующий отделом	Амелина О.Н.	Отдел формирования и хранения фонда	
22	Главный библиотекарь	Мочалина О.А.	Отдел обслуживания	
23	Главный библиотекарь	Полунина О.О.	Отдел обслуживания	
24	Ведущий библиотекарь	Моисеева М.С.	Отдел обслуживания	
25	Ведущий библиотекарь	Борисова О.Н.	Отдел обслуживания	
26	Главный библиотекарь	Кильдишева Л.И.	Методико-библиографический отдел	
27	Главный библиограф	Иванова-Пальмова Т.О.	Методико-библиографический отдел	
28	Ведущий библиотекарь	Игнаткина Ю.А.	Отдел формирования и хранения фонда	
29	Библиотекарь II категории	Юркова Е.В.	Отдел обслуживания	
30	Ведущий библиотекарь	Чичкова Ю.А.	Отдел обслуживания	
31	Главный библиотекарь	Сорокина Ю.Д.	Отдел формирования и хранения фонда	
32	Ведущий библиотекарь	Булатова Н.Н.	Отдел обслуживания	

33	Ведущий методист	Захарова Э.В.	Методико-библиографический отдел	
34	Ведущий библиотекарь	Маслова О.П..	Отдел обслуживания	
35	Главный библиотекарь	Щелокова Е.А.	Отдел обслуживания	

Приложение № 1
к Положению об обработке и защите
персональных данных работников
ГБУК РО «Рязанская ОДБ»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации (персональных данных работников и третьих лиц)

В соответствии с трудовым договором и действующим законодательством
_____
_____
должность, фамилия, имя, отчество

обязан(а) знать перечень сведений конфиденциального характера в Рязанской областной детской библиотеке. Хранить в тайне известные ему персональные данные, информировать руководителя о фактах нарушения порядка обращения с названными сведениями, о ставших ему известными попытках несанкционированного допуска к информации;

соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них от посторонних лиц;

знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения трудовой функции и вытекающих из нее служебных обязанностей.

С Положением о защите персональных данных работников библиотеки и третьих лиц, обязанностями о неразглашении персональных данных, ставших известными мне в результате выполнения должностных обязанностей, и ответственностью за их разглашение ознакомлен(а).

_____ __ _____ _____
должность подпись Ф.И.О.

«____» _____ 20 ___ г.

Приложение № 2
к Положению об обработке и защите
персональных данных работников
ГБУК РО «Рязанская ОДБ»

СОГЛАСИЕ

Я, _____даю согласие на обработку ГБУК РО «Рязанская ОДБ» предоставленных мною персональных данных, с целью ведения регистра работников учреждения. Мои персональные данные, в отношении которых даю согласие, включают следующие сведения о (об):

- анкетных и биографических данных;
- образовании;
- трудовом стаже;
- составе семьи;
- паспортных данных;
- занимаемой должности;
- заработной плате;
- семейном положении;
- отношении к воинской обязанности;
- отсутствии судимости;
- адресе регистрации (проживания);
- данных страхового свидетельства обязательного пенсионного страхования;
- ИНН;
- медицинском освидетельствовании (заключении);
- сведения о близких родственниках.
- личных делах и трудовых книжках;
- аттестации, повышении квалификации и переподготовке.

Перечень действий с персональными данными, в отношении которых дано согласие, включает обработку моих персональных данных неавтоматизированным и автоматизированным способом.

Условием прекращения обработки персональных данных является расторжение трудового договора.

«____»_____ 20____г. _____ _____

подпись расшифровка подписи

Приложение № 1
к Положению об обработке и защите
персональных данных читателей
ГБУК РО «Рязанская ОДБ»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации (персональных данных читателей и третьих лиц)

В соответствии с трудовым договором и действующим законодательством
_____
_____
должность, фамилия, имя, отчество

обязан(а) знать перечень сведений конфиденциального характера в Рязанской областной детской библиотеке. Хранить в тайне известные ему персональные данные, информировать руководителя о фактах нарушения порядка обращения с названными сведениями, о ставших ему известными попытках несанкционированного допуска к информации;

соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них от посторонних лиц;

знакомиться только с теми служебными документами, к которым получен доступ в силу исполнения трудовой функции и вытекающих из нее служебных обязанностей.

С Положением о защите персональных данных читателей библиотеки и третьих лиц, обязанностями о неразглашении персональных данных, ставших известными мне в результате выполнения должностных обязанностей, и ответственностью за их разглашение ознакомлен(а).

_____	_____	_____
должность	подпись	Ф.И.О.

«____» _____ 20 ___ г.

Министерство культуры и туризма Рязанской области

Государственное бюджетное учреждение культуры Рязанской области «Рязанская областная детская библиотека»

ПРИКАЗ

11.01.2021 г. № 1/1

г. Рязань

По административной деятельности

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ ст. 22.1 «О персональных данных» и обеспечения защиты персональных данных работников ГБУК РО «Рязанская ОДБ»:

ПРИКАЗЫВАЮ:

1. Назначить ведущего юрисконсульта Иванова Александра Юрьевича ответственным за обработку персональных данных в учреждении.
2. Назначить главного специалиста по защите информации Бызова Андрея Владимировича ответственным за информационную безопасность персональных данных в учреждении.
3. Ознакомить с настоящим приказом ведущего юрисконсульта и главного специалиста по защите информации.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Т. Н. Окружная

№	Ф. И. О.	Подпись
1	Иванов А. Ю.	
2	Бызов А. В.	