Министерство культуры и туризма Рязанской области Государственное бюджетное учреждение культуры Рязанской области
«Рязанская областная универсальная научная библиотека имени Горького»
(ГБУК РО «Библиотека имени Горького»)

ПРИКАЗ

17.04.2017 № 68

Рязань

Об обеспечении безопасности персональных данных

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и в целях обеспечения защиты персональных данных работников и пользователей государственного бюджетного учреждения культуры Рязанской области «Рязанская областная универсальная научная библиотека имени Горького»

ПРИКАЗЫВАЮ:

1. Отменить Положение о защите персональных данных сотрудников ГУК «Библиотека им. Горького», утвержденное приказом директора от 20.04.2011 г. № 22.
2. Утвердить Политику ГБУК РО «Библиотека им. Горького» в отношении обработки персональных данных (Приложение № 1).
3. Утвердить Положение о порядке обработки персональных данных работников ГБУК РО «Библиотека им. Горького» (Приложение № 2).
4. Утвердить Положение о порядке обработки данных пользователей ГБУК РО «Библиотека им. Горького» (Приложение 3).
5. Утвердить, Список сотрудников ГБУК РО «Библиотека им. Горького», допущенных к работе с персональными данными (Приложение № 4).
6. Указанные в Списке сотрудники ГБУК РО «Библиотека им. Горького», допущенные к работе с персональными данными, должны неукоснительно соблюдать требования соответствующих нормативных документов, а также несут персональную ответственность за:
   -сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с базой персональных данных работников. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

-нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

-неправомерный доступ к компьютерной информации, содержащей персональные данные работников или пользователей ГБУК РО «Библиотека им. Горького».

7. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Н.Н. Гришина

Приложение № 1
к приказу директора
ГБУК РО «Библиотека им. Горького»
от 17.04 2017 г. № 68

ПОЛИТИКА
ГБУК РО «Библиотеки им. Горького»
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 территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2. Назначение и правовая основа документа

Политика Рязанской областной универсальной научной библиотеки им. Горького (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 информационной 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 являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, 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 системе 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 Библиотека являются:

– Библиотека, как собственник информационных ресурсов;

– руководство и сотрудники Библиотеки, в соответствии с возложенными на них функциями;

– физические лица (граждане) - пользователи Библиотеки;

– физические лица (граждане), состоящие с Библиотекой в гражданско-правовых отношениях;

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– своевременного 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 (подтверждение 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 информационной 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 негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– защиту от вмешательства в процесс 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 аутентификации 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 передаче по каналам связи.

3.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем Библиотеки (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;

– 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 систем 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;

– применением 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

Построение системы, обеспечения безопасности персональных данных Библиотеки, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;

– системность;

– 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 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 информационной 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 согласованное 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

Обеспечение 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 совокупность 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 зависит 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.). Перерывы 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 систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, 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 систем Библиотеки и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

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 негативных воздействий 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 обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный 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 предоставляться 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 критичных 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 возможности 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 ответственным за организацию обработки персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в Библиотеке 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 больше возможностей 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 число 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 секретности 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 малопонятных 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 экономической 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

5.1. Меры обеспечения информационной безопасности

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 неписаные, 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 мер 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 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 обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в Библиотеке целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Библиотеки в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;

– кто имеет права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.3. Регламентация доступа в помещения

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.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

По окончании 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 таких 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.

Допуск пользователей к работе с информационными системами Библиотеки и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных;

– руководитель Библиотеки имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

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 Департамента.

Обработка персональных данных в компонентах информационных систем Библиотеки должна производиться в соответствии с утвержденными технологическими инструкциями.

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

В целях поддержания режима информационной безопасности аппаратно-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. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационной системы, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.7. 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 и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в Библиотеке.

Обеспечение безопасности персональных данных возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Библиотеки. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем Библиотеки, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем Библиотеки должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных Библиотеки, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

5.8. 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.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5.9. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности Библиотеки используются следующие средства защиты:

– физические средства;

– технические средства;

– средства идентификации и аутентификации 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 Департамента, независимо от их вида и формы представления информации в них.

5.9.1. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем Библиотеки необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки персональных данных, на:

– наличие специально внедренных закладных устройств;

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных;

– оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

5.9.2. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

5.9.3. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем Департамента посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.9.4. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды Библиотеки и элементам системы защиты персональных данных (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

5.9.5. Средства обеспечения и контроля целостности»

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

5.9.6. Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые

могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения ответственного за организацию обработки персональных данных о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;

– идентификатор субъекта, осуществляющего регистрируемое действие;

– действие (тип доступа).

5.10. Контроль эффективности системы 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 проводиться привлекаемыми для этой цели организациями, 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 «Библиотека им. Горького»
от 17.04.2017 г. № 68

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ГБУК РО «БИБЛИОТЕКА ИМ. ГОРЬКОГО»

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных работников ГБУК РО «Библиотека им. Горького» от несанкционированного доступа.

1.2. Настоящее Положение разработано в соответствии с требованиями ТК РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и определяет особенности обработки персональных данных работника.

1.3. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.4. Должностные лица, в обязанность которых входит ведение персональных данных сотрудников, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.5. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.6. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

1.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов согласно законодательства Российской Федерации.

1.9. Настоящее Положение утверждается директором ГБУК РО «Библиотека им. Горького» и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудника.

2. Перечень документов и сведений, содержащих персональные данные работника

2.1. В соответствии с ТК РФ, локальными нормативными актами ГБУК РО «Библиотека им. Горького» лицо, поступающее на работу, предъявляет работодателю следующие документы, содержащие его персональные данные:

- паспорт или иной документ, удостоверяющий личность, содержащий сведения о паспортных данных работника, сведения о месте регистрации (месте жительства), сведения о семейном положении;
- трудовую книжку, содержащую данные о трудовой деятельности работника;
- страховое свидетельство государственного пенсионного страхования, содержащее сведения о номере и серии страхового свидетельства;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии.

2.2. В перечень документов и сведений, содержащих персональные данные, включаются:

- трудовой договор;
- анкетные и паспортные данные;
- сведения о заработной плате;
- образование;
- другая информация.

3. Понятие и состав персональных данных

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

3.1. Состав персональных данных работника:

- анкетные и биографические данные;
- сведения об образовании;

- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- адрес места жительства, номер домашнего телефона;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

3.2. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

4. Требования по обработке персональных данных работников

4.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами;
- все персональные данные работника следует получать у него самого.
- 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, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

- при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет своих средств в порядке, установленном федеральным законом.

- работники и их представители должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

- работник не должен отказываться от своих прав на сохранение и защиту тайны.

5. Обязанности работника

5.1. Работник обязан:

5.1.1. Передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РФ.

5.1.2. Своевременно сообщать работодателю об изменении своих персональных данных.

6. Права работника

6.1. Работник имеет право:

- получения полной информации о своих персональных данных и обработке персональных данных;

- требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ и настоящего Положения;

- заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия в случае отказа работодателя исключить или исправить персональные данные работника;

- дополнить заявлением, выражающим его собственную точку зрения, персональные данные оценочного характера;

- требовать об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- свободного бесплатного доступа к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

- определять своих представителей для защиты своих персональных данных;

- работник не должен отказываться от своих прав на сохранение и защиту тайны.

7. Сбор, обработка и хранение персональных данных

7.1. Порядок получения персональных данных:

7.1.1. Все персональные данные работника следует получать у него самого. 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, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

7.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.1.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

7.2. Обработка, передача и хранение персональных данных работника:

7.2.1.Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

7.2.2. Круг лиц, допущенных к работе с документами, содержащими персональные данные работников, определяется приказом директора ГБУК РО «Библиотека им. Горького».

7.2.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники бухгалтерии, сотрудники отдела кадров, сотрудники службы безопасности, сотрудники компьютерных отделов.

7.3. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работника в порядке, установленном ТК РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

7.4. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

7.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

7.7. С работниками, ответственными за хранение персональных данных, а также с работниками, владеющими персональными данными в силу своих должностных обязанностей, заключаются Соглашения о неразглашении персональных данных работников (Приложение 1). Экземпляр Соглашения хранится в отделе кадров.

7.8. Автоматизированная обработка и хранение персональных данных работников допускаются только после выполнения всех основных мероприятий по защите информации.

7.9. Персональные данные, зафиксированные в бумажных носителях хранятся в запираемых шкафах.

7.10. Персональные данные, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

7.11. Не допускается хранение и размещение документов, содержащих персональные данные в открытых электронных каталогах (файлообменниках).

7.12. Помещения, в которых хранятся персональные данные работников, должны быть оборудованы надежными замками и сигнализацией на вскрытие помещений.

7.13. Помещения в рабочее время при отсутствии в них работников отдела кадров должны быть закрыты.

7.14. Проведение уборки помещения должно производиться в присутствии работников отдела кадров.

8. Доступ к персональным данным работника

8.1. Право доступа к персональным данным работника имеют:

- директор ГБУК РО «Библиотека им. Горького»;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);
- руководитель нового подразделения при переводе работника из одного структурного подразделения в другое;
- сам работник, носитель данных;
- другие сотрудники организации (согласно приложения № 4), которые имеют доступ к персональным данным работника, только с письменного согласия самого работника, носителя данных.

8.2. Внешний доступ.

8.2.1. К числу массовых потребителей персональных данных вне ГБУК РО «Библиотека им. Горького» можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

8.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные

пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

8.2.4. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

8.2.5. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

8.2.6. В случае развода бывшая супруга (супруг) имеет право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия.

9. Защита персональных данных

9.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создазать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически развивающийся технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

9.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании.

9.1.2. Для защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание работником требований нормативно-методических документов по защите информации и сохранению тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушений требований разрешительной системы доступа работниками подразделения;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел сотрудников на рабочие места руководителей.

9.1.3. Личные дела могут выдаваться на рабочие места только директору и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения.

9.2. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

9.3. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.

9.4. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

- технические средства охраны, сигнализации;

- порядок охраны территории, зданий, помещений;

-требования к защите информации при интервьюировании и собеседованиях.

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

10.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

10.2. Каждый сотрудник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут в соответствии с федеральными законами ответственность:

- дисциплинарную (замечание, выговор, увольнение);
- административную (предупреждение или административный штраф);
- гражданско-правовую (возмещение причиненного убытка).

10.4. Работник, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность, вплоть до увольнения.

11. Заключительные положения

11.1. Настоящее Положение вступает в силу с момента его утверждения директором и вводится в действие приказом директора ГБУК РО «Библиотека им. Горького».

Положение обязательно для всех работников ГБУК РО «Библиотека им. Горького», если иные условия не предусмотрены в трудовом договоре работника.

Директор ГБУК РО «Библиотека им. Горького» вправе вносить изменения и дополнения в Положение. Работники ГБУК РО «Библиотека им. Горького» должны быть поставлены в известность о вносимых изменениях и дополнениях за 5 дней до вступления их в силу посредством издания директором приказа и ознакомления с ним всех работников ГБУК РО «Библиотека им. Горького»

Приложение № 1
к Положению «О порядке обработки
персональных данных работников
ГБУК РО «Библиотека им. Горького»

Соглашение
о неразглашении персональных данных работника

Я, _____, паспорт серии _____, номер _____,
выданный _____ "__" _____ _____ года.
понимаю, что получаю доступ к персональным данным работников ГБУК РО «Библиотека им. Горького». Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб сотрудникам фирмы, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными работника соблюдать все описанные в Положении о защите персональных данных работника требования.

Я подтверждаю, что не имею права разглашать сведения о (об):
- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате работника;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- характере взаимоотношений в семье;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;

- личных делах и трудовых книжках сотрудников;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.

С Положением о порядке обработки персональных данных работников ГБУК РО «Библиотека им. Горького» и гарантиях их защиты ознакомлен(а).

_____
_____
(должность)
(Ф.И.О.)

"__" _____ 20__ г.
_____(подпись)

Приложение № 2
к Положению «О порядке обработки
персональных данных работников
ГБУК РО «Библиотека им. Горького»

СОГЛАСИЕ

Я, _____
даю согласие на обработку ГБУК РО «Библиотека им. Горького», предоставленных мною своих персональных данных, с целью ведения регистра работников учреждения. Мои персональные данные, в отношении которых дано согласие, включает следующие сведения о (об):

- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате;
- социальных льготах;
- специальности;
- занимаемой должности;
- адресе места жительства, домашнем и мобильном телефонах;
- содержании трудового договора;
- подлинниках и копиях приказов по личному составу;
- личных делах и трудовых книжках сотрудников;

- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

- копиях отчетов, направляемых в органы статистики.

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.

«_____»_____ 2017 г.

_____ _____

(подпись) (расшифровка подписи)

Приложение № 3
к приказу директора
ГБУК РО «Библиотека им. Горького»
от 17.04.2017 г. № 68

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ ГБУК РО «БИБЛИОТЕКА ИМ. ГОРЬКОГО»

1. Общие положения

1.1. Настоящее Положение определяет порядок и условия обработки персональных данных пользователей в ГБУК РО «Библиотека им. Горького» (далее – библиотека), возникающие в процессе их сбора, хранения, использования и уничтожения, и направлено на соблюдение прав пользователей библиотеки при обработке персональных данных.

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

1.3. Основные понятия, используемые в настоящем Положении:

- персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

- 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, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному 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.

2. Принципы обработки персональных данных пользователей

2.1. Сбор персональных данных пользователей библиотекой осуществляется сцелью:

- повышения оперативности и качества обслуживания пользователей, организациидресного, дифференцированного и индивидуального их обслуживания, установленного Правилами пользования Рязанской областной универсальной научной библиотеки им. Горького;Федеральным законом от 29.12.1994 № 78-ФЗ «О библиотечном деле»,

- обеспечения сохранности библиотечного фонда в соответствии с Правиламипользования Рязанской областной универсальной научной библиотеки им. Горького,

- предоставления доступа к дополнительным сервисам сайта библиотеки (rounb.ru),

- осуществления электронного заказа документов через сайт библиотеки (rounb.ru),

- продления срока использования книг.

2.2. Персональные данные пользователей обрабатываются библиотекой наосновании ст. 5 и ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и с согласия пользователя библиотеки на обработку его персональных данных.

2.3. Источником персональных данных служит:

-заявление о согласии на обработку персональных данныхдля информационной системы персональных данных пользователей библиотеки, заполняемое пользователем лично или с его слов библиотекарем при оформлении в библиотеку, удостоверенное собственноручной подписью пользователя,

- форма регистрации пользователя на сайте rounb.ru- заполняется пользователем с целью получения доступа к дополнительным сервисам сайта библиотеки (при заполнении формы пользователю предлагается ознакомиться с пользовательским соглашением на обработку персональных данных и дать свое согласие),

- форма электронного заказа документов на сайте rounb.ru- заполняется пользователем с целью осуществления возможности электронного заказа документов (при заполнении формы пользователю предлагается ознакомиться с пользовательским соглашением на обработку персональных данных и дать свое согласие),

- форма на продление срока использования книг на сайте rounb.ru- заполняется пользователем с целью продления срока использования книг (при заполнении формы пользователю предлагается ознакомиться с пользовательским соглашением на обработку персональных данных и дать свое согласие).

2.4. Персональныеданныепользователейявляютсяконфиденциальнойинформацией, не подлежащей разглашению, и не могут быть использованы библиотекойили ее сотрудниками для целей, не перечисленных в п. 2.1 настоящего Положения.

2.5. Предоставление персональных данных пользователя или их части допускаетсятолько в случаях, предусмотренных действующим законодательством РоссийскойФедерации о безопасности, об оперативно-розыскной деятельности, а также в соответствиис уголовно-исполнительным законодательством Российской Федерации, либо с отдельногописьменного согласия пользователя.

2.6. Перечень персональных данных,заполняемых пользователем.

2.6.1 В заявлении о согласии на обработку персональных данных для информационной системы персональных данных пользователей библиотеки указываются следующие персональные данные:

- Фамилия, имя и отчество пользователя

- Дата рождения (число, месяц, год)

-Сведения о документе, удостоверяющем личность (наименование и серия документа, кем и когда выдан)

- Адрес регистрации (прописки) по месту жительства
- Адрес фактического проживания
- Профессия
- Место работы, должность
- Место учебы, курс, факультет
- Адрес электронной почты

2.6.2 В форме регистрации на сайте rounb.ru указываются следующие персональные данные: адрес электронной почты.

2.6.3 В форме электронного заказа документов через сайт rounb.ru указываются следующие персональные данные: адрес электронной почты, номер читательского билета, телефон.

2.6.4 В форме на продление срока использования книг через сайт rounb.ru указываются следующие персональные данные: адрес электронной почты, номер читательского билета.

3. Условия обработки персональных данных пользователей

3.1. Персональные данные пользователей библиотеки на бумажных носителях хранятся в отделе регистрации пользователей, отделах с функциями обслуживания. Обработка персональных данных на бумажных носителях выполняется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Персональные данные, предоставляемые пользователями при регистрации на сайте библиотеки, хранятся в электронном виде в административной системе сайта библиотеки.

Персональные данные, предоставляемые пользователями при электронном заказе документов через сайт библиотеки, передаются на электронную почту центра межбиблиотечного абонемента отдела библиотечных и информационных коммуникаций, издательско-полиграфической деятельности и дополнительного обслуживания. В административной системе сайта библиотеки эти данные хранятся не более пяти рабочих дней.

Персональные данные, предоставляемые пользователями при продлении срока использования книг через сайт библиотеки, передаются на электронную почту кафедры регистрации, учета и контроля читателей отдела книги и чтения. В административной системе сайта библиотеки эти данные хранятся не более пяти рабочих дней.

3.2. Право доступа к персональным данным пользователей имеют работники библиотеки согласно Приложению № 4 к приказу директора ГБУК РО «Библиотека им. Горького» от 17.04.2017 № 68.

3.3. Работники отделов обслуживания вправе передавать персональные данные пользователя работникам администрации и отдела автоматизации 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 пользователя третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровью пользователя, а также в иных случаях, установленных действующим законодательством.

3.5. При передаче персональных данных пользователя директор предупреждает лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и передает сведения только после получения от этих лиц письменного подтверждения соблюдения этого условия.

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

3.7. Персональные данные пользователя уточняются ежегодно при первом посещении пользователем библиотеки в году, следующем за годом регистрации, либо годом последнего уточнения персональных данных. В случае изменения персональных данных библиотека вносит изменение в заявление о согласовании на обработку персональных данных для информационной системы персональных данных пользователей библиотеки.

3.8. При отсутствии перерегистрации пользователя в течение пяти лет подряд заканчивается срок обработки персональных данных, и они уничтожаются на бумажных носителях и в электронном виде – при условии, что пользователь полностью возвратил в Библиотеку литературу, выданную ему на дом во временное пользование. В противном случае персональные данные блокируются, а уничтожаются и обезличиваются только после снятия задолженности. (Приложение № 1).

4. Права пользователей

4.1. Пользователь 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 пользователя может повлечь за собой обработка его персональных данных.

4.2. Обработка персональных данных в целях информирования пользователя о новых услугах библиотеки, новых поступлениях литературы, проводимых в библиотеке мероприятиях путем осуществления прямых контактов с ним с помощью средств связи и (или) сервиса рассылок допускается только при условии предварительного согласия пользователя и прекращается немедленно по его требованию.

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

4.4. Пользователь 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 пользователей

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

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

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

5.4. Библиотека обязана внести по требованию пользователя необходимые изменения, блокировать его персональные данные по предоставлении пользователем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему пользователю 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 пользователя или его законного представителя и третьих лиц, которым персональные данные этого пользователя были переданы.

5.5. В случае выявления недостоверных персональных данных или неправомерных действий с ними библиотека при обращении или по запросу пользователя осуществляет блокирование персональных данных, относящихся к соответствующему пользователю, с момента такого обращения на период проверки.

5.6. В случае подтверждения факта недостоверности персональных данных библиотека на основании документов, представленных пользователем 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 пользователя или его законного представителя.

5.8. Все обращения субъектов персональных данных фиксируются в журнале учета обращений. (Приложение №2).

6. Ответственность библиотеки и ее сотрудников

6.1. Защита прав пользователей, установленных настоящим Положением изаконодательством РФ, осуществляется судом, в целях пресечения неправомерного использования персональных данных пользователя, 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 пользователя библиотекой и иными лицами, они несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение №1
к Положению о порядке обработки
персональных данных пользователей
ГБУК РО им. Горького

АКТ № _____
об уничтожении персональных данных пользователей библиотеки

Комиссия в составе:_____
_____
_____

назначенная приказом библиотеки от "___" _____ 20___г. № _____, составила настоящий акт в том, что за период с "___" _____ 20___г. по "___" _____20___г. подлежат уничтожению персональные данные пользователей библиотеки на бумажных носителях/машиночитаемые записи в электронных базах данных

N п/п	Ф.И.О. пользователя	N ч/б	Причина уничтожения

В присутствии членов комиссии вышеперечисленные **персональные данные пользователей библиотеки** уничтожены.

Председатель комиссии

_____

Члены комиссии:

_____

_____

"_____" _____ 20____г.

Приложение №2
к Положению о порядке обработки
персональных данных пользователей
ГБУК РО «Библиотека им. Горького»

Журнал учета обращений субъектов персональных данных
о выполнении их законных прав при обработке персональных данных

N п/п	ФИО субъекта ПД	Дата обращения	Цель обращения

Приложение №3
к Положению о порядке обработки
персональных данных пользователей
ГБУК РО «Библиотека им. Горького»

Лист ознакомления

С Положением о порядке обработки персональных данных пользователей ГБУК РО «Библиотека им. Горького», утвержденным приказом от 17.04.2017 г. № 68 ознакомлены:

N п/п	Ф.И.О.	Должность	Дата	Подпись

Приложение № 4
к приказу директора ГБУК РО «Библиотека им. Горького»
от 17.04.2017 № 68

Список сотрудников ГБУК РО «Библиотека им. Горького»,
допущенных к работе с персональными данными

№ п/п	ФИО	Должность	Вид персональных данных
1.	Просин А.А.	первый заместитель директора	Персональные данные работников
2	Чернова Н.Н.	заместитель директора по социокультурной деятельности и связям с общественностью	Персональные данные работников
3.	Полымова А.Д.	заместитель директора по экономике и финансам	Персональные данные работников
4.	Винокурова С.А.	заместитель директора по развитию	Персональные данные работников
5.	Самандина Н.С.	председатель профсоюзного комитета библиотеки	Персональные данные работников
7.	Герасимова Т.Н.	начальник отдела бухгалтерского учета и экономического планирования	Персональные данные работников
8.	Мезенцева Т.М.	ведущий бухгалтер отдела бухгалтерского учета и экономического планирования	Персональные данные работников
9.	Коробова Л.Н.	ведущий бухгалтер отдела бухгалтерского учета и экономического планирования	Персональные данные работников
10.	Суркова Л.А.	ведущий экономист отдела бухгалтерского учета и экономического планирования	Персональные данные работников
11.	Левина И.А.	бухгалтер 1 категории	Персональные данные работников
12.	Теплухина Т.Ю.	ведущий бухгалтер отдела бухгалтерского учета и экономического планирования	Персональные данные работников
13.	Орлова Т.Н.	начальник правовогс отдела	Персональные данные работников
14.	Демидкина Л.А.	начальник отдела кадров	Персональные данные работников

№ п/п	ФИО	Должность	Вид персональных данных
15.	Деева Л.А.	ведущий специалист по кадрам отдела кадров	Персональные данные работников
16.	Пилатова Н.В.	ведущий инженер по охране труда	Персональные данные работников
17.	Чебрякова Г.Н.	начальник отдела автоматизации	Персональные данные работников Персональные данные пользователей
18.	Самандин П.А.	начальник сектора технического обеспечения отдела автоматизации	Персональные данные работников Персональные данные пользователей
19.	Давлетшин М.И.	ведущий программист отдела автоматизации	Персональные данные работников Персональные данные пользователей
20.	Мартынов Д.И.	ведущий программист отдела автоматизации	Персональные данные работников
21.	Ясинская С.А.	главный библиотекарь кафедры абонемента зала книги и чтения по ул. Грибоедова 26/6 зала книги и чтения	Персональные данные пользователей
22.	Сергеева М.В.	библиотекарь 1 категории кафедры регистрации, учета и контроля читателей зала книги и чтения	Персональные данные пользователей
23.	Селихова И.Ю.	ведущий библиотекарь кафедры регистрации, учета и контроля читателей зала книги и чтения	Персональные данные пользователей
24.	Рощина О.А.	главный библиотекарь группы работы с задолжниками центра книги и чтения	Персональные данные пользователей
25.	Русалеева Е.В.	библиотекарь 1 категории кафедры регистрации, учета и контроля читателей зала книги и чтения	Персональные данные пользователей
26.	Искакова Н.А.	ведущий программист отдела автоматизации	Персональные данные пользователей
27.	Демша С.А.	ведущий программист отдела автоматизации	Персональные данные пользователей

№ п/п	ФИО	Должность	Вид персональных данных
28.	Серегина Галина Борисовна	главный библиотекарь Центра МБА и ЭДД	Персональные данные пользователей
29.	Чиникина Светлана Борисовна	главный библиотекарь Центра МБА и ЭДД	Персональные данные пользователей